بسم الله الرحمن الرحیم

مقام معظم رهبری:
تنها راه جبران عقب‌ماندگی علمی کشور، وجود اراده مستحکم برای پیشرفت واقعی در علم و فناوری است.

نشریه علمی
علوم و فناوری‌های پدافند نوین

سال یازدهم / شماره ۴ / زمستان ۱۳۹۹ (شماره پیاپی ۴۲)

صاحب امتیاز: دانشگاه جامع امام حسین(ع)
مدیر مسئول: دکتر روح اله رضوی نژاد
سردبیر: دکتر حسین فخرائیان
مدیر اجرایی: سعید زردار

- دارای درجه علمی- پژوهشی بر اساس نامه شماره ۸۹/۳/۱۱/۵۱۱۵۰ مورخ ۱۳۸۹/۸/۳۰ وزارت علوم، تحقیقات و فناوری
- شماره پروانه انتشار: ۱۲۴/۳۹۴۲ مورخ ۱۳۸۷/۹/۱۳ وزارت فرهنگ و ارشاد اسلامی
- کارشناس: امیرمهدی داداش‌زاده
- ویراستار و صفحه‌آرا: مهندس مهربان اسماعیل‌زاده
- لیتوگرافی چاپ و صحافی: مرکز چاپ سپاه
- شاپا: ۲۹۳۵- ۲۶۷۶
- قیمت: ۲۰۰۰۰۰ریال

این مجله در پایگاه‌های زیر در دسترس می‌باشد:

- پایگاه استنادی علوم جهان اسلام (ISC) (www.isc.gov.ir)
- مرکز منطقه‌ای اطلاع رسانی علوم و فناوری (www.ricest.ac.ir)
- بانک اطلاعات نشریات علمی کشور (www.magiran.com)
- پایگاه علمی جهاد دانشگاهی (www.SID.ir)
- پایگاه گوگل اسکالر (www. scholar.google.com)
- پایگاه سیویلیکا (www.civilica.com)

این مجله به مدیریت دانشکده و پژوهشکده علوم پایه و با همکاری دانشکده‌ها و پژوهشکده‌های پدافند غیرعامل، فناوری اطلاعات و ارتباطات و فنی و مهندسی منتشر می‌گردد.

نشانی: تهران، بزرگراه شهید بابایی، دانشگاه جامع امام حسین(ع)، موقعیت امام صادق(ع)، ساختمان باقرالعلوم(ع)، دایره نشریات، نشریه علمی "علوم و فناوری‌های پدافند نوین"

تلفن و نمابر: ۷۴۱۸۹۱۹۷ **صندوق پستی:** ۱۸۷- ۱۶۵۸۵

www.adst.ihu.ac.ir **Padafandn@ihu.ac.ir**

اعضای هیئت تحریریه

۱) **دکتر سید غلامرضا اسلامی** (استاد- دانشگاه تهران)

۲) **دکتر رمضانعلی ایزدی‌فرد** (استادیار- دانشگاه بین‌المللی امام خمینی (ره))

۳) **دکتر محمدحسین بهشتی** (استاد- پژوهشگاه پلیمر و پتروشیمی ایران)

۴) **دکتر پرویز پروین** (استاد- دانشگاه صنعتی امیرکبیر)

۵) **دکتر حسین خدارحمی** (استاد- دانشگاه جامع امام حسین(ع))

۶) **دکتر غلامحسین ریاضی** (استاد- دانشگاه تهران)

۷) **دکتر مجتبی سمنانی رهبر** (دانشیار- دانشگاه جامع امام حسین(ع))

۸) **دکتر احمد شعبانی** (استاد- دانشگاه شهید بهشتی)

۹) **دکتر محمود صالح اصفهانی** (استادیار- دانشگاه جامع امام حسین(ع))

۱۰) **دکتر سید محمد علوی** (دانشیار- دانشگاه جامع امام حسین(ع))

۱۱) **دکتر محمدرضا علیزاده پهلوانی** (دانشیار- دانشگاه صنعتی مالک اشتر)

۱۲) **دکتر حسین فخرائیان** (استاد- دانشگاه جامع امام حسین(ع))

۱۳) **دکتر محمدحسین کشاورز** (استاد- دانشگاه صنعتی مالک اشتر)

۱۴) **دکتر علی‌محمد لطیفی** (دانشیار- دانشگاه علوم پزشکی بقیه‌الله الاعظم(عج))

۱۵) **دکتر مصطفی محمدپورامینی** (استاد- دانشگاه شهید بهشتی)

۱۶) **دکتر محمد مردانی شهربابک** (دانشیار- دانشگاه جامع امام حسین(ع))

۱۷) **دکتر عبدالرسول میرقدری** (دانشیار- دانشگاه جامع امام حسین(ع))

۱۸) **دکتر علی‌اکبر یوسفی** (استاد- پژوهشگاه پلیمر و پتروشیمی ایران)

مشاوران و داوران

۱) **فرنوش باسلیقه** (دانشگاه صنعتی شاهرود)

۲) **سمیه ملایی** (دانشگاه بناب آذربایجان شرقی)

۳) **محمد ملکشاهی** (دانشگاه صنعتی بیرجند)

۴) **صفا پیمان** (دانشگاه جامع امام حسین(ع))

۵) **ابراهیم زمانی بیدختی** (دانشگاه صنعتی شاهرود)

۶) **مرتضی حسین‌پور** (دانشگاه صنعتی امیرکبیر)

۷) **حسن آقابراتی** (دانشگاه صنعتی امیرکبیر)

۸) **رضا کامگار** (دانشگاه شهرکرد)

۹) **حبیب اله اعلمی** (دانشگاه جامع امام حسین(ع))

۱۰) **محمدحسین ولایتی** (دانشگاه سمنان)

۱۱) **سیدمیثم سیدبرزگر** (دانشگاه صنعتی شاهرود)

۱۲) **محمد میرزایی** (دانشگاه صنعتی نوشیروانی بابل)

۱۳) **شهاب دهقان** (دانشگاه آزاد اسلامی واحد قزوین)

۱۴) **امین حاجی‌زاده** (دانشگاه آلبورگ دانمارک)

۱۵) **محمد بهروزیان نژاد** (دانشگاه آزاد اسلامی واحد شادگان)

۱۶) **مصطفی عباسی** (دانشگاه جامع امام حسین(ع))

۱۷) **مهدی نقوی** (دانشگاه جامع امام حسین(ع))

۱۸) **محمدرضا پارسائی** (دانشگاه صنعتی شیراز)

۱۹) **حاتم عبدلی** (دانشگاه بوعلی سینا)

۲۰) **آرش غفوری** (دانشگاه جامع امام حسین(ع))

۲۱) **دانیال جواهری** (دانشگاه آزاد اسلامی واحد علوم و تحقیقات)

۲۲) **عبدالرسول میرقدری** (دانشگاه جامع امام حسین(ع))

۲۳) **مریم ایلچی** (سازمان انرژی اتمی ایران)

۲۴) **سعید علیایی** (دانشگاه تربیت دبیر شهید رجایی)

۲۵) **مصطفی جانی** (دانشگاه شهید بهشتی)

۲۶) **مریم کریمی** (سازمان انرژی اتمی ایران)

۲۷) **رضا غفارپور** (دانشگاه جامع امام حسین(ع))

۲۸) **جواد خلیل‌زاده** (دانشگاه جامع امام حسین(ع))

۲۹) **محمدرضا علیزاده پهلوانی** (دانشگاه صنعتی مالک اشتر)

۳۰) **رمضانعلی ایزدی‌فرد** (دانشگاه بین‌المللی امام خمینی(ره))

۳۱) **محمد مردانی شهر بابک** (دانشگاه جامع امام حسین(ع))

۳۲) **حسین فخرائیان** (دانشگاه جامع امام حسین(ع))

دانشگاه‌ها ومؤسسات همکار

۱) دانشگاه صنعتی مالک اشتر

۲) دانشگاه علوم پزشکی بقیه‌الله‌الاعظم(عج)

۳) مرکز تحقیقات ساختمان و مسکن وزارت راه و شهرسازی

۴) مؤسسه پژوهشی علوم و فناوری رنگ

۵) پژوهشگاه شیمی و مهندسی شیمی ایران

۶) پژوهشگاه پلیمر و پتروشیمی ایران

فهرست مطالب

- **بررسی عددی تأثیر هندسه بر میزان جذب انرژی پانل‌های ساندویچی تحت بارگذاری انفجاری ۳۴۷**
صفا پیمان، علی ابراهیم‌زاده
- **بررسی رفتار میراگر اصطکاکی در مهاربندهای ضربدری در برابر نیروی انفجار ۳۵۷**
سلیمان قوهستانی، محمد کارکن، مجید یعقوبی، صفر خلیفه
- **بررسی اثر تخریبی انفجار در فواصل مختلف بر دیوار حائل بتنی ۳۶۹**
محمدحسین تقوی‌پارسا، علی گراوند
- **ارزش‌گذاری خطوط سامانه‌های توزیع برق جهت تسریع روند بازیابی و بهبود شاخص تاب‌آوری با در نظر گرفتن تولیدات پراکنده ۳۸۳**
حمیدرضا شریف مقدم، رضا دشتی
- **ارائه الگوریتمی جهت شناسایی آسیب‌پذیرترین شین در شبکه هوشمند برق در حمله سایبری مبتنی بر تخمین حالت ۳۹۱**
امیرحسین طیبی، رضا شریفی، امیرحسین سالمی، فرامرز فقیهی
- **یک سامانه حفاظت ویژه جدید جهت جلوگیری از وقوع ناپایداری ولتاژ بلندمدت در مقابل حملات گرافیتی ۴۰۳**
سیاوش یاری، حمید خوشخو، عرفان اسدی
- **تبیین نقش بازدارنده ذخیره‌سازهای الکتریکی و برنامه‌ریزی واحدهای تولیدی UC با و بدون حضور ذخیره‌سازها از منظر پدافند غیرعامل ۴۱۵**
سعید عسکری، حبیب‌الله سهامی، عباس علی‌آبادی
- **کاهش هشدارهای سامانه‌های تشخیص نفوذ به کمک تعمیم ویژگی‌های حملات در حوزه داده‌کاوی چندبعدی ۴۲۹**
مهدی ملکی، محمد لطفی
- **بهبود احراز هویت در خانه هوشمند مبتنی بر رمز یکبار مصرف و رمزنگاری منحنی بیضوی..... ۴۳۹**
نرگس اسدنجفی، مهدی ملامطلبی
- **طراحی یک حسگر زیستی جدید ضریب شکستی مبتنی بر بلورفوتونی مناسب جهت تشخیص DNA ۴۵۱**
یدالله شهامت، جواد خلیل‌زاده، علی ریاحی

راهنمای تهیه مقاله..... ۴۶۵

فرم اشتراک مجله..... ۴۶۶

- ✓ مطالب ارائه شده در مقاله‌ها، لزوماً نظرات هیئت تحریریه را منعکس نمی‌کند.
- ✓ ذکر مطالب، تنها با ارجاع به این مجله بلامانع است.
- ✓ نسخه الکترونیکی این مقالات به‌صورت رنگی در سایت مجله (www.adst.ihu.ac.ir) در دسترس می‌باشد.

محورهای فعالیت مجله

دانشکده و پژوهشکده فنی و مهندسی دانشگاه جامع امام حسین(ع) به‌منظور فراهم آوردن بستری مناسب برای ارتقاء دانش پدافند غیرعامل در کشور و ارائه پیشرفت‌های جدید و دستاوردهای علمی و پژوهشی پژوهشگران، محققان و دانشجویان، نشریه علمی «*علوم و فناوری‌های پدافند نوین*» را با همکاری دانشکده‌ها و پژوهشکده‌های فناوری اطلاعات و ارتباطات، علوم پایه و پدافند غیرعامل و نیز مشارکت فعال پژوهشگاه شیمی و مهندسی شیمی ایران، پژوهشگاه پلیمر و پتروشیمی ایران، پژوهشگاه علوم و فناوری رنگ، دانشگاه صنعتی مالک اشتر، دانشگاه علوم پزشکی بقیه‌الله‌الاعظم(عج) و مرکز تحقیقات ساختمان و مسکن وزارت راه و شهرسازی منتشر می‌نماید.

این مجله، مقاله‌های علمی-پژوهشی را به چاپ می‌رساند که حاصل پژوهش‌های اصیل و حاوی نتایج جدید در زمینه‌های تخصصی ذیل باشند:

۱. مدیریت بحران (تحلیل مکانی و مکان‌یابی شبکه‌های اطلاعاتی، تأسیسات، سازه‌های حساس و ...)

۲. آشکارسازی، رفع آلودگی و حفاظت و ایمنی (شیمیایی، زیستی و هسته‌ای و...)

۳. نور و لیزر (شنود لیزری، لیزر قدرت و...)

۴. شناسایی (استتار، اختفاء، پوشش، فریب، رنگ‌های نامرئی و...)

۵. استحکامات و تخریب (پلیمرها، کامپوزیت‌ها، مصالح مقاوم در مقابل انفجار و...)

۶. صوت و آکوستیک (بازدارنده‌های صوتی و...)

۷. IT و جنگ سایبری (امنیت داده، نفوذ و اختلال در شبکه‌های اطلاعاتی، رادارها، مقابله با هکرها و...)

۸. الکترومغناطیس و الکترونیک (اختلال در امواج، جمینگ، امواج میکروویو قوی و...)

۹. مواد (چسبنده‌ها، لغزنده‌ها، آتش‌گیرها و...)

۱۰. داروها و ناتوان کننده‌ها (خواب‌آورها، بی‌حس‌کننده‌ها و...)

۱۱. رمزنگاری و کدگذاری (اطلاعات، تصاویر و ...)

- **از اعضای هیئت علمی، پژوهشگران و دانشجویان تحصیلات تکمیلی دعوت می‌نماید مقاله‌های فارسی خود را مطابق راهنمای تنظیم مقاله تهیه و با مراجعه به سایت مجله (adst.ihu.ac.ir) و ثبت نام در آن، نسخه الکترونیکی مقاله را به دفتر مجله ارسال نمایند.**
- **مقاله‌های ارسالی نباید قبلاً در هیچ مجله داخلی یا خارجی چاپ شده باشند.**

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۳۵۵-۳۴۷

«علمی- پژوهش»

بررسی عددی تأثیر هندسه بر میزان جذب انرژی پانل‌های ساندویچی تحت بارگذاری انفجاری

صفا پیمان[۱*]، علی ابراهیم‌زاده[۲]
۱- استادیار، ۲- دانشجوی کارشناسی ارشد، دانشگاه جامع امام حسین (ع)
(دریافت: ۹۷/۱۲/۱۹، پذیرش: ۹۸/۱۲/۲۳)

چکیده

در سال‌های اخیر با پیشرفت فناوری‌های نوین در حوزه سازه، توجه زیادی به المان‌هایی مانند پانل‌های ساندویچی شده است. این نوع از المان‌ها درعین‌حال که وزن کمی دارند دارای مقاومت بالایی نیز هستند. اجزای ساندویچی از پرکاربردترین المان‌ها برای مقابله با فشار ناشی از موج انفجار هستند. هسته پانل‌های ساندویچی مهم‌ترین نقش را در جذب و استهلاک انرژی، بر عهده دارد. شکل هندسی هسته می‌تواند در میزان جذب انرژی نقش تعیین‌کننده‌ای داشته باشد. بر این اساس، در این مقاله، اثر شکل هندسی هسته پانل ساندویچی فولادی، بر رفتار و میزان جذب انرژی آن در برابر موج انفجار با روش عددی بررسی‌شده است. حل عددی با استفاده از نرم‌افزار اجزای محدود آباکوس انجام می‌شود. اعتبارسنجی پاسخ‌های به‌دست‌آمده از حل عددی، با داده‌های تجربی مقالات معتبر انجام شده است. در ادامه، پانل‌های ساندویچی با چهار نوع هسته مختلف متداول و دارای قابلیت ساخت آسان، تحت اثر فشارهای متفاوت موج انفجار مدل شدند و اثر هندسه هسته بر میزان جابجایی و جذب انرژی، موردبررسی قرار گرفت. دو معیار مهم در طراحی این نوع پانل‌های ساندویچی بیشینه کردن میزان جذب انرژی و کمینه کردن مقدار بیشینه جابجایی است. نتایج به‌دست‌آمده نشان می‌دهد، در فشارهای پایین مدل ۴ با هسته دارای شبکه افقی چهارضلعی، بیشترین میزان جذب انرژی و کمترین جابجایی را دارد. با این وجود، در فشارهای بالا مدل ۲ با هسته دارای شبکه عمودی شش‌ضلعی دارای کمترین میزان جابجایی و مدل ۱ با شبکه عمودی شش‌ضلعی دارای بیشینه میزان جذب انرژی است. به عبارت دیگر وابسته به میزان فشار انفجار، پانل ساندویچی با هندسه خاصی می‌تواند بهترین عملکرد را داشته باشد.

کلیدواژه‌ها: پانل ساندویچی، تحلیل عددی، موج انفجار، جذب انرژی

Numerical Investigation of the Effect of Geometry on the Energy Absorption Rate of Sandwich Panels under Blast Loading

S. Peyman*, A. Ebrahimzade
*Imam Hossein University
(Received: 10/03/2019; Accepted: 13/03/2020)

Abstract

In the recent years, advent of new technologies in the field of Structural Engineering, elements such as Sandwich Panels has attracted more attention, which are lightweight and highly resistant.Sandwich components are the most widely used elements to resist against the pressure of explosion wave. The core of the sandwich panels does the most important role in absorbing and dissipating the energy of the explosion.And geometric shape of the core can have a decisive role in the amount of energy absorption. Accordingly, in this paper, the effect of geometric shape of the core of the steel sandwich panel on its behavior and amount of energy absorption against the explosion wave is analyzed by numerical methods. Abaqusfinite element software is used for simulation and analyzing. Validation of the responses obtained from numerical solution was performed with experimental data of valid papers. In the following, sandwich panels with four different types of regular and easily fabricated cores, were modeled under different pressures of explosive wave. And the effect of core geometry on the amount of energy absorption and displacement was investigated.Two important criteria in designing these types of sandwich panels are maximizing energy absorption and minimizing maximum displacement. The results show that at low pressures Model 4 with a quadrilateral horizontal core has the maximum energy absorption and minimum displacement value. However, at high pressures Model 2 with a hexagonal vertical core has the minimum displacement and Model 1 with a quadrilateral vertical has the maximum energy absorption. In other words related to the explosion pressure, a sandwich panel with the special geometry can have the best performance.

Keywords: Sandwich Panel, Numerical Analysis, Explosion Wave, Energy Absorption

*Corresponding Author E-mail: speyman@ihu.ac.ir

۱. مقدمه

نیاز به سازه‌های سبک و ایمن، اهمیت طرح سازه‌های جدید ازنظر طرح هندسی و مواد را روشن می‌کند. پانل ساندویچی از ارزشمندترین آرایش‌های سازه‌ای جهت استفاده بهینه و مؤثر در طراحی و ساخت سازه‌ها می‌باشد. پانل‌های ساندویچی از دو جزء اصلی هسته و پوسته تشکیل‌شده‌اند.استفاده از پانل ساندویچی در سازه موجب می‌شود که با توجه به فضای خالی موجود در آن، علاوه بر کاهش وزن سازه، عملکرد سازه را در برابر حرارت و ارتعاشات وارده بهبود بخشد. همچنین این نوع از سازه‌ها به‌دلیل سختی زیاد و ظرفیت جذب انرژی قابل‌توجهی که دارند در برابر بارهای دینامیکی مانند خستگی، ضربه یا بارهای انفجاری مقاومت خوبی را از خود نشان می‌دهند. اخیراً به مسئله اثر موج انفجار روی پانل ساندویچی فلزی توجه ویژه‌ای شده است. اغلب وقتی تنش خمشی و ساختار فوق سبک در طراحی موردتوجه است، ساختار ساندویچی مطرح می‌شود [۱]. پانل ساندویچی نسبت به کامپوزیت‌های لایه‌ای قابلیت جذب انرژی بیشتری دارند. هرچه ضخامت هسته پانل ساندویچی بیشتر شود، مقاومت آن در برابر ضربه ناشی از موج انفجار افزایش پیدا می‌کند [۲]. پانل‌ها به‌دلیل شکل هندسی ویژه‌ای که دارند، علاوه بر فاکتور سبکی، رفتار بسیار مناسبی در برابر ضربه ناشی از انفجار و جذب انرژی ناشی از آن، دارد. ازاین‌رو بسیاری از جاذب‌های انرژی به شکل پانل طراحی می‌گردند. هسته پانل مهم‌ترین نقش را در استهلاک انرژی انفجار دارد؛ که به‌عنوان فدا شونده می‌تواند از دو جنبه هندسی و خواص مکانیکی مواد مورد ارزیابی قرار بگیرد. ویژگی‌های هندسی هسته مانند اندازه و تعداد سلول‌ها، شکل هندسی سلول‌ها، ضخامت ورق هسته، ضخامت یا عمق هسته و... می‌توانند در میزان جذب انرژی پانل مؤثر باشند [۳].

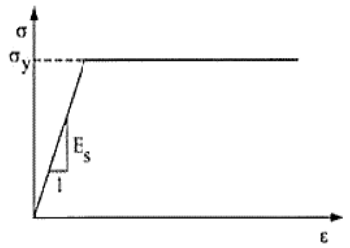
نوریک و مارتین [۴ و ۵] روابط تئوری و نتایج آزمایشگاهی تغییر شکل صفحات نازک در برابر بار انفجاری را تحلیل و ارائه نمودند. در مطالعه آن‌ها نسبت ضخامت به خیز به‌عنوان تابعی از بار وارده، خواص مواد، هندسه و ابعاد صفحه، مورد ارزیابی قرار گرفت. همچنین راجندرانا و لی [۶] به بررسی رفتار ورق‌ها تحت بارگذاری انفجاری پرداختند و روابط ریاضی حاکم بر مدل‌سازی بار انفجاری را به‌دست‌آمده آوردند. ژاکوب و همکارانش [۷] تحقیقات خود را روی صفحات فولادی با نسبت های متغیر طول به عرض و همچنین تغییر در ضخامت، ارائه نموده و نتایج تحقیقات خود را با روش المان محدود ارزیابی نمودند. زئو و هاتچینسون [۸] مطالعه‌ای جهت ارزیابی پانل ساندویچی تحت موج انفجار انجام دادند. مطالعه آن‌ها نشان داد که پانل ساندویچی با هسته دارای مقاومت کافی، می‌تواند ایمپالس بزرگ‌تری را نسبت به یک صفحه فلزی با جرم یکسان، تحمل کند. یکی از مطالعات آزمایشگاهی توسط موری [۹] باهدف تعیین عملکرد و مودهای شکست سازه ساندویچی که تحت اثر موج انفجار واقع‌شده بود، صورت گرفت. عملکرد سازه ساندویچی نسبت به صفحه فلزی معادل مورد ارزیابی قرار گرفت. این مطالعه پیشنهاد کرد که استفاده از سازه ساندویچی مفید است و قادر است مقدار بیشینه جابجایی را به ۶۸٪ جابجایی ورق معادل برساند. این مطالعه روابط تئوری که پیشنهاد می‌دهد هسته نرم میزان عملکرد پانل را ارتقاء می‌دهد را نیز تائید کرد. والدویت [۱۰] یک مطالعه تحلیلی- آزمایشگاهی روی پانل ساندویچی فلزی با هسته موج‌دار، تحت بارگذاری‌های طولی و عرضی انجام داد. طراحی پانل بر اساس طرح‌های سازوکار شکست با استفاده از مدل‌های تحلیلی شکست صورت گرفت. نتایج با داده‌های آزمایشگاهی و تحلیل اجزاء محدود مقایسه شدند. والدویت بارگذاری‌های محدود را نیز مورد تحلیل قرارداد و به این نتیجه رسید که این بارها می‌توانند نسبت به سازوکارهای شکست حساس باشند. بر اساس نتایج وقتی تسلیم رویه غالب می‌شود، سخت شدگی قابل‌ملاحظه‌ای که در اثر غیرخطی شدن اولیه رخ می‌دهد، موجب استحکام زیادی می‌شود. در مقابل، برای طراحی‌هایی که توسط کمانش الاستیک یا پلاستیک کنترل می‌شود، شروع گسیختگی توسط نرم شدگی رخ می‌دهد. این نشان می‌دهد که وقتی‌که استحکام سازه یک نیاز کلیدی است، توصیه می‌شود که طراحی بر اساس دامنه گسیختگی رویه پانل ساندویچی صورت گیرد. جینگ [۱۱] پاسخ دینامیکی پانل ساندویچی استوانه‌ای با هسته‌های آلومینیوم و فوم را به‌صورت عددی در مقابل موج انفجار موردبررسی قرارداد. نتایج عددی نشان داد که کرنش فشاری که مهم‌ترین نقش را در جذب انرژی سازه ساندویچی دارد، تقریباً با ایمپالس نرمال شده به‌صورت خطی افزایش می‌یابد. این کرنش با افزایش چگالی نسبی (افزایش ضخامت هسته یا پوسته‌ها)، نیز کاهش می‌یابد.

وطنی اسکویی و کیا کجوری [۱۲] مطالعاتی روی اثر موج انفجار روی پانل ساندویچی با هسته I-شکل به‌صورت عددی انجام داد؛ و به این نتیجه رسید که هسته I-شکل با سوراخ‌های دایره‌ای در جان خود می‌تواند جذب انرژی بیشتر و جابجایی کمتری نسبت به هسته I-شکل و همچنین صفحه فلزی معادل داشته باشد. آری هاران و همکاران [۱۳]، رفتار ساندویچ پانل با هسته لانه زنبوری تماما فولادی را با ساندویچ پانلی که لایه در معرض انفجار آن فولادی و هسته لانه زنبوری و لایه پایینی آن از جنس سبک پلیمری باشد، را با هم مقایسه نمودند. مطالعه آنها نشان داد ساندویچ پانل کامپوزیتی در عین سبک بودن عملکرد بسیار مناسب‌تری دارد. سلیمانی و همکاران اثر انفجار بر پانل‌های ساندویچی با هسته‌های لانه زنبوری و مربعی را به‌صورت عددی و آزمایشگاهی بررسی نمودند. نتایج بررسی آنها نشان داد با افزایش سایز المان‌های هسته میانی، هسته با شکل مربع عملکرد بهتری دارد [۱۴]. سبزواری و شهابیان تحلیل

رفتاری، چهار نوع ورق موجدار مستطیلی، ذوزنقه‌ای، مثلثی و بیضوی را برای هسته پانل‌های ساندویچی در معرض انفجار بررسی نمودند[۱۵]. در بحث جذب انرژی، پارامترهای مختلفی مانند اندازه و هندسه‌ی سازه، جنس سازه و نحوه اعمال بار و همچنین میزان بار وارده بر رفتار سازه اثرگذار می‌باشند. برای دستیابی به یک جاذب بهینه، باید سازه از دیدگاه‌های گوناگونی بررسی گردد. مهم‌ترین معیار طراحی در سازه، معیار سختی است؛ بدین معنا که هرچه سازه سخت‌تر باشد مفیدتر خواهد بود. این مهم با کمینه کردن میزان جابجایی سازه حاصل می‌گردد. سختی یک المان با میزان جذب انرژی آن رابطه مشخصی ندارد. در اینجا چون المان‌های ساندویچی نقش غیر سازه‌ای و فداشونده دارند بنابراین، بهتر است معیار طراحی را در این المان‌های فداشونده میزان جذب انرژی قرار داد. اگر معیار طراحی، جذب انرژی باشد؛ (این معیار بیشتر جهت طراحی جاذب‌های فدا شونده به‌کار می‌رود.) باید میزان جذب انرژی سازه را حداکثر نمود. میزان استهلاک انرژی وابسته به‌سرعت با عنوان انرژی جنبشی، میزان استهلاک انرژی در اثر کرنش‌های الاستیک با عنوان انرژی کرنشی و میزان استهلاک انرژی در اثر کرنش‌های در محدوده پلاستیک با عنوان انرژی پلاستیک معرفی‌شده است. در بارگذاری‌های انفجاری چون غالباً مواد وارد محدوده پلاستیک می‌شوند و میزان انرژی کرنشی در مقابل انرژی پلاستیک قابل‌چشم‌پوشی است. لذا معیار غالب جهت بررسی میزان جذب انرژی، جذب انرژی پلاستیک در نظر گرفته‌شده است. از طرفی معیار مقایسه باید جذب انرژی ویژه باشد؛ اما با توجه به این‌که در این پژوهش جرم همه پانل‌ها با یکدیگر برابر فرض شده‌اند؛ بنابراین، خود جذب انرژی ملاک ارزیابی قرارگرفته است. قسمت بیشتر انرژی ناشی از موج انفجار، توسط تغییر شکل‌های پلاستیک هسته میانی پانل ساندویچی جذب می‌شود. هسته‌های دارای سلول‌های با هندسه چهارضلعی و شش‌ضلعی به‌دلیل قابلیت ساخت آسان و همچنین مقاومت و استحکام هندسی بالا در صنعت کاربرد زیادی دارند. در این مقاله این پانل‌های دارای هسته با شبکه‌های چهارضلعی و شش‌ضلعی مدل شده‌اند. ضمن مقایسه شبکه‌های چهارضلعی و شش‌ضلعی، میزان جذب انرژی و جابجایی پانل‌ها در صورت قرارگرفتن شبکه هسته به‌صورت افقی و عمودی نیز مورد بررسی قرار گرفته است. بر این اساس، با طراحی ۴ نمونه پانل ساندویچی مرسوم و متداول، اثر تغییر شکل هندسی سلول‌های هسته پانل بر رفتار آن‌ها در حالت قرار گرفتن در برابر فشارهای ناشی از انفجار یک، دو و سه کیلوگرم تی‌ان‌تی بررسی‌شده، و میزان جذب انرژی و جابجایی آن‌ها با یکدیگر مقایسه شده است.

۲. جذب انرژی

جذب انرژی با تغییر شکل بروز کرده و با کمیت‌های مربوط به تغییر شکل قابل‌اندازه‌گیری است. نمونه این کمیت‌ها، بیشینه مقدار خیز سازه یا چرخش‌های تکیه‌گاهی آن است. مواد سازه‌ای دارای رفتاری الاستیک و پلاستیک هستند. رفتار الاستوپلاستیک را برای راحت‌تر شدن محاسبات به‌صورت‌های مختلف ساده‌سازی کرده‌اند. معروف‌ترین و ساده‌ترین مدل که بسیار موردتوجه قرارگرفته است، رفتار الاستوپلاستیک کامل است؛ که در شکل (۱) نشان داده‌شده است. که ε بیانگر کرنش و σ بیانگر تنش و E_s نیز مدول الاستیسیته ماده مورد نظر را نشان می‌دهد.



شکل ۱. رفتار الاستوپلاستیک کامل

در طی این مدل از رفتار مواد، پس از رسیدن نیرو به حد جاری شدن، نیرو دیگر افزایش نمی‌یابد؛ و نیروی خارجی اعمال‌شده به‌صورت انرژی کرنشی درون ماده ذخیره می‌شود؛ که به‌صورت تغییر شکل ظاهر می‌گردد. این تغییر شکل تا آنجا ادامه می‌یابد که سازه دیگر قادر به جذب انرژی خارجی نباشد؛ و سرانجام گسیختگی در حدود جابجایی حد پلاستیک روی دهد. ازاین‌رو مواد شکل‌پذیر در برابر مواد ترد، قابلیت جذب انرژی بیشتری دارند. شکل (۱) منحنی تنش-کرنش را برای یک المان پانل ساندویچی، تحت بارگذاری انفجاری نشان می‌دهد. سطح زیر منحنی تنش-کرنش ، انرژی جذب‌شده توسط المان را ارائه می‌دهد. برای به‌دست‌آوردن کل انرژی جذب‌شده (E_A) می‌توان از رابطه (۱) استفاده نمود.

$$E_A = \int_0^{S_b} P ds \qquad (۱)$$

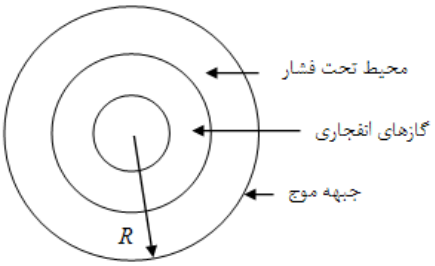
در رابطه (۱)، P نیروی اعمالی، S_b میزان جابجایی نهایی و ds المان جابجایی در طول روند مچاله شدن است.

۳. شناخت و بررسی موج انفجار

انفجار ناشی از یک خرج کروی در هوای آزاد، امواجی با فشار و سرعت زیاد به شکل کروی تولید و در محیط اطراف منتشر می‌کند. باگذشت زمان هرقدر که شعاع کره و به‌تبع آن حجم محیط متأثر از امواج انفجار بیشتر می‌شود، فشار و سرعت موج ناشی از انفجار به‌شدت کاهش می‌یابد.

به فشار ناشی از موج انفجار در هر نقطه از محیط اطراف انفجار که مقدار آن با وزن ماده منفجره رابطه مستقیم و بافاصله از مرکز انفجار رابطه معکوس دارد، اضافه فشار می‌گویند. محاسبه

اندازه این فشار و تغییرات آن در طی زمان از اهمیت کاربردی زیادی برخوردار است. در ادامه فرایند موردنیاز برای محاسبه اضافه فشار آورده می‌شود.



شکل ۲. انتشار موج انفجار در محیط [۱۶]

با توجه به پیچیده بودن پدیده انفجار، معمولاً رابطه‌های ارائه‌شده برای محاسبه اضافه فشار یا فشار ناشی از انفجار، ترکیبی از روابط تئوری و نتایج آزمایشگاهی است. در قرن نوزده میلادی آزمایش‌های گسترده‌ای درباره بررسی پدیده انفجار و آثار آن بر سازه‌ها و تأسیسات نزدیک به محل انفجار توسط پژوهشگران انجام‌شده است [۱۷]. بر مبنای نتایج حاصل از این آزمایش‌ها و نظریه‌های حاکم بر انتشار موج، روابط مختلفی برای محاسبه اندازه اضافه فشار ناشی از انفجار ارائه‌شده است. در ادامه دو رابطه‌ای که ارزش کاربردی بیشتری دارند و توسط آیین‌نامه‌ها و دستورالعمل‌های طراحی سازه‌ها در برابر انفجار نیز پذیرفته‌شده‌اند، برای محاسبه اضافه فشار آورده می‌شوند:

برود [۱۸] در سال ۱۹۵۵، با توجه به‌اندازه فشار در هر نقطه، رابطه‌ای دو ضابطه‌ای را برای محاسبه اضافه فشار انفجار در فاصله‌های نزدیک و دور از محل انفجار ارائه کرد:

$$P_s = \frac{6.7}{z^3} + 1 \qquad P_s > 10\ bar \qquad (۲)$$

$$P_s = \frac{0.975}{z} + \frac{1.455}{z^2} + \frac{5.85}{z^3} - 0.019 \quad P_s < 10\ bar$$

هنریچ [۱۹] بر مبنای مطالعات نظری و آزمایشگاهی رابطه‌ای سه ضابطه‌ای را برای محاسبه اضافه فشار ناشی از انفجار ارائه نمود:

$$P_s = \frac{14.027}{z} + \frac{5.540}{z^2} + \frac{0.357}{z^3} + \frac{0.00625}{z^4} bar \quad 0.05 \le z \le 0.3$$

$$P_s = \frac{6.194}{z} - \frac{0.326}{z^2} + \frac{2.132}{z^3} bar \quad 0.3 \le z \le 1 \qquad (۳)$$

$$P_s = \frac{0.662}{z} + \frac{4.05}{z^2} + \frac{3.288}{z^3} bar \qquad 1 \le z \le 10$$

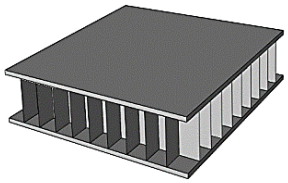
در این رابطه‌ها P_s اضافه فشار دینامیکی و Z فاصله مقیاس شده است که از رابطه زیر به دست می‌آید:

$$z = R[\frac{1}{w}]^{1/3} \qquad (۴)$$

در رابطه بالا، w وزن تی‌ان‌تی معادل ماده انفجاری موردنظر یا قدرت انفجار و R فاصله نقطه موردبررسی تا مرکز انفجار است.

۴. طرح آزمایش و اعتبارسنجی

با توجه به پرهزینه بودن تحقیق‌های آزمایشی و نظر به موجود بودن نتایج آزمایش‌های انجام‌شده، برای بررسی و صحت‌سنجی تحلیل‌های عددی انجام‌شده در این تحقیق، با استفاده از نتایج به‌دست‌آمده توسط دهارماسنا [۲۰] صحت مدل‌سازی پانل ساندویچی تحت بار انفجار در محیط نرم‌افزار موردبررسی قرارگرفته است.

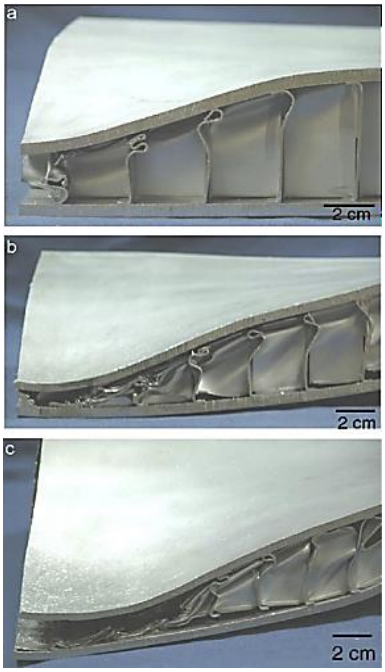


شکل ۳. پانل ساندویچی با هسته مربعی دارای شبکه عمودی

همان‌گونه که در شکل (۳) نشان داده شده است. پانل ساندویچی شامل یک هسته مربعی دارای شبکه عمودی که به دو صفحه بالایی و پایینی متصل است، تحت بار انفجار ناشی از انفجار خرج ۱،۲ و۳ کیلوگرمی قرارگرفته است. ابعاد بیرونی پانل ۶۱۰×۶۱۰×۶۱ میلی‌متر، ضخامت صفحه بالایی و پایینی ۵ میلی‌متر و ضخامت هسته مربعی ۰/۷۶ میلی‌متر است. پانل ساندویچی از جنس فولاد ضدزنگ با شکل‌پذیری بالا می‌باشد که آلیاژی از ۴۹٪ آهن، ۲۴٪ نیکل، ۲۱٪ کروم و ۶٪ مولیبدن است [۲۱]. خواص مکانیکی فولاد در جدول (۲) ارائه‌شده است [۲۱]. برای مدل‌سازی رفتار الاستیک- پلاستیک از مدل جانسون-کوک استفاده‌شده است که پارامترهای آن در جدول (۳) ارائه‌شده است. پروفیل‌های فشار- زمان و ایمپالس- زمان موج انفجار در هوا برای خرج‌های موجود در فاصله موردنظر بر اساس آیین‌نامه انفجاری آمریکا (یو-اف-سی) قابل‌تعیین است. در جدول (۱) مقادیر بیشینه فشار و ایمپالس برای خرج‌های موجود در فاصله موردنظر از آیین‌نامه تعیین و ارائه گردیده است. با فرض رفتار متقارن برای پانل ساندویچی مفروض، فقط یک‌چهارم آن در نرم‌افزار مدل شده است. منبع انفجار در نقطه‌ای به فاصله عمودی ۱۰۰ میلی‌متر از مرکز صفحه بالایی پانل ساندویچی قرارگرفته است. لبه‌های پانل ساندویچی گیردار و ثابت تعریف شدند. در شکل (۴) نحوه تغییر شکل یک‌چهارم پانل ساندویچی تحت بارگذاری‌های مختلف در آزمایشگاه نشان داده شده است.

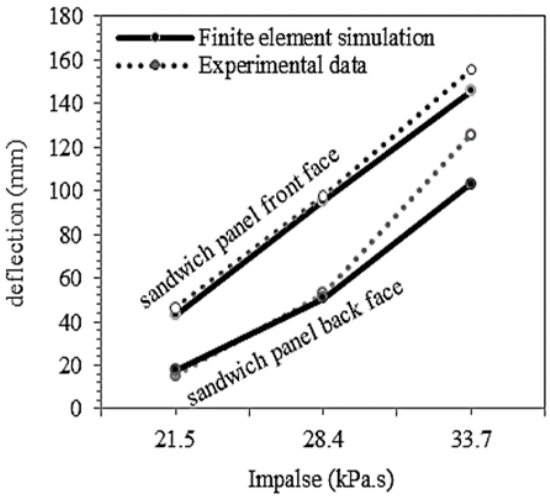
جدول ۱. بیشینه فشار و ایمپالس انعکاسی حل عددی

جرم خرج (کیلوگرم)	حداکثر فشار (مگاپاسکال)	ایمپالس (کیلوپاسکال‌ثانیه)
۱	۳۶۶	۲۱/۵
۲	۴۵۸	۲۸/۴
۳	۵۰۶	۳۳/۷



شکل ۴. فشرده شدن یک‌چهارم هسته لانه‌زنبوری مدل شده در آزمایشگاه برای خرج‌های یک، دو و سه کیلوگرم[۲۰]

در هرکدام از حالت‌های مدل‌سازی شده، جابجایی مرکز بعد از ۱/۵ میلی‌ثانیه با مقدار متناظر آن در نتایج آزمایش تجربی دهارماسنا[1] [۲۰] مقایسه شده است. مقایسه نتایج در شکل (۵) ارائه گردیده است. همان‌طور که مشاهده می‌شود تطابق مناسبی بین داده‌های تجربی و نتایج مدل‌سازی وجود دارد. علت تفاوت بین نتایج آزمایشگاهی و عددی در حالت ایمپالس ۳۳/۷ کیلو پاسکال ثانیه پایین آمدن دقت نتایج حل عددی در فواصل معادل کوچک است.



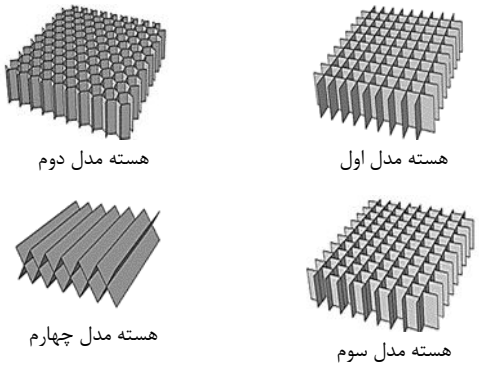
شکل ۵. مقایسه جابجایی مرکز رویه‌های پانل برای مدل‌سازی اجزاء محدود و داده‌های تجربی

[1] Dharmasena

۵. مدل‌سازی عددی

۵-۱. هندسه مدل

در این مقاله چهار مدل پانل ساندویچی با ابعاد کلی ۶۱۰ ×۶۱۰ ×۶۱ میلی‌متر در برابر موج انفجار مورد تحلیل و بررسی قرار گرفت. پوسته برای همه مدل‌ها یکسان و با ابعاد ۶۱۰ ×۶۱۰ میلی‌متر و ضخامت ۵ میلی‌متر در نظر گرفته شد. هسته‌ها نیز در ابعاد یکسان ۵۱ ×۶۱۰ ×۶۱۰ میلی‌متر، وزن برابر و چگالی نسبی یکسان تقریباً برابر ۶٪ ولی با هندسه متفاوت است. به خاطر تقارن سازه و شرایط بارگذاری، جهت ساده‌سازی فقط یک‌چهارم پانل مدل‌سازی و تحلیل‌شده است. مدل اول و دوم و سوم دارای هسته با شبکه عمودی، و مدل چهارم دارای هسته با شبکه افقی می‌باشند. شبکه‌های عمودی به‌علت این‌که مقاومت بیشتری در برابر فشار دارند، در صنعت کاربرد بیشتری دارند. متداول‌ترین شبکه‌ها در صنعت که دارای استحکام هندسی بالایی هستند، و همچنین قابلیت ساخت آسانی دارند، شبکه‌های با سلول‌های چهارضلعی و شش‌ضلعی می‌باشند. در اینجا هسته مدل اول و سوم دارای شبکه عمودی چهارضلعی، هسته مدل دوم دارای شبکه عمودی شش‌ضلعی و هسته مدل چهارم دارای شبکه افقی چهارضلعی است. در شکل (۶) هندسه هسته مدل‌ها آورده شده است.



شکل ۶. هسته‌های شبیه‌سازی‌شده پانل‌های ساندویچی

۵-۲. خواص مواد

پانل ساندویچی از جنس فولاد ضدزنگ با شکل‌پذیری بالا است. این فولاد آلیاژی از ۴۹٪ آهن، ۲۴٪ نیکل، ۲۱٪ کروم و ۶٪ مولیبدن است [۲۱]. در ناحیه الاستیک خواص پانل توسط مدول یانگ و ضریب پواسون و در ناحیه پلاستیک نیز توسط تنش و کرنش پلاستیک معرفی‌شده است. برای مدل‌سازی رفتار الاستیک- پلاستیک از مدل جانسون کوک استفاده‌شده است که تنش جاری شدن فولاد را با استفاده از معادله (۵) بیان می‌کند. خواص مکانیکی فولاد در جدول (۲) و پارامترهای مدل جانسون-کوک در جدول (۳) آورده شده است [۲۱].

$$\sigma_y = [A + B\varepsilon_p^{eqn}]\left[1 + cln\left(\frac{\dot{\varepsilon}_p^{eq}}{\dot{\varepsilon}_0}\right)\right]\left[1 - \left(\frac{T-T_r}{T_m-T_r}\right)^m\right] \quad (۵)$$

که ε_p^{eq} کرنش پلاستیک معادل، $\dot{\varepsilon}_p^{eq}$ نرخ کرنش پلاستیک معادل، $\dot{\varepsilon}_0$ نرخ کرنش اولیه، A و B ضرایب ثابت، T دمای ماده، T_m دمای ذوب ماده و T_r دمای محیط می‌باشد.

جدول ۲. خصوصیات فولاد [۲۱]

خصوصیات فولاد	مقادیر
مدول الاستیسیته	۱۶۱ (GPa)
ضریب پواسون	۰/۳۵
چگالی	۷۸۵۰ (kg/m^3)

جدول ۳. پارامترهای مدل جانسون- کوک

پارامترها	مقادیر
تنش تسلیم (A)	۴۰۰ (MPa)
ثابت سختی (B)	۱۵۰۰ (MPa)
ثابت نرخ کرنش (C)	۰/۰۴۵
توان سختی (n)	۰/۴
شاخص نرم شوندگی حرارتی (m)	۱/۲
کرنش (ε)	۰/۰۰۱ (s^{-1})
دمای محیط (T_r)	۲۹۳ (k)
دمای ذوب ماده (T_m)	۱۸۰۰ (k)

۵-۳. شرایط مرزی و بارگذاری

شرایط مرزی در پانل اصلی به‌صورت گیردار در نظر گرفته‌شده است؛ اما با توجه به اینکه یک‌چهارم پانل مدل‌سازی شده است، در اینجا دو سمت از پانل با شرایط مرزی متقارن تعریف‌شده است. موج انفجار به دو قسمت فاز مثبت و فاز منفی تقسیم می‌شود. در بخش فاز مثبت بیشینه اضافه فشار به‌صورت آنی تقریباً در زمان صفر شکل‌گرفته و طی زمان کوتاهی به مقدار فشار محیط کاهش پیدا می‌کند. بعدازآن موج وارد فاز منفی خود می‌شود که دارای زمان طولانی‌تر اما دامنه‌ای کمتر از اضافه فشار فاز مثبت است. رابطه بین فشار انفجار و زمان‌بر طبق معادله نمایی (۶) تعریف می‌شود.

$$\mathbf{p(t)} = \boldsymbol{P_s}(\mathbf{1} - \frac{\mathbf{t}}{\boldsymbol{T_a}})\mathbf{e}^{\frac{-\mathbf{b}}{\boldsymbol{T_a}}} \quad (۶)$$

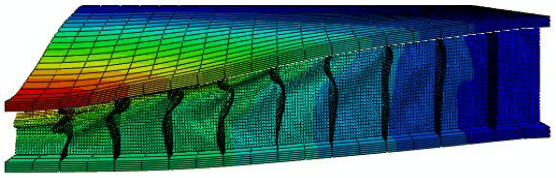
P(t) اضافه فشار در زمان t، T_a مدت زمان رسیدن موج به سازه، P_s بیشینه اضافه فشار و b یک ثابت تجربی است. از روش‌های مرسوم در حل مسائل موج شوک، اعمال مستقیم فشار موج انفجار به سازه لاگرانژی و یا کانوپ است. فشار اعمالی با توجه به معادلات تجربی تنظیم‌شده در قسمت بارگذاری انفجار محاسبه می‌شود که این معادلات با استفاده از جمع‌آوری نتایج هزاران آزمایش انفجار ماده منفجره به‌دست‌آمده‌اند. در این روش، ازآنجایی‌که نیازی به مدل هوا و ماده منفجره نیست، از المان‌های تماسی استفاده نمی‌شود و برای شبیه‌سازی موج انفجار، نیازمند ورودی‌های جرم معادل تی‌ان‌تی، نوع موج انفجار، مکان ماده منفجره در فضا و مشخصات سطح برای انتخاب نوع فشار اعمالی است. با اطلاعات کسب‌شده، کانوپ فشار مناسب را برای نوع سطح انتخاب‌شده، محاسبه می‌کند. این روش، ازنظر هزینه محاسباتی نسبت به روش لاگرانژی-اویلری انتخابی دارای هزینه کمتری است.

۵-۴. روش تحلیل، نوع المان‌ها و مش‌بندی

در این مقاله برای تحلیل دینامیکی اجزاء محدود از روش صریح استفاده‌شده است. این روش نسبت به روش انتگرال ضمنی برای بارگذاری‌های شدید در زمان کوتاه (مانند ضربه و انفجار) بهتر است و جواب‌های مناسب‌تری ارائه می‌دهد. برای مدل‌سازی ورق‌های پوسته از المان سه‌بعدی بیست گرهی و پانزده گرهی و برای هسته از المان‌های پوسته‌ای استفاده‌شده است. ورق‌های پوسته با ۵ لایه المان R8D3C در راستای ضخامت ورق، مش بندی شده است. این المان‌ها قابلیت این را دارند که تنش و کرنش را با دقت خیلی بالایی برآورد کنند. هسته نیز با ۳۰ لایه المان R4S در راستای ارتفاع هسته، مش بندی می‌گردد. اگرچه این المان‌ها امکان تغییر شکل محدودی دارند اما امکان دوران بالایی را دارا هستند. این عامل موجب می‌شود، المان‌های مزبور گزینه مناسبی برای تحلیل کمانشی هسته باشند.

۶. بررسی نتایج

برای ارزیابی اثر هسته‌های مختلف، در جذب انرژی موج انفجار چهار مدل هسته با ضخامت و شکل هندسی متفاوت اما با ابعاد، وزن و مواد یکسان در مقابل موج انفجار ناشی از سه نوع خرج یک، دو و سه کیلوگرمی مورد مقایسه قرار می‌گیرد. شکل (۷) مدل تغییر شکل یافته مدل ۱ را برای ایمپالس ۲۸/۴ kPa.s نشان می‌دهد.

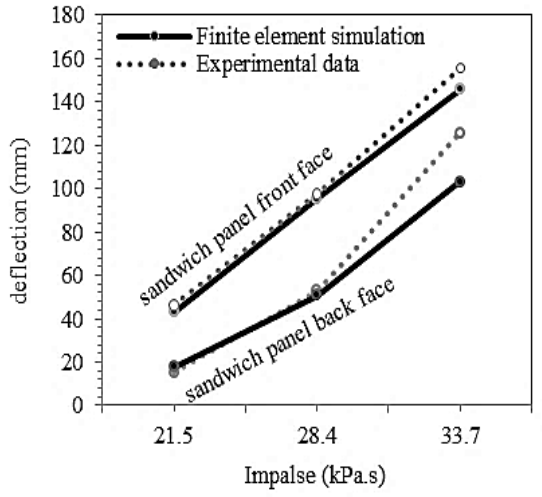


شکل ۷. فشرده شدن یک‌چهارم مدل ۱ برای خرج دو کیلوگرم تی‌ان‌تی

۶-۱. بررسی جابجایی ناشی از موج انفجار

همان‌طور که انتظار می‌رود به علت جذب انرژی توسط هسته، جابجایی پوسته مقابل خرج نسبت به پوسته دیگر باید بیشتر

باشد. همچنین مسلم است که جابجایی در فشارهای بالاتر، مقادیر بیشتری خواهد داشت. برای ارزیابی کارایی سازه‌های موردنظر، یک ورق فلزی با وزن معادل، در برابر موج انفجار مدل شده و از نتایج به‌دست‌آمده از آن برای مقایسه استفاده‌شده است. در جدول (۴) بیشینه جابجایی استخراج‌شده از مدل‌سازی برای مدل‌های مختلف ارائه گردیده است. جابجایی کمتر پوسته عقب پانل، نسبت به ورق فلزی معادل، جذب انرژی هسته و کارایی پانل ساندویچی در مقابل موج انفجار را مشخص می‌کند. شکل (۸) میزان بیشینه جابجایی پوسته عقب پانل ساندویچی و ورق فلزی را در حالت‌های مختلف نشان می‌دهد. محدوده فشارهای بررسی‌شده در این مقاله بین ۳۶۶ تا ۵۰۶ مگاپاسکال است. همان‌طور که مشاهده می‌شود درهرصورت پوسته عقب پانل ساندویچی به علت جذب انرژی هسته دارای جابجایی کمتری نسبت به ورق فلزی است بنابراین، می‌توان گفت اگر معیار طراحی میزان جابجایی بیشینه باشد، یک پانل ساندویچی درهرصورت عملکرد بهتری نسبت به ورق فلزی معادل خواهد داشت. جابجایی پوسته عقب پانل ساندویچی برای فشار بیشتر (۵۰۶ مگاپاسکال) حدود ۷۰-۹۰٪ ورق فلزی معادل و برای فشارهای ضعیف‌تر (۳۶۶ مگاپاسکال) حدود ۲۵-۵۰٪ ورق فلزی معادل است. پانل ساندویچی دارای قابلیت کارایی بهینه باید بر اساس میزان فشار وارده از موج انفجار طراحی شود. در فشار متوسط (۴۵۸ مگاپاسکال) همه پانل‌ها تقریباً دارای عملکرد مشابه می‌باشند. در فشارهای پایین‌تر موج انفجار (۳۶۶ مگاپاسکال) مدل ۴ که دارای هسته با هندسه غیر عمودی است، دارای کمترین میزان جابجایی بوده و بهترین عملکرد را دارد؛ اما این مدل در فشارهای بالا (۵۰۶ مگاپاسکال) دارای بدترین عملکرد یعنی بیشترین جابجایی نسبت به سایر مدل‌ها است. در این فشار مدل ۲ کمترین جابجایی و درنتیجه بهترین عملکرد را خواهد داشت.



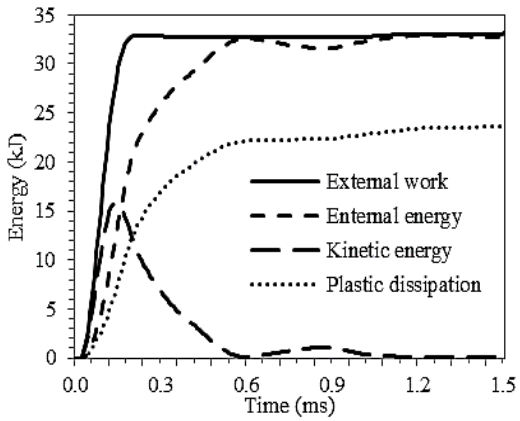
شکل ۸. بیشینه جابجایی مرکز رویه عقب پانل ساندویچی در برابر موج انفجار

جدول ۴. بیشینه جابجایی (برحسب میلی‌متر) مرکز پانل ساندویچی در مقابل موج انفجار

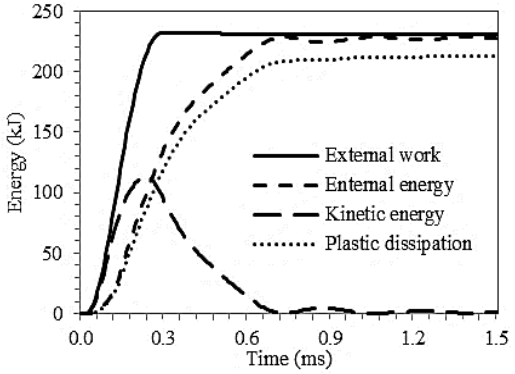
جابجایی	مدل۱		مدل۲		مدل۳		مدل۴		ورق فلزی
(میلی‌متر)	رویه جلو	رویه عقب	رویه جلو	رویه عقب	رویه جلو	رویه عقب	رویه جلو	رویه عقب	معادل
۱کیلوگرم تی‌ان‌تی	۴۳/۱	۱۷/۸	۳۶/۲۸	۱۷/۹۴	۴۴/۳۷	۱۶/۲۵	۵۶/۰۵	۹/۸۶	۳۷/۴۸
۲ کیلوگرم تی‌ان‌تی	۹۵/۵	۵۰/۸	۸۲/۲۶	۴۸/۸	۹۵/۱۲	۵۰/۲۷	۹۰/۰۸	۴۸/۵۹	۶۸/۳۶
۳ کیلوگرم تی‌ان‌تی	۱۴۵/۷	۱۰۳/۰۰۲	۱۴۳/۸	۹۷/۹	۱۴۶/۹	۱۰۳/۶۱	۱۵۶	۱۱۳/۵	۱۳۱/۱۱

۶-۲. بررسی جذب انرژی ناشی از موج انفجار

نمودار انرژی- زمان که برای خرج‌های ۱ و ۳ کیلوگرم برای مدل ۱ در شکل‌های (۹ و ۱۰) رسم شده است. در این شکل‌ها External work، Enternal work، Kinetic energy و Plastic dissipation به ترتیب بیانگر کار خارجی، کار داخلی، انرژی جنبشی و انرژی استهلاک شده ناشی از کرنش پلاستیک است. مقایسه بین کار انجام‌شده و انرژی استهلاک شده ناشی از کرنش پلاستیک، نشان می‌دهد که نسبت زیادی از کار انجام‌شده توسط موج انفجار، با کرنش‌های پلاستیک که در سازه به وجود می‌آید، مستهلک می‌شود. همچنین مشاهده می‌گردد که با افزایش جرم خرج و درنتیجه آن با افزایش میزان فشار، چون مواد به محدوده غیرخطی می‌رسند، این نسبت بیشتر می‌شود.

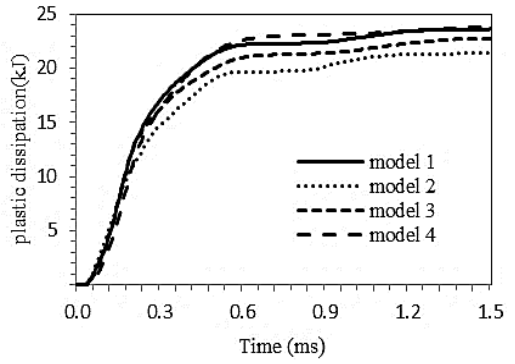


شکل ۹. مقایسه کل انرژی و انرژی استهلاک شده پلاستیک (مدل ۱، ۱ کیلوگرم تی‌ان‌تی)

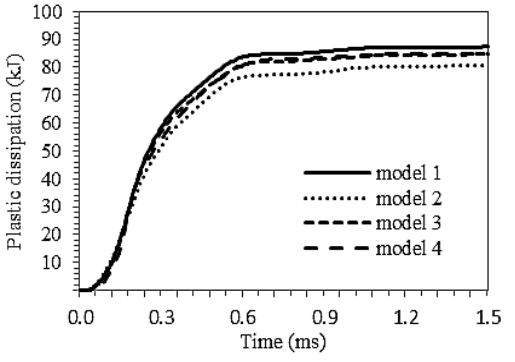


شکل ۱۰. مقایسه کل انرژی و انرژی استهلاک شده پلاستیک (مدل ۱، ۳ کیلوگرم تی‌ان‌تی)

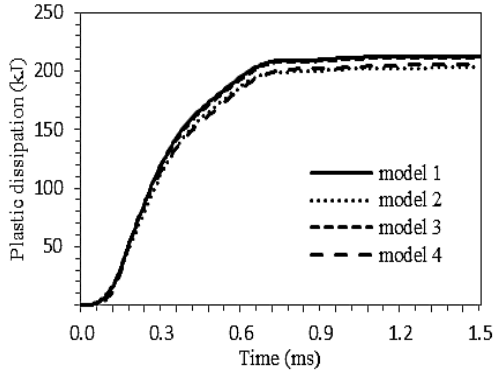
بیشتر فشار ناشی از موج انفجار توسط کرنش‌های پلاستیک ایجادشده در هسته مستهلک می‌شود. در هنگام انفجار مقدار کمی از انرژی جنبشی می‌تواند توسط خمش و کشش به وجود آمده در کل سازه جذب گردد. از سوی دیگر نسبت زیادی از انرژی جنبشی به‌وسیله تغییر شکل‌های پلاستیک جذب می‌شود [۲۰]؛ بنابراین، برای مقایسه جذب انرژی مدل‌های مختلف میزان انرژی مستهلک‌شده توسط کرنش‌های پلاستیک در آن‌ها با یکدیگر مقایسه شده است. شکل‌های (۱۲، ۱۱ و ۱۳) این انرژی را به ترتیب برای خرج‌های یک، دو و سه کیلوگرم تی‌ان‌تی در طول زمان نشان می‌دهند.



شکل ۱۱. مقایسه انرژی استهلاک شده پلاستیک (۱ کیلوگرم تی‌ان‌تی)



شکل ۱۲. مقایسه انرژی استهلاک شده پلاستیک (۲ کیلوگرم تی‌ان‌تی)



شکل ۱۳. مقایسه انرژی استهلاک شده پلاستیک (۳ کیلوگرم تی‌ان‌تی)

با توجه به شکل (۱۱) در فشارهای پایین (۳۶۶ مگاپاسکال) مدل ۴ با هسته دارای شبکه افقی با جذب انرژی ۲۳/۷۵۵ کیلوژول دارای بیشترین جذب انرژی و بهترین عملکرد خواهد بود. در فشارهای بالاتر (۵۰۶-۴۵۸ مگاپاسکال) با توجه به شکل‌های (۱۲ و ۱۳) مدل ۱ دارای هسته با شبکه عمودی با جذب انرژی ۸۷/۳۳ و ۲۱۲/۷۷ کیلوژول به ترتیب برای خرج‌های ۲ و ۳ کیلوگرم بیشترین جذب انرژی و بهترین عملکرد را خواهد داشت.

۷. نتیجه‌گیری

در این مقاله میزان جابجایی و جذب انرژی ناشی از موج انفجار توسط چند مدل پانل ساندویچی با هسته‌های متفاوت با روش عددی مورد بررسی قرار گرفت. داده‌های به‌دست‌آمده از روش عددی اجزاء محدود، با مقادیر آزمایشگاهی متناظر مقایسه شد و تطابق خوبی بین داده‌های تجربی و عددی مشاهده گردید. با بررسی دو پارامتر متغیر فشار موج انفجار (ناشی از تفاوت در وزن خرج) و هندسه هسته‌های پانل ساندویچی روشی جهت بررسی عملکرد سازه ساندویچی ارائه شد. نتایج نشان داد که پانل‌های ساندویچی نسبت به ورق فلزی معادل آن، نقش بسیار مؤثرتری جهت مقاومت در برابر موج انفجار دارند. از طرفی برای هر مقدار فشار انفجار و برای هر کاربرد مشخص، یک پانل ساندویچی خاصی می‌تواند بهترین عملکرد را داشته باشد؛ که این عملکرد متأثر از هندسه هسته پانل ساندویچی است. معیارهای موردبررسی جهت برآورد کارایی سازه در مقابل فشار ناشی از موج انفجار، جابجایی مرکز پانل و میزان جذب انرژی پانل در نظر گرفته شد. برای چهار نمونه پانل مدل‌سازی شده نتایج نشان داد که در محدوده فشارهای موردبررسی، در فشارهای پایین‌تر مدل ۴ که دارای هسته با شبکه چهارضلعی افقی بود، با توجه به اینکه وب افقی نسبت به وب‌های عمودی زودتر مچاله شده بیشترین جذب انرژی را داشت و در نتیجه کمترین جابجایی را داشت.

بنابراین، در فشارهای پایین هندسه با شبکه افقی نسبت به شبکه‌های عمودی می‌تواند مناسب‌تر باشد. ولی در فشارهای بیشتر هسته با وب عمودی به‌علت مقاومت بالاتر کارایی بیشتری خواهد داشت. در این فشارها اگر معیار طراحی حداقل جابجایی باشد مدل ۲ با شبکه عمودی شش‌ضلعی بهترین مدل بوده و اگر معیار طراحی میزان جذب انرژی باشد مدل ۱ دارای شبکه عمودی چهارضلعی بیشترین میزان جذب انرژی را دارد و بهترین مدل جهت طراحی موردنظر خواهد بود.

۸. مرجع‌ها

[1] Heimbs, S. “Foldcore Sandwich Structures and their impact Behaviour: an Overview”; Dynamic failure of composite and sandwich structures. Springer, Dordrecht, 2013.

[2] Gilkie, R.; Sundararaj, P. “The Impact Resistance of Plastics Sandwich Constructions using Low Density Urethane Foam Cores”; J. Cell. Plast. 1971, 7, 313-318.

[3] Nayak, S. K.; “Optimization of Honeycomb Core Sandwich Panel to Mitigate the Effects of Air Blast Loading”; MS. Thesis, The Pennsylvania State University, 2010.

[4] Nurick, G.; Martin, J. “Deformation of Thin Plates Subjected to impulsive Loading—a Review Part II: experimental Studies”; Int. J. Impact. Eng. 1989, 8, 171-186.

[5] Nurick, G.; Martin, J. “Deformation of Thin Plates Subjected to Impulsive Loading—a Review: Part i: Theoretical Considerations”; Int. J. Impact. Eng. 1989, 8, 159-170.

[6] Rajendran, R.; Lee, J. “Blast Loaded Plates”; Mar. Struct. 2009, 22, 99-127.

[7] Jacob, N.; Yuen, S. C .K.; Nurick, G.; Bonorchis, D.; Desai, S.; Tait, D.“Scaling Aspects of Quadrangular Plates Subjected to Localised Blast Loads—Experiments and Predictions”; Int. J. Impact. Eng. 2004, 30, 1179-1208.

[8] Xue, Z.; Hutchinson, J. W. “Preliminary Assessment of Sandwich Plates Subject to Blast Loads”; Int. J. Mech. Sci. 2003, 45, 687-705.

[9] Mori, L.;Queheillalt, D.;Wadley, H.;Espinosa, H. “Deformation and Failure Modes of I-core Sandwich Structures Subjected to Underwater Impulsive Loads”; Exp. Mech. 2009, 49, 257-275.

[10] Valdevit, L.; Wei, Z.; Mercer, C.; Zok, F. W.; Evans, A. G.; “Structural Performance of Near-Optimal Sandwich Panels with Corrugated Cores”; Int. J. Solids. Struct. 2006, 43, 4888-4905.

[11] Jing, L.;Yang, F.;Wang, Z.;Zhao, L.“A Numerical Simulation of Metallic Cylindrical Sandwich Shells Subjected to Air Blast Loading”; Lat. Am. J. Solids Stru. 2013, 10, 631-645.

[12] Vatani Oskouei, A.;Kiakojouri, F.“Non-linear Dynamic Analysis of Steel Hollow I-Core Sandwich Panel under Air Blast Loading”; Civil. Eng. Civil. Infr. 2015, 48, 323-344.

[13] Peyman, S.;Ghazanfarinia, S.“Defence and Secutity Structures”; MAUT Press, 2007.

[14] Sayed M. Soleimani, Nader H. Ghareeb, Nourhan H. Shaker, Modeling, Simulation and Optimization of Steel Sandwich Panels under Blast Loading, American Journal of Engineering and Applied Sciences, 2018.

[15] Sabzevari, S.; Shahabian, F. “Optimum Selection of Corrugated Sandwich Panels Shape and Materials Subjected to Blast Loading”.

[16] Peyman, S.;Sonbolestan, S.H.“Analysis of Underground Tunnels in Explosion Loading Based on Peak Particle Velocity”; Advanced Defence Sci. & Technol. 2017, 8, 45-50.

[17] Bulson, P. S. “Explosive Loading of Engineering Structures”; CRC Press: 2002.

[18] Brode, H. L. “Numerical Solutions of Spherical Blast Waves”; J. Appl. Phys. 1995, 26, 766-775.

[19] Henrych, J.; Major, R. “The Dynamics of Explosion and its Use”; Elsevier/North-Holland, Inc., New York, 1979.

[20] Dharmasena, K. P.; Wadley, H. N.; Xue, Z.; Hutchinson, J. W. “Mechanical Response of Metallic Honeycomb Sandwich Panel Structures to High-Intensity Dynamic Loading”; Int. J. Impact. Eng. 2008, 35, 1063-1074.

[21] Nahshon, K.; Pontin, M.; Evans, A.; Hutchinson, J.; Zok, F.; “Dynamic Shear Rupture of Steel Plates”; J. Mech. Mater. Struct. 2007, 2, 2049-2066 .

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۳۶۷-۳۵۷

«علمی- پژوهش»

بررسی رفتار میراگر اصطکاکی در مهاربندهای ضربدری در برابر نیروی انفجار

سلیمان قوهستانی[۱*]، محمد کارکن[۲]، مجید یعقوبی[۳]، صفر خلیفه[۴]

۱- استادیار گروه عمران، دانشکده مهندسی، دانشگاه فسا، فسا، ایران، ۲- استادیار گروه عمران، دانشکده مهندسی، دانشگاه آزاد اسلامی، واحد لارستان، لارستان، ایران ۳- استادیار گروه عمران، دانشکده مهندسی، دانشگاه تربت حیدریه، تربت حیدریه، ایران ۴- دانشجوی کارشناسی ارشد، گروه عمران، دانشکده مهندسی، موسسه آموزش عالی تابناک لامرد، لامرد، ایران

(دریافت: ۹۸/۰۵/۲۰، پذیرش: ۹۹/۰۳/۲۲)

چکیده

خطرات متعدد اغلب بر روی پایداری سازه‌ها اثر می‌گذارد و هنگام طراحی و آنالیز سازه باید این نکته در نظر گرفته شود. با افـزایش مقاومـت لرزه‌ای سازه، مقاومت سازه در مقابل نیروهای دیگر نظیر نیروی انفجار نیز افزایش پیدا می‌کند. یکی از سامانه‌های متداول طراحی ساختمان‌ها در برابر بارهای جانبی استفاده از سامانه مهاربند ضربدری می‌باشد. استفاده از مهاربنـدهای ضـربدری فـولادی مجهـز بـه میراگـر اصـطکاکی می‌تواند میراگری و جذب انرژی بیشتری در مقایسه با مهاربندهای ضربدری فولادی فاقد میراگر داشـته باشـد و در انفجارهـای بـزرگ رفتـار بهتری از خود نشان دهد. در این مقاله تأثیر مهاربندهای ضربدری دارای میراگر اصطکاکی و فاقد میراگر اصطکاکی در عملکرد سازه بتنـی در برابر نیروی انفجار مطالعه شده است. به این منظور جابه‌جایی و تغییرمکان نسبی طبقات در حالـت‌هـای مختلـف بارگـذاری انفجـار محاسـبه گردیده است. درنهایت نتایج نشان‌دهنده تأثیر میراگر اصطکاکی در کاهش تغییرمکان جانبی و تغییرمکان نسبی طبقات می‌باشد؛ به‌طوری‌کـه در سازه با میراگر در مقایسه با سازه بدون میراگر، تغییرمکان جانبی و تغییرمکان نسبی طبقات به‌طور چشم‌گیری کاهش یافته است. مطالعات نشان می‌دهد اضافه کردن میراگر اصطکاکی به سازه باعث افزایش سختی سازه می‌شود، بنابراین، زمان تناوب سازه کاهش می‌یابد.

کلیدواژه‌ها: بار انفجار، مهاربند ضربدری، میراگر اصطکاکی، Opensees

Investigation of Friction Damper Behavior in Cross Braces Subjected to Blast Load

S. Ghouhestani[*], M. Karkon, M. Yaghoobi, S. Kalife
[*]Department of Civil Engineering, Faculty of Engineering, Fasa University, Fasa, Iran.

(Received: 11/08/2019; Accepted: 11/06/2020)

Abstract

Several hazards often affect the stability of structures, and when designing and analyzing the structure, this should be considered. With increasing seismic strength of the structure, the strength of the structure increases against other forces, such as the explosion force. One of the most commonly used building design systems for lateral loads is the use of a cross bracing system. Using cross braces with friction damper can have more damping and energy absorption compared to cross braces without friction damper; it will behave better in big bangs. In this paper, the effect of cross braces with a friction damper and no friction damper on the performance of concrete structures against explosive force has been studied. For this purpose, the displacement and relative displacement of the floors in different modes of loading of the explosion have been calculated. Finally, the results show the effect of friction damper on reducing lateral displacement and relative displacement of the floors, so that in the structure with the damper compared with the structure without a damper, the lateral displacement and relative displacement of the floors significantly decreased. Studies show that adding a friction damper to the structure increases the stiffness of the structure, so the frequency of the structure is reduced.

Keywords: Blast Load, Cross Brace, Friction damper, Opensees

[*]Corresponding Author E-mail: ghouhestani@fasau.ac.ir

۱. مقدمه

بر اساس آمارهای منتشرشده از سوی سازمان‌های بین‌المللی، کشور ایران در یکی از پرمخاطره‌ترین نقاط دنیا ازنظر بروز جنگ و حملات تروریستی قرار گرفته است [۱]. این مسئله به‌خودی‌خود اهمیت پرداختن به مبحث پدافند غیرعامل در همه زمینه‌ها و به‌طور ویژه در طراحی سازه‌های مهم را انکارناپذیر جلوه می‌دهد. لذا مسلم است که بررسی پارامترهای مهم در این زمینه ضروری باشد. همچنین لازم است تا تلاش‌های جدیدی برای نگارش آیین‌نامه‌هایی در این زمینه صورت پذیرد. آیین‌نامه‌هایی که به‌راحتی در دسترس مهندسین و متخصصین باشد و به‌وسیله آن بتوان امنیت سازه‌های مهم را تأمین نمود. اولین دستورالعمل توسط بخش نیروی زمینی ارتش آمریکا در سال ۱۹۸۶ برای سازه‌های مقاوم در برابر انفجار تهیه شده است [۲]. پس از آن در سال ۱۹۹۰ با همکاری مشترک بخش‌های نیروی زمینی، نیروی هوایی و نیروی دریایی ارتش آمریکا دستورالعمل TM5-1300 [۳] تهیه شد و به‌طور وسیعی در طراحی سازه‌ها در برابر انفجار استفاده گردید. پس از آن در سال ۲۰۰۸ دستورالعمل UFC3-340-02 [۴] که نسخه به‌روز شده دستورالعمل TM5-1300 است؛ توسط بخش دفاع آمریکا تهیه شد و اکنون مبنای اصلی طراحی و تحقیق در این حوزه است. با توجه به خطرات روزافزون و خسارت‌های سنگین وقایع تروریستی و جنگ، شناخت پدیده انفجار و راه‌های پایداری سازه‌ها در برابر انفجار از ضروریات امروز جهان است.

معمولاً طراحی ساختمان در برابر نیروهای جانبی از قبیل انفجار و زلزله‌های قوی بر این اساس استوار است که سازه بتواند با شکل‌پذیری خود انرژی را جذب و مستهلک نماید. خطرات متعدد اغلب بر روی پایداری و عمر مفید سازه اثر می‌گذارند و هنگام طراحی و آنالیز سازه باید این نکات در نظر گرفته شود. فرض اساسی کاهش خطرات این است که سازه در مقابل یک خطر طراحی می‌شود و در برابر دیگر خطرات احتمالی مقاومت کافی دارد. یکی از سامانه‌های متداول طراحی ساختمان در کشور استفاده از قاب خمشی بتن مسلح می‌باشد. این سامانه به‌دلیل در دسترس بودن مصالح موردنیاز و نیز اجرای ساده به یکی از سامانه‌های متداول در ایران تبدیل شده است. چون ارزیابی لرزه‌ای قاب‌های خمشی نشان داده است که به‌دلیل عدم رعایت ضوابط بارگذاری لرزه‌ای و نیز تغییرات ایجاد شده در آیین‌نامه‌ها، ساختمان‌های طرح‌شده موجود در برابر انفجار و حتی بارهای لرزه‌ای اصلاح‌شده مقاوم نمی‌باشند؛ استفاده از مهاربندهای ضربدری با میراگرهای اصطکاکی در این نوع قاب‌های خمشی تأثیرهای مثبت و زیادی در کاهش پاسخ‌ها دارند.

میراگرهای اصطکاکی برای اولین بار توسط دو کانادایی به نام‌های پال و مارش در سال ۱۹۸۲ معرفی گردید. در این نوع، میراگرها در محل تلاقی مهاربندها در یک قاب خمشی نصب می‌شوند که تاکنون در ساختمان‌های زیادی در دنیا مورد استفاده قرار گرفته است [۵].

بیکر و همکارانش [۶] در سال ۱۹۸۳ بارهای ناشی از انفجارهای داخلی را مورد مطالعه و بررسی قرار دادند. بررسی آن‌ها نشان داد که در یک سازه نیمه محبوس دو نوع بار انفجاری ایجاد می‌شود که نوع اول فشار بازتاب و نوع دوم فشار گاز می‌باشد که هر دو نوع برای خروج نیاز به بازشو دارد. در سال ۱۹۸۸ رزکی [۷] به بررسی ساختمان کنترل در کارخانه‌های صنعتی تحت اثر فشار ناشی از انفجار پرداخته است. وی الزامات بارگذاری، ملاحظات ایمنی، فلسفه طراحی، انتخاب مفاهیم سازه‌ای انفجار و رفتار مواد در حالت بارگذاری دینامیکی را مورد بررسی قرار داد. یان و همکارانش [۸] در سال ۱۹۹۳ میرایی بهینه میراگرهای اصطکاکی را برای یک سازه محاسبه کرد. مولا و بیلیو [۹] در سال ۲۰۰۲ به بررسی قاب فولادی یک طبقه دارای سامانه مهاربند جانبی فلزی پیش‌تنیده مجهز به میراگر اصطکاکی پرداختند. آن‌ها اثر نیروی پیش‌تنیدگی را بر روی رفتار میراگر اصطکاکی مورد بررسی قرار دادند. نتایج بررسی آن‌ها نشان داد که میزان نیروی پیش‌تنیدگی مهاربند در تغییر پاسخ سازه نقشی ندارد و پیش‌تنیدگی باعث اقتصادی شدن مقطع مهاربند و جلوگیری از کمانش آن می‌گردد؛ به‌نحوی‌که حداکثر تفاوت بین پاسخ دو سازه یکی با مهاربند دارای ۱۰۰ درصد نیروی پیش‌تنیدگی و دیگری با مهاربند دارای ۲۰ درصد نیروی پیش‌تنیدگی بیش از ۴ درصد نیست. یوامین و چری در سال ۲۰۰۰ مقالاتی در زمینه طراحی سازه‌های با میراگر تحت اثر بار جانبی ارائه کردند. وی و همکارانش [۱۰] در ادامه تحقیقات قبلی با انجام آزمایش‌هایی، به بررسی تأثیر پارامترهایی مانند دامنه جابه‌جایی، تعداد دفعات بارگذاری، مقدار نیروی پیش‌تنیدگی مهاربندها بر روی قاب فلزی دارای مهاربند فلزی مجهز به میراگر اصطکاکی پرداخته‌اند. بینگ و همکارانش [۱۱] مدل‌سازی یک قاب از ساختمان شش طبقه بتنی را با استفاده از نرم‌افزار ABAQUS انجام داده‌اند. آن‌ها به بررسی اثر وجود یا عدم وجود میان قاب‌ها بر روی رفتار قاب تحت اثر بار انفجار پرداختند. نتایج مطالعه آن‌ها نشان می‌دهد که اثر بار انفجار بر قاب‌های دارای میان قاب بسیار بزرگ‌تر است و سازه برای مستهلک کردن انرژی ناشی از انفجار، تغییرشکل‌های بزرگ‌تر و خسارت بیشتری را تجربه خواهد کرد. در این مطالعه تغییرمکان نسبی طبقه به‌عنوان یک معیار کلی ملاک ارزیابی قرار گرفته است.

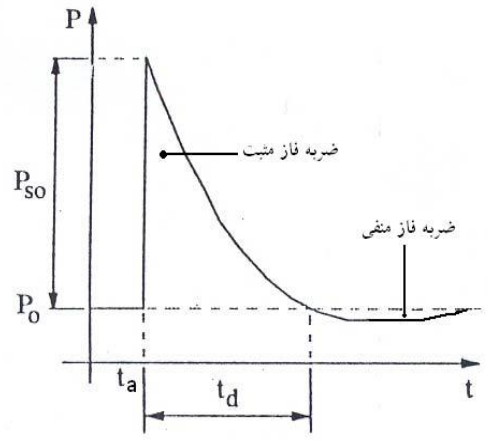
یاسر و همکارانش [۱۲] به بررسی رفتار قاب بتن مسلح تحت

اثر بار انفجار پرداخته‌اند. در این تحقیق تحلیل اجزای محدود با استفاده از نرم‌افزار ABAQUS برای ارزیابی عملکرد قاب بتن مسلح انجام شده است. به این منظور یک مدل دو بعدی از قاب بتنی چهار طبقه انتخاب شد. پاسخ مدل ایجادشده تحت بارهای انفجاری شبیه‌سازی‌شده نشان داد که با تغییر ستون‌های خارجی، به ویژه با استفاده از لوله‌های فولادی پرشده از بتن، عملکرد سازه بهبود می‌یابد. در پژوهشی دیگر زبیر و همکارانش [۱۳] نیز به بررسی عملکرد قاب‌های بتنی تحت اثر بار انفجار پرداخته‌اند. آن‌ها اقدام به مدل‌سازی سه‌بعدی سازه و طراحی آن بر اساس آیین‌نامه IBC و ACI318-11 با شرایط منطقه ابوظبی کردند. سپس این سازه در شرایط مختلف فاصله مقیاس شده و وزن ماده منفجره تحلیل شد. تحلیل‌ها منجر به تعیین فاصله ایمن در برابر انفجار در این نوع سازه‌ها گردید. آن‌ها تأثیر تغییر پارامترهایی از قبیل خصوصیات مواد و همچنین نوع پیکره‌بندی سازه در نحوه عملکرد آن در برابر بار انفجار را نیز مورد بررسی قرار داده‌اند. یانگ و همکارانش [۱۴] به تحلیل احتمالاتی خرابی پیش‌رونده در سازه‌های فولادی تحت اثر بار انفجار پرداخته‌اند. آن‌ها یک روش دو مرحله‌ای برای ارزیابی پتانسیل واژگونی سازه‌ها در برابر بار انفجار ارائه کردند. در مرحله اول، درجه تخریب و واکنش‌های اعضای سازه‌ای تحت اثر بار انفجار بر اساس سامانه معادل یک درجه آزادی تعیین می‌شوند. در مرحله دوم، رفتار خرابی سازه فولادی پس از انفجار با استفاده از یک مدل عددی غیرخطی سه‌بعدی ماکروسکوپی مورد بررسی قرار گرفته است. نتایج نشان می‌دهد که چارچوب ارزیابی قابلیت اطمینان مورداستفاده در این مطالعه، یک پیش‌بینی دقیق از خطر خرابی سازه‌ها در برابر بار انفجار ارائه می‌کند که در مقایسه با روش شبیه‌سازی مستقیم مونت‌کارلو دقیق‌تر است.

در سال‌های اخیر در کشور ما نیز پژوهش‌هایی در زمینه انفجار صورت گرفته است. از جمله این تحقیقات تدوین پیش‌نویس مبحث ۲۱ مقررات ملی ساختمان (پدافند غیرعامل) می‌باشد [۱۵]. این آیین‌نامه شامل ضوابط مربوط به بارگذاری انفجار و نیز طراحی ساختمان‌ها در برابر این بارگذاری است. نوری‌زاده و همکارانش [۱۶] عملکرد قاب بتنی مسلح طراحی‌شده بر اساس آیین‌نامه زلزله ایران [۱۷] را در برابر بارگذاری انفجار بررسی کرده‌اند. آن‌ها بارگذاری انفجاری را بر اساس پیش‌نویس مبحث بیست و یکم مقررات ملی ساختمان بر قاب مورد مطالعه اعمال و با لحاظ نمودن آثار غیرخطی مصالح و هندسه، تحلیل را انجام داده‌اند. شیراوند و همکارانش [۱۸] به بررسی رفتار سازه‌های فولادی با قاب خمشی ویژه و قاب مهاربندی تحت اثر بار انفجار پرداخته‌اند. آن‌ها با مطالعه عددی بر روی مدل‌های سازه‌ای سه‌بعدی با تعداد طبقات ۳، ۵ و ۱۰ نشان دادند که سامانه مهاربند برون‌محور نسبت به سایر سامانه‌ها عملکرد بهتری در برابر بارهای ناشی از انفجار دارد. کامکار و شمس [۱۹] به بررسی تأثیر بار انفجار بر پاسخ دینامیکی غیرخطی هسته فولادی مهاربندهای کمانش ناپذیر پرداخته‌اند. آن‌ها با استفاده از نرم‌افزار ABAQUS، پاسخ غیرخطی هسته مهاربند کمانش ناپذیر تحت بارگذاری‌های انفجاری با مدت زمان فاز مثبت متفاوت را بررسی کرده‌اند. نتایج نشان می‌دهد که افزایش مدت زمان فاز مثبت سبب افزایش مقادیر بیشینه تنش فشاری، میزان جذب انرژی در ناحیه فشاری و مقدار جابجایی پلاستیک و کاهش مقدار ماکزیمم تنش کششی در هسته مهاربند کمانش ناپذیر می‌شود.

۲. مروری بر مفاهیم انفجار

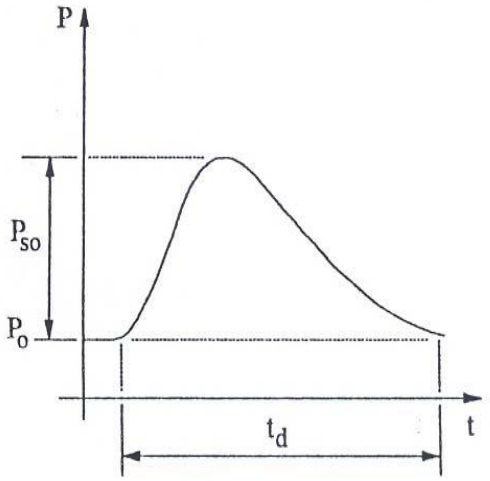
انفجار واکنش شیمیایی مواد منفجره است که انرژی قابل ملاحظه‌ای را آزاد می‌نماید. در اثر فشار و دمای بسیار زیاد، مواد منفجره به گاز تبدیل شده و با ازدیاد بسیار سریع فشار هوا، موج انفجار به وجود می‌آید که با سرعت اولیه حدود ۲۰۰۰ تا ۱۰/۰۰۰ متر بر ثانیه، منتشر می‌شود. امواج انفجار بر حسب منشأ آن به دو نوع موج ضربه و موج فشار تقسیم می‌شوند. موج ضربه، ناشی از انفجار، در حوزه نزدیک مواد منفجره جامد است. مطابق شکل (۱) در هر نقطه از مسیر انتشار موج، در وهله اول، فشار محیط به فشار مبنای انفجار افزایش یافته و با گذشت زمان به فشار محیط کاهش می‌یابد که به آن فاز مثبت می‌گویند. با عبور موج، کاهش فشار یا مکش رخ می‌دهد که به آن فاز منفی می‌گویند. فشار گام منفی، نسبتاً کوچک و تدریجی بوده و در اکثر مواقع، از اثر آن صرف‌نظر می‌شود [۲۰ و ۲۱ و ۲۲ و ۲۳].



شکل ۱. موج ضربه.

نوع دیگر موج انفجار، موج فشار می‌باشد. موج فشار، از انفجار حوزه نزدیک مواد منفجره گازی و مایع و حوزه دور مواد منفجره جامد ایجاد می‌شود. مطابق شکل (۲) در هر نقطه از مسیر انتشار

آن میزان فشار محیط به‌صورت تدریجی تا فشار مبنای انفجار افزایش یافته و سپس به فشار محیط کاهش می‌یابد و معمولاً گام منفی ندارد.



شکل ۲. موج فشار.

۲-۱. پیش‌بینی فشار ناشی از موج انفجار

قدرت یک بارگذاری انفجار، همواره توسط دو عامل وزن ماده منفجره و فاصله از منبع انفجار که به‌صورت پارامتر فاصله مقیاس شده (Z) است؛ طبق رابطه زیر محاسبه می‌گردد.

$$Z = \frac{R}{W^{\frac{1}{3}}} \qquad (۱)$$

که W = وزن ماده منفجره بر حسب کیلوگرم، معادل‌سازی شده وزن بر حسب وزن TNT.

R = فاصله سازه موردنظر از منبع انفجار بر حسب متر.

آیین‌نامه مقررات ملی ساختمان مبحث ۲۱ برای تعیین حداکثر فشار برخورد ناشی از انفجار در هوای آزاد برای فواصل میانی و دور، روابط براد و برای فواصل نزدیک به حوزه، روابط هنریش که مطابقت خوبی با نتایج آزمایشگاهی دارند را پیشنهاد کرده است.

-روابط براد

$$P_{so} = (6.7)/z\text{^}3 + 1 \qquad (۲)$$

$$(P_{so} > 10 \ \ kg/cm^2)$$

$$P_{so} = (0.975)/z + (1.455)/z\text{^}2 + (5.85)/z\text{^}3 - 0.019 \qquad (۳)$$

$$(0.1 < P_{s0} < 10 \ \ kg/cm^2)$$

- روابط هنریش

(z فاصله مقیاس شده بر حسب $m/kg^{1/3}$)

$$P_{so} = (14.072)/z + (5.54)/z\text{^}2 + (0.357)/z\text{^}3 + (0.00625)/z\text{^}4 \quad (0.05 \le z < 0.3) \qquad (۴)$$

$$P_{so} = (6.194)/z + (0.326)/z\text{^}2 + (20.32)/z\text{^}3 \quad (0.3 \le z < 3) \qquad (۵)$$

$$P_{so} = (0.662)/z + (4.05)/z\text{^}2 + (3.288)/z\text{^}3 \quad (3 \le z \le 10) \qquad (۶)$$

طبق آیین‌نامه مقررات ملی ساختمان مبحث ۲۱ مدت زمان فاز مثبت انفجار بر اساس فاصله مقیاس شده بر حسب ثانیه مطابق رابطه زیر پیشنهاد شده است.

$$\log\left(\frac{t_d}{W^{\frac{1}{3}}}\right) = 2.5\log_{10}\left(\frac{R}{W^{\frac{1}{3}}}\right) + 0.28 \quad (z \le 1) \qquad (۷)$$

$$\log\left(\frac{t_d}{W^{\frac{1}{3}}}\right) = 0.31\log_{10}\left(\frac{R}{W^{\frac{1}{3}}}\right) + 0.28 \quad (z \ge 1) \qquad (۸)$$

۲-۲. پارامترهای مهم موج انفجار در هوا

الف- سرعت جبهه‌ی موج انفجار (U_s)

سرعت انتشار جبهه‌ی موج انفجار (موج فشار و موج ضربه) در هر نقطه، از رابطه زیر محاسبه می‌شود.

$$U_s = 340 \times (1 + 0.83\ P_{so})^{0.5} \qquad (۹)$$

که در این رابطه U_s، سرعت انتشار موج بر حسب متر بر ثانیه و P_{so} فشار مبنای انفجار بر حسب کیلوگرم بر سانتیمتر مربع است.

ب- مدت زمان گام مثبت (زمان اقدام انفجار -t_d)

مطابق شکل (۱) مدت زمان گام مثبت(t_d) زمانی است که فشار، بیش از فشار محیطی(P_o) است و مقدار آن برای سطوح بارگذاری مختلف محاسبه شده است.

پ- تکانه ویژه انفجار(i_s)

همان‌طور که در شکل (۳) نشان داده شده است سطح زیر منحنی فشار- زمان را تکانه ویژه انفجار برای هر نقطه محدوده انفجار گویند که به دو جزء مثبت و منفی تقسیم می‌گردد. تکانه مثبت از رابطه زیر به‌دست می‌آید.

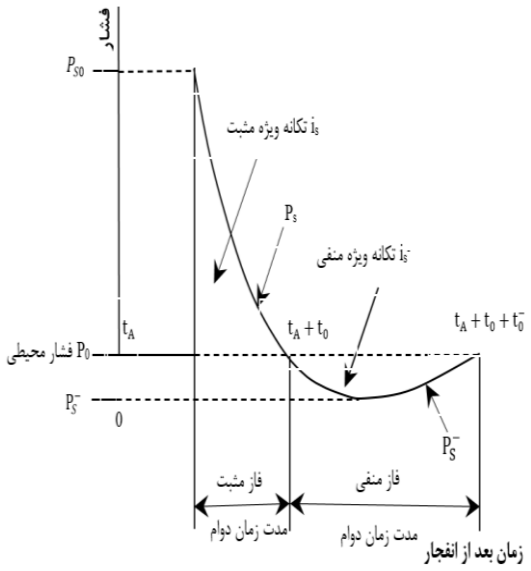
برای موج ضربه

$$i_s = 0.5 \times P_{so} \times t_d \qquad (۱۰)$$

برای موج فشار

$$i_s = 0.64 \times P_{so} \times t_d \qquad (۱۱)$$

به‌دلیل کوچک بودن مقدار تکانه منفی، از آن صرف‌نظر شده است.



شکل ۳. تاریخچه زمانی فشار ناشی از انفجار [۲۴].

ت- طول موج (λ_{rw})

فاصله هر نقطه تحت فشار مبنا واقع در سطح جبهه انفجار تا اولین نقطه تحت فشار محیطی واقع در پشت جبهه انفجار، «طول موج» نامیده می‌شود. مقدار طول موج بر حسب متر، از رابطه زیر به‌دست می‌آید.

$$(\lambda_{rw}) = U_s \times t_d \qquad (۱۲)$$

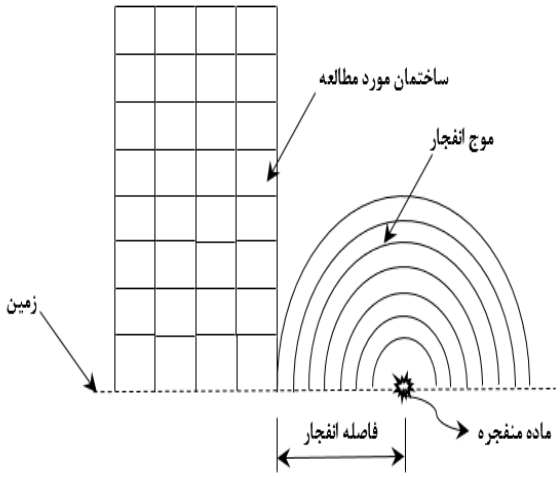
که در آن، $U_s(m/s)$ و $t_d(sec)$ به ترتیب سرعت انتشار موج و مدت زمان گام مثبت در انفجار است.

۲-۳. انواع حالت انفجار

اثر امواج ناشی از انفجار بر سازه در سه حالت قابل بررسی است. در حالت اول امواج ناشی از انفجار به وجهی از ساختمان که دارای نزدیک‌ترین فاصله به محل وقوع انفجار است برخورد می‌کند. که با توجه به‌شدت انفجار باعث آسیب و یا تخریب اجزای ساختمان می‌گردد. در حالت دوم با نفوذ موج از بازشوهای ساختمان، فشار بر روی پوشش‌های کف و سقف طبقات وارد می‌شود. این فشار باعث تغییر طول اعضای سازه‌ای و آسیب به پوشش کف و سقف ساختمان می‌گردد. در انتها، موج انفجار در حالت سوم تمام سازه را احاطه کرده و باعث ایجاد فشار بر روی پشت‌بام، دیوارهای پیرامونی و دیوارهای دورتر نسبت به محل وقوع انفجار می‌گردد. در این پژوهش با توجه به اثرات قابل‌ملاحظه حالت اول ناشی از انفجار بر روی سازه‌ها، به بررسی اثر حالت اول بر سازه پرداخته شده است.

۲-۴. نوع انفجار مورد مطالعه

با توجه به موقعیت وقوع انفجار نسبت به سازه، انفجار به دو گروه انفجار داخلی و انفجار خارجی تقسیم می‌گردد. انفجار خارجی نیز با توجه به فاصله محل وقوع آن نسبت به سطح زمین به سه دسته انفجار در هوای آزاد، انفجار هوایی و انفجار سطحی تقسیم‌بندی شده است. انفجار در هوای آزاد نوعی از انفجار خارجی در بالای یک سازه می‌باشد به‌نحوی‌که هیچ‌گونه تقویت‌کننده موج ضربه اولیه میان محل وقوع انفجار و سازه وجود ندارد. حال چنانچه انفجار در فاصله‌ای مشخص از سطح زمین واقع شود موج اولیه ناشی از انفجار پس از برخورد با زمین و انعکاس، به سطح خارجی سازه برخورد می‌کند. در این حالت موج انفجار در امتداد سطح زمین در ارتفاعی موسوم به ارتفاع ماخ منتشر می‌شود. نوع دیگر انفجار خارجی، انفجار سطحی است. انفجار در نظر گرفته‌شده در این تحقیق، از این نوع انفجار می‌باشد. انفجار در این حالت در سطح زمین رخ می‌دهد. موج ناشی از انفجار پس از برخورد با زمین منعکس می‌گردد و با ترکیب این موج با موج اولیه ناشی از انفجار، موج حاصل به‌صورت یک موج به شکل نیم‌کره مطابق شکل (۴) منتشر می‌گردد.



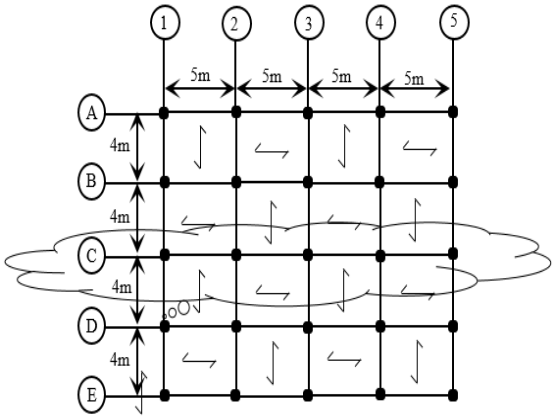
شکل ۴. شماتیک امواج کروی شکل انفجار.

مطالعات انجام‌شده [۲۵] نشان می‌دهد که در شرایط یکسان از نظر مقدار ماده منفجره و فاصله، انفجارهای سطحی دارای اثرات شدیدتری نسبت به سایر انواع انفجار می‌باشد.

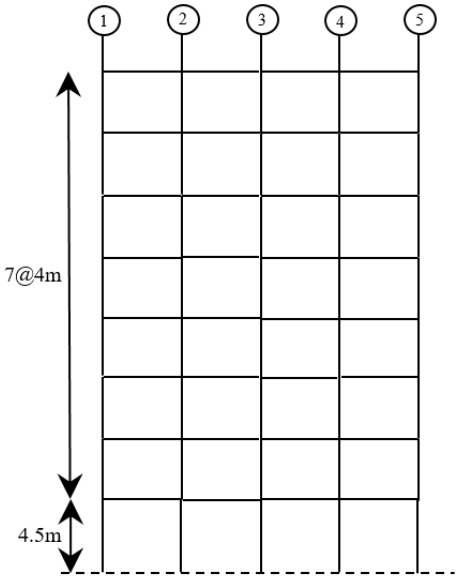
۳. روش تحقیق

یک ساختمان ۸ طبقه بتن مسلح با کاربری اداری، بر اساس مبحث ششم مقررات ملی ساختمان و استاندارد ۲۸۰۰ (ویرایش

چهارم) بارگذاری و تحلیل گردیده است. سپس بر اساس ضوابط مبحث نهم مقررات ملی ساختمان طراحی شده است. با توجه به متقارن بودن پلان، یک قاب میانی از ساختمان (قاب C) در نظر گرفته شده است. بر اساس سطح بارگیر قاب از بار ثقلی و انفجار، مدل‌سازی و تحلیل انجام شده است. شکل‌های (۵) و (۶) به ترتیب پلان ساختمان مورد مطالعه و نمای قاب انتخاب‌شده را نشان می‌دهد.



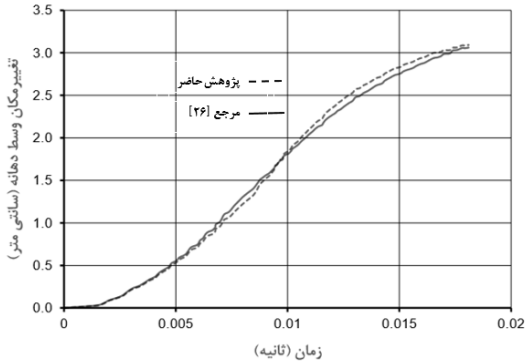
شکل ۵. پلان ساختمان مورد مطالعه.



شکل ۶. قاب محور C ساختمان مورد مطالعه.

در این پژوهش برای تحلیل و طراحی ساختمان از نرم‌افزار Etabs استفاده شده است. پس از طراحی و تعیین ابعاد اعضا، قاب مورد مطالعه در نرم‌افزار *Opensees* مدل‌سازی شده است و تحت بارهای انفجاری با مقادیر مختلف TNT در فاصله ثابت ۱۰ متری از قاب قرار گرفته است. برای مدل‌سازی اعضای بتنی سازه، المان دوبعدی به‌کار برده شد که امکان در نظر گرفتن تغییر جابجایی در طول بارگذاری را دارد. سختی مهاربند ۰/۵ kN/m و نیروی آستانه لغزشی ۰/۵ kN در نظر گرفته شده است.

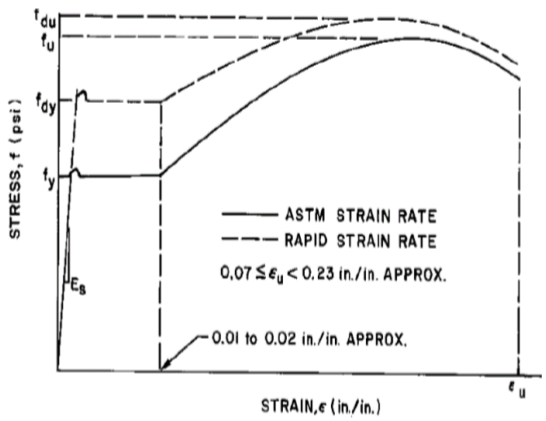
جهت صحت‌سنجی روش به‌کاررفته در این تحقیق، از نتایج کار آزمایشگاهی انجام‌شده بر روی تیرهای بتن مسلح تحت بارگذاری استاتیکی و دینامیکی [۲۶] استفاده شده است. همان‌طور که در شکل (۷) ملاحظه می‌شود مقایسه نتایج، بیانگر سازگاری خوب بین تحلیل عددی انجام‌شده در این پژوهش با کار آزمایشگاهی مورد اشاره است. در بررسی دیگر زمان تناوب سازه هشت طبقه مدل شده در این پژوهش با نتایج کار انجام‌شده توسط واحدی [۲۷] مقایسه شده است. زمان تناوب به‌دست‌آمده در این تحقیق ۱/۷۹۵ ثانیه و نتیجه کار واحدی ۱/۸ ثانیه است که بیانگر سازگاری قابل قبول بین نتایج است.



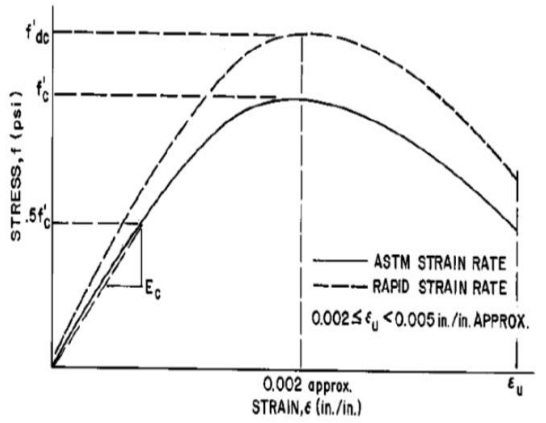
شکل ۷. مقایسه نتایج آزمایشگاهی با مدل‌سازی عددی.

۳-۱. مشخصات مصالح مصرفی

با توجه به این‌که بارگذاری انفجاری از نوع بارگذاری‌های سریع است این خاصیت باعث ایجاد افزایش در سطح تنش تسلیم و تنش نهایی قبل از وقوع گسیختگی این نوع مصالح می‌گردد [۳-۴]. در این حالت عضو سازه‌ای تحت بارگذاری انفجاری از خود مقاومت بیشتری نسبت به حالت تحت بارگذاری استاتیکی نشان می‌دهد. این افزایش مقاومت در هر دو نوع مصالح مصرفی فولاد و بتن همراه با نرخ بالای کرنش است که در اعضای تحت بارگذاری دینامیکی اتفاق می‌افتد. این تنش‌های افزایش‌یافته یا مقاومت دینامیکی مصالح معیاری برای محاسبه مقاومت دینامیکی اعضا تحت اثر بار انفجار است. زیرا مقاومت نهایی دینامیکی اعضا تحت اثر بار انفجار بیش از مقاومت استاتیکی نهایی آن‌ها است. از ضریب افزایش دینامیکی (DIF) برای بیان این ویژگی استفاده می‌شود. این ضریب برابر نسبت مقاومت فشاری نهایی دینامیکی مصالح مصرفی به مقاومت فشاری این نوع مصالح است. شکل‌های (۸) و (۹) اثرات نرخ کرنش بر منحنی تنش – کرنش بتن و فولاد را نشان می‌دهد.



شکل ۸. اثر نرخ کرنش بر منحنی تنش – کرنش فولاد [۲۶].

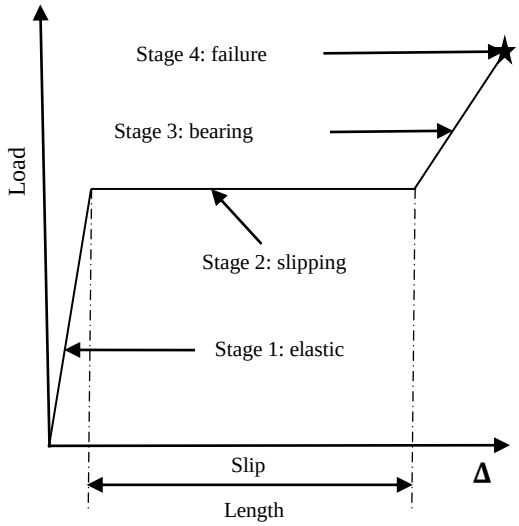


شکل ۹. اثر نرخ کرنش بر منحنی تنش – کرنش بتن [۲۶].

در بارهای دوره‌ای، رفتار بتن پیچیده‌تر می‌شود زیرا که شامل باز و بسته شدن ترک‌های مویی که قبلاً تشکیل شده‌اند و نیز اندرکنش آن‌ها با یکدیگر می‌باشد. هدف کلی این تحقیق بررسی تأثیر استفاده از میراگر اصطکاکی در مهاربند فولادی ضربدری برای مقاوم‌سازی قاب خمشی بتنی است. به این منظور سازه ۸ طبقه طراحی شده، در نرم‌افزار Opensees مدل‌سازی گردیده است. سپس قاب با مهاربند فولادی ضربدری تحت اثر بار انفجار با مقادیر ۱۰، ۱۵ و ۲۰ کیلوگرم ماده منفجره بر حسب TNT قرار گرفته و نتایج بررسی شده است. در گام بعد همین قاب‌ها با مهاربند فولادی ضربدری دارای میراگر اصطکاکی مدل شده است. میراگر اصطکاکی به‌صورت یک فنر در نرم‌افزار Opensees با استفاده از المان Bouck wen material مدل شده است. در گام آخر قاب ۸ طبقه با مهاربند فولادی ضربدری دارای میراگر اصطکاکی تحت اثر همان بار انفجاری ۱۰، ۱۵ و ۲۰ کیلوگرم ماده منفجره بر حسب TNT مورد بررسی قرار گرفته است. در کلیه قاب‌ها مدت زمان تحلیل ۲۵ ثانیه در نظر گرفته شده است. همان‌طور که قبلاً بیان شد میراگر اصطکاکی در نرم‌افزار $Opensees$ به‌صورت یک فنر مدل می‌شود که رفتار این فنر مطابق با رفتار هیسترزیس میراگر اصطکاکی می‌باشد. برای مدل‌سازی میراگر بایستی دو پارامتر سختی و نیروی آستانه لغزشی محاسبه شود. میزان انرژی مستهلک‌شده توسط این میراگر برابر حاصل‌ضرب بار لغزشی در میزان جابه‌جایی میراگر است.

۳-۲. رفتار شماتیک میراگر اصطکاکی

در شکل (۱۰) منحنی بار- تغییرمکان میراگر در فازهای مختلف نشان داده شده است.



شکل ۱۰. رفتار شماتیک میراگر اصطکاکی.

همان‌طور که در این شکل ملاحظه می‌شود رفتار میراگر تحت اثر بار به چهار فاز قابل تفکیک است که به ترتیب عبارت‌اند از:

فاز اول سختی(k) میراگر
فاز دوم نیروی آستانه لغزشی
فاز سوم طول لازم جهت لغزش
فاز چهارم وقوع گسیختگی

۴. نتایج و بحث

۴-۱. نمودار تاریخچه زمانی بام

شکل‌های (۱۱) تا (۱۳) نشان‌دهنده تغییرمکان بام در مقابل زمان می‌باشد. در این شکل‌ها نتایج تحلیل برای دو حالت سازه با

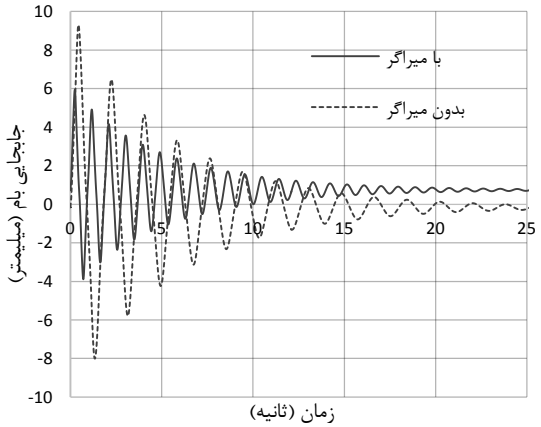
مهاربند فولادی ضربدری بدون میراگر و سازه با مهاربند فـولادی ضربدری با میراگر، تحت بار انفجار با مقادیر مختلف مواد منفجره، در فاصله ۱۰ متری از سازه نشان داده شده است.

همان‌گونه که ملاحظه می‌شود حداکثر تغییرمکان اندکی بعد از ارتعاش اجباری، در ابتدای ارتعاش آزاد رخ می‌دهد. این نمودار همچنین نشان‌دهنده توانایی سازه در میرا کردن ارتعاش ناشی از انفجار می‌باشد. با توجه به شکل می‌توان دید که سازه با مهاربنـد فولادی ضربدری بدون میراگر دارای میرایی کمـی در مقابـل بـار ضربه‌ای انفجار می‌باشد. به‌طوری‌که در پایان تحلیل، ارتعاش سازه تقریباً به مقدار صفر رسیده است.

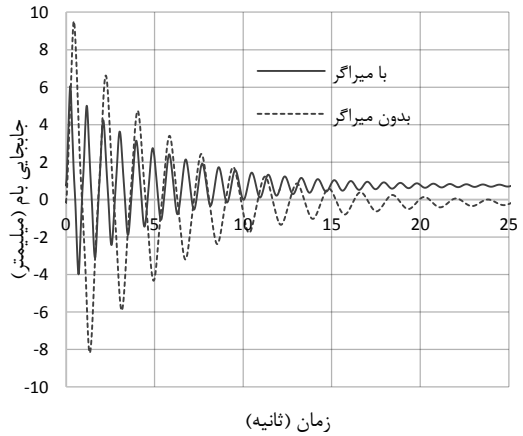
در این سازه حداکثر تغییرمکان جـانبی در فـاز ارتعـاش آزاد صورت گرفته است. سـازه‌ی مـورد مطالعـه در فاصـله ۱۰ متـری تحت بارهـای انفجـار ۱۰، ۱۵ و ۲۰ کیلـوگرم مـاده منفجـره بـر حسب TNT قرار گرفته است و نمودار تغییرمکان – زمـان آن‌هـا در شکل‌های (۱۱) تا (۱۳) برای دو حالـت سـازه دارای مهاربنـد فولادی ضربدری با میراگر و سازه دارای مهاربند فولادی ضربدری بدون میراگر با یکدیگر مقایسه شده است. همان‌طور کـه در ایـن شکل‌ها مشاهده می‌شود با گذشت زمان مقدار جابجـایی کـاهش یافته است. نرخ کاهش تغییرمکان کـه بـه‌صـورت مقـدار کـاهش تغییرمکان در واحد زمان تعریف شده است در حالت سـازه دارای مهاربند فولادی ضربدری با میراگر بـیش از سـازه دارای مهاربنـد فولادی ضربدری بدون میراگر است.

مطالعات نشان می‌دهد جابجایی بام در سـازه دارای مهاربنـد فولادی ضربدری با میراگـر در مقایسـه بـا سـازه دارای مهاربنـد فولادی ضربدری بدون میراگر تا ۲۰ درصد کاهش یافته است که این مقدار کاهش در نمودارهای ترسیم شده مشاهده می‌شود.

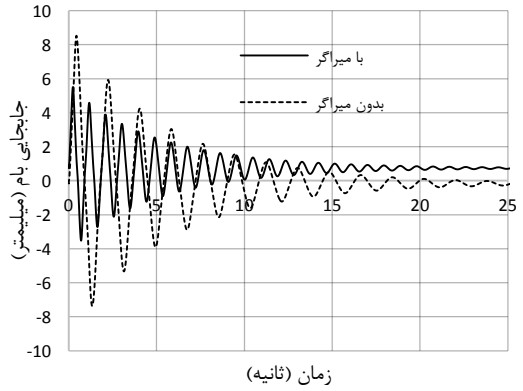
بررسی نحوه تغییر میزان جابجایی بام در برابـر مقـدار مـاده منفجره بیانگر آن است که با افزایش مقدار ماده منفجـره میـزان جابجایی بام کاهش می‌یابد. این مسئله مـی‌توانـد ناشـی از بـروز پدیده نرخ کرنش در مصالح باشـد کـه در شـکل‌هـای (۸) و (۹) نشان داده شده است. همان‌طـور کـه در ایـن شـکل‌هـا ملاحظـه می‌شود با توجه به ماهیت بارگذاری سریع انفجار بر سازه، این امر باعث افزایش مقاومت سازه در برابر بار دینامیکی ناشی از انفجـار می‌گردد. نتایج به‌دست‌آمده در شکل‌های (۱۱) تا (۱۳) بیانگر آن است که با افزایش مقدار ماده منفجره این میزان مقاومت سازه در برابر تغییرمکان جانبی بیشتر بروز می‌کند.



شکل ۱۱. نمودار تاریخچه زمانی جابجایی بام قاب ۸ طبقـه در فاصـله ۱۰ متری از محل وقوع انفجار در دو حالت بدون میراگر و بـا میراگـر در برابـر ۱۰ کیلوگرمTNT.



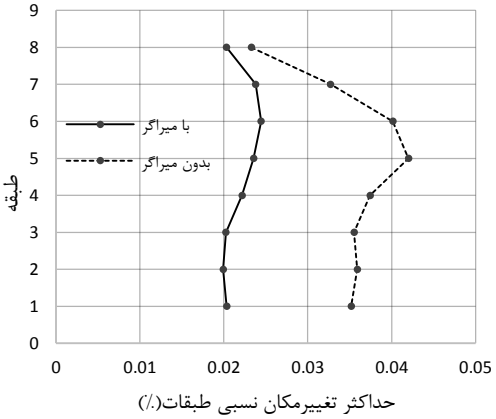
شکل ۱۲. نمودار تاریخچه زمانی جابجایی بام قاب ۸ طبقـه در فاصـله ۱۰ متری از محل وقوع انفجار در دو حالت بدون میراگـر و بـا میراگـر در برابر ۱۵ کیلوگرم TNT.



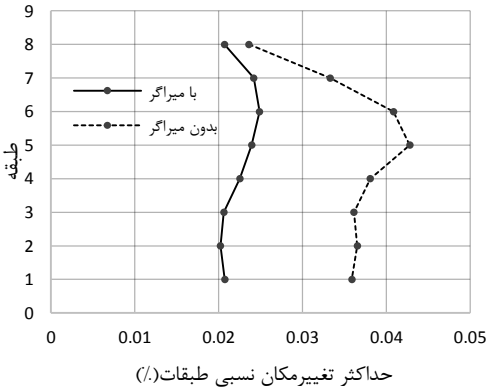
شکل ۱۳. نمودار تاریخچه زمانی جابجایی بام قاب ۸ طبقه در فاصـله ۱۰ متری از محل وقوع انفجار در دو حالت بدون میراگـر و بـا میراگـر در برابر ۲۰ کیلوگرم TNT.

۴-۲. نمودار حداکثر تغییرمکان نسبی طبقات

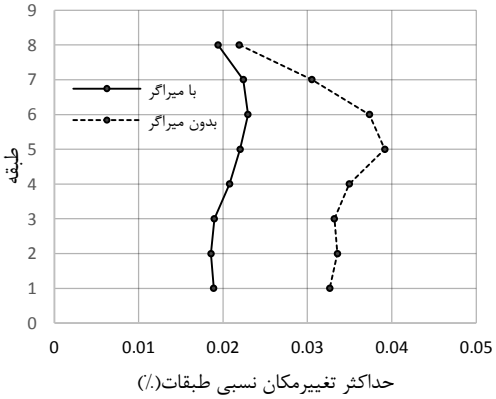
شکل‌های (۱۴) تا (۱۶) نمودار حداکثر تغییرمکان نسبی طبقات سازه ۸ طبقه دارای مهاربند فولادی بدون میراگر و با میراگر در برابر نیروی انفجار در فاصله ۱۰ متری از سازه را نشان می‌دهد.



شکل ۱۴. نمودار حداکثر تغییرمکان نسبی طبقات قاب ۸ طبقه در فاصله ۱۰ متری از محل وقوع انفجار در حالت بدون میراگر و با میراگر در برابر ۱۰ کیلوگرم TNT.



شکل ۱۵. نمودار حداکثر تغییرمکان نسبی طبقات قاب ۸ طبقه در فاصله ۱۰ متری از محل وقوع انفجار در دو حالت بدون میراگر و با میراگر در برابر ۱۵ کیلوگرم TNT.

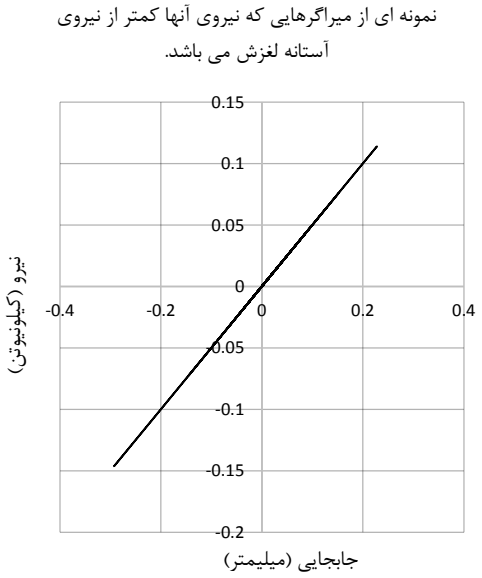


شکل ۱۶. نمودار حداکثر تغییرمکان نسبی طبقات قاب ۸ طبقه در فاصله ۱۰ متری از محل وقوع انفجار در دو حالت بدون میراگر و با میراگر در برابر ۲۰ کیلوگرم TNT.

از مقایسه حداکثر تغییرمکان نسبی طبقات در دو حالت سازه دارای مهاربند فولادی ضربدری بدون میراگر و سازه دارای مهاربند فولادی ضربدری با میراگر، کاهش قابل‌توجهی در حداکثر تغییرمکان نسبی سازه دارای مهاربند فولادی ضربدری با میراگر دیده می‌شود که این مطلب نشان‌دهنده تأثیر و اهمیت میراگر اصطکاکی مهاربند فولادی ضربدری در سازه است.

مقایسه حداکثر تغییرمکان نسبی طبقات در سه حالت ساختمان تحت تأثیر ۱۰ کیلوگرم، ۱۵ کیلوگرم و ۲۰ کیلوگرم ماده منفجره در فاصله ۱۰ متری از قاب مورد مطالعه، نشان می‌دهد که با افزایش مقدار ماده منفجره، حداکثر تغییرمکان نسبی طبقات کاهش یافته است. این اثر ناشی از بروز پدیده نرخ کرنش در مصالح تحت اثر بار انفجار می‌باشد.

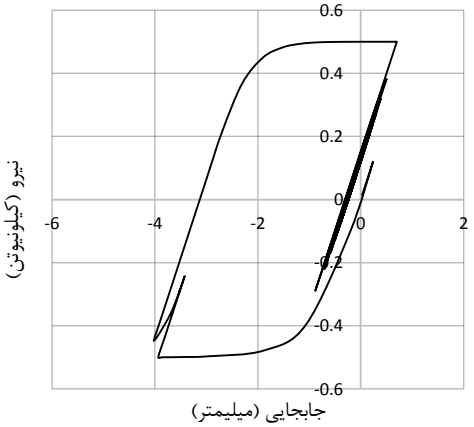
شکل (۱۷) نمونه‌ای از نمودار هیسترزیس را نشان می‌دهد که در آن نیروی میراگرها کمتر از نیروی آستانه لغزش در سازه می‌باشد. در این حالت سازه وارد فاز لغزش نمی‌شود و بنابراین، نمودار هیسترزیس به‌صورت یک خط ملاحظه می‌شود.



شکل ۱۷. نمودار هیسترزیس در حالت نیروی میراگر کمتر از نیروی آستانه لغزش.

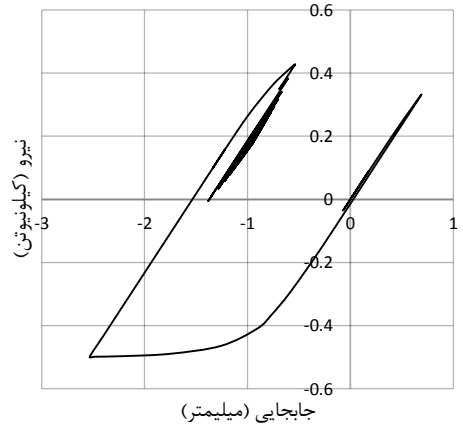
شکل‌های (۱۸) و (۱۹) نمونه‌هایی از نمودار هیسترزیس را نشان می‌دهند که در آن نیروی میراگر بیشتر از نیروی آستانه لغزش در سازه است و وارد فاز لغزش گردیده و شکل آن مطابق شکل (۱۰) شماتیک رفتار میراگر اصطکاکی به‌دست آمده است.

نمونه ای از میراگرهایی که نیروی آنها از نیروی آستانه لغزش بیشتر شده است.



شکل ۱۸. نمودار هیسترزیس در حالت نیروی میراگر بیشتر از نیروی آستانه لغزش.

نمونه ای از میراگرهایی که نیروی آنها از نیروی آستانه لغزش بیشتر شده است.



شکل ۱۹. نمودار هیسترزیس در حالت نیروی میراگر بیشتر از نیروی آستانه لغزش.

۵. نتیجه‌گیری

با بررسی و مقایسه قاب بتنی ۸ طبقه دارای مهاربند فولادی ضربدری بدون میراگر و مجهز به میراگر مشاهده می‌شود که در قاب دارای مهاربند فولادی بدون میراگر، حداکثر تغییرمکان نسبی طبقات در برابر انفجار به مراتب بیشتر از حداکثر تغییرمکان نسبی طبقات در قاب دارای مهاربند فولادی با میراگر می‌باشد که این امر بیانگر آن است که استفاده از میراگر باعث کاهش تغییرمکان نسبی طبقات می‌گردد. بررسی تاریخچه زمانی جابه‌جایی بام نشان می‌دهد که در قاب بدون میراگر حداکثر تغییرمکان اندکی بعد از ارتعاش آزاد رخ داده که در قاب دارای میراگر دارای کاهش قابل‌ملاحظه‌ای است. این کاهش نشان‌دهنده تأثیر میراگر اصطکاکی در کاهش حداکثر جابه‌جایی بام در قاب دارای میراگر است.

با توجه به نتایج فوق، پیشنهاد استفاده از مهاربند فولادی مجهز به میراگر جهت تقویت و بهسازی قاب‌های بتنی، راهکار مؤثر و کارآمدی جهت مقابله با تهدیدات ناشی از بارهای جانبی ناشی از انفجار است.

۶. مرجع‌ها

[1] Bangash, M. Y. H. “Shock, Impact and Explosion”; Springer Berlin, Heidelberg, London, 2009.

[2] Ngo, T.; Mendis, P.; Gupta, A.; Ramsay, J. “Blast Loading and Blast Effects on Structures, an Overview”; EJSE. Special Issue: Loading on Structures, Uni. Melbourne, Australia, 2007, 7, 76-91.

[3] TM, 5-1300. “The Design of Structures to Resist the Effects of Accidental Explosions”; US Department of the Army, Navy and Air Force, Washington DC, 1990.

[4] Unified Facilities Criteria, UFC 3-340-02. “Structures to Resist the Effects of Accidental Explosions”; US Department of Defense, Washington DC, 5 December 2008.

[5] Pall, A. S.; Marsh, C. “Response of Friction Damped Braced Frames”; Journal of Structural Division, ASCE. 108, 9, 1313-1323, 1982.

[6] Baker, W. E.; Cox, P. A.; Westine, P. S.; Kulesz, J. J. “Explosion Hazards and Evaluation”; Elsevier Scientific Publishing Company. New York, 1983.

[7] Rouzsky, N. “Blast-Resistance Control Buildings”; Structural Safety. 5, 253-266, 1988.

[8] Ian, D. A.; Douglas, K.; Adrew, S. W.; James, M. K. “Testing of Passive Energy Dissipation Systems”; Earthquake Spectra. Vol. 9, NO. 3, Earthquake Engineering Research Institute California. August, 1993.

[9] Mualla, I. H.; Belev, B. “Performance of Steel Frames with a New Friction Damper Device under Earthquake Excitation”; J. of Eng. Struct. 24, 365–371, 2002.

[10] Mualla, I. H.; Nielsen, L.O.; Belev, B.; Liao, W. I.; Loh, C. H.; Agrawal, A. “Numerical Prediction of Shaking Table Tests on a Full Scale Friction Damped Structure”; 12th European Conference on Earthquake Engineering, London, UK, 2002.

[11] Bing, L.; Tso-Chien P.; Anand, N. “A Case Study of the Effect of Cladding Panels on the Response of Reinforced Concrete Frames Subjected to Distant Blast Loadings”; Nucl. Eng. Des. 239, 455-469, 2009.

[12] Yasser, E. I.; Mostafa, A. I.; Marwa, N. “Response of Reinforced Concrete Frame Structures under Blast Loading”; Procedia Eng. 171, 890-898, 2017.

[13] Zubair I. S.; Osama A. M.; Kumail M.; Manish K. “Performance of Earthquake-resistant RCC Frame Structures under Blast Explosions”; Procedia Eng. 180, 82-90, 2017.

[14] Yang, D.; Xiaoran, S.; Hai-Tao Z. “Probabilistic Progressive Collapse Analysis of Steel Frame Structures against Blast Loads”; J. of Eng. Struct. 147, 679-691, 2017.

[15] Iranian National Building Code, Part 21, Passive Defense, Tehran (Iran), Ministry of Housing and Urban Development, 2012 (In Persian).

[16] Nourizadeh, A.; Izadifard, R. A. "Performance of Reinforced Concrete Frame Designed According to Iranian Earthquake Code, Subjected to Blast Loading"; Adv. Def. Sci. Tech. 3, 169-181, 2016. (In Persian).

[17] Standard No. 2800. "Iranian Code of Practice for Seismic Resistant Design of Buildings"; 4th Revision, Building and Housing Research Center, Tehran, 2013, (In Persian).

[18] Shiravand, M. R.; Shabani, M. J. "Behavior of the Special Moment Frames and Braced Frames in Steel Structures under Blast Loadings"; Adv. Def. Sci. Tech. 2, 109-114, 2013. (In Persian).

[19] Kamgar, R.; Shams, Gh. R. "Effect of Blast Load in Nonlinear Dynamic Response of the Buckling Restrained Braces Core"; Adv. Def. Sci. Tech. 1, 107-118, 2017. (In Persian).

[20] FEMA427.; "Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks"; Federal Emergency Management Agency, December 2003, Chapter 4, 1-10.

[21] FEMA426.; "Reference Manual to Mitigate Potential Terrorist Attacks against Building"; Federal Emergency Management Agency, December 2003, Chapter 4, 1-20.

[22] Bangash, N. Y. H.; Bangash, T.; "Shock, Impact and Explosion"; Springer-Verlag, Berlin Heidelberg, 388-393, 2009.

[23] ISC.; "Facts for Steel Buildings, Blast and Progressive Collapse"; American Institute of Steel Construction, 1-13, 2004.

[24] Richard, L. J. "Survivability of Steel Frame Structures Subject to Blast and Fire"; Journal of Constructional Steel Research, Vol. 64, Pages 854-866, 2008.

[25] Ngo, T.; Mendis, P.; Gupta, A.; Ramsay, J. "Blast Loading and Blast Effects on Structures-An Overview"; The University of Melbourne, Australia. EJSE Special Issue: Loading on Structures, 76-91, 2007.

[26] Seabold, R. H. "Dynamic Shear Strength of Reinforced Concrete Beams, Part II"; Naval Civil Engineering Laboratory, Port Hueneme, California, 1967.

[27] Vahedi, J. "Investigation of the effect of passive dampers on controlling the response of frames against explosive loading", Master of Science (MSc), Urmia Uni, 2007. (In Persian).

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۳۸۲-۳۶۹

بررسی اثر تخریبی انفجار در فواصل مختلف بر دیوار حائل بتنی

محمدحسین تقوی‌پارسا[1*]، علی گراوند[2]
۱- دکتری، دانشگاه جامع امام حسین(ع)، ۲- کارشناس ارشد مهندسی سازه، دانشگاه اصفهان
(دریافت: ۹۸/۱۰/۲۱، پذیرش: ۹۹/۰۶/۱۵)

چکیده

استفاده از دیوارهای حائل بتنی به‌دلیل جرم زیاد گزینه مطلوبی برای مقاومت در برابر انفجار است. این دیوارها عموماً به‌صورت بتن آرمه یا بتن الیافی ساخته می‌شوند. در این پژوهش اثرات تخریبی انفجار بر دیوار حائل از جنس بتن آرمه و بتن الیافی مورد مطالعه قرار گرفته است. به این منظور، دیوار در نرم‌افزار آباکوس شبیه‌سازی شده و بارهای انفجار متفاوت در فواصل مختلف بر آن اعمال شده است. سپس برای بررسی خرابی حاصل از انفجار، مواد منفجره در سه حالت چسبیده به دیوار، در فاصله یک متری و در فاصله ده متری از دیوار، عمود بر بالاترین نقطه میانی سازه و نیز محل اتصال دیوار و زمین مدل‌سازی شده‌اند. نتایج حاصل از مدل‌سازی نشان داد که انفجار در محل اتصال دیوار و زمین تأثیرات مخرب‌تری نسبت به انفجار در بالاترین نقطه دیوار دارد. بارهای منجر به تخریب دیوار بتن آرمه و بتن الیافی در محل اتصال دیوار به زمین، در فاصله چسبیده به آن برابر با ۵ کیلوگرم C4 و ۱۰ کیلوگرم TNT و در فاصله یک متری از دیوار برابر با ۱۵ کیلوگرم C4 و ۱۵ کیلوگرم TNT خواهد بود. در فاصله ۱۰ متری از دیوار و در محل اتصال دیوار به زمین، بارهای منجر به تخریب برابر با ۶۰ کیلوگرم C4 و ۷۰ کیلوگرم TNT برای دیوار بتن آرمه و ۹۰ کیلوگرم C4 و ۱۰۰ کیلوگرم TNT برای دیوار بتن الیافی می‌باشد. همچنین انفجار در فاصله چسبیده به دیوار و یک متری، تأثیر موضعی بر دیوار داشته و باعث خرابی‌های موضعی می‌گردد. این در حالی است که انفجار در فاصله ده متری به علت فاصله زیاد انفجار از دیوار به‌صورت موضعی عمل نکرده و برای تخریب دیوار در این فاصله ماده منفجره بیشتری لازم است.

کلیدواژه‌ها: انفجار، آباکوس، دیوار بتن آرمه، بتن الیافی، خرابی.

Investigating the Destructive Effect of Explosions at Different Distances on Concrete Retaining Walls

M. H. Taghavi Parsa*, A. Geravand
Imam Hossein University
(Received: 11/01/2020; Accepted: 15/09/2020)

Abstract

Concrete retaining walls gratitude to their significant-high mass are considered a protective barrier and explosion resistance. The fabricated walls generally made of reinforced or fiber-reinforced concrete. This study deals with investigating the destructive effects of the explosion on retaining walls made of reinforced and fiber-reinforced concrete. For this purpose, the intended wall simulated by Abaqus software with various blast loads at different distances. Then, to investigate the damage caused by the explosion, the explosives were modeled in three positions attached to the wall, at a distance of one meter and at a distance of ten meters from the wall, perpendicular to the highest midpoint of the structure and the junction of wall and ground. The modeling results showed that the explosion at the connection of the wall to the ground has more destructive effects than the detonation at the highest point of the wall. The failure load of the reinforced concrete wall and fiber-reinforced concrete at the junction of the wall to the ground equals 5 kg C4 and 10 kg TNT and 15 kg C4 and 15 kg TNT at attached and distance of one meter from the wall respectively. The failure load was equal to 60 kg C4 and 70 kg TNT and 90 kg C4 and 100 kg TNT for reinforced concrete and fiber-reinforced concrete wall respectively at a distance of 10 meters from the wall and at the junction of the wall to the ground. Also, the explosion at the position attached to the wall and one meter from the wall showed local effects on the wall and occasion local damage. However, the explosion at a distance of ten meters did not act locally due to the large distance of the explosion from the wall, and more explosives are needed to destroy the wall at this distance.

Keywords: Explosion, Abaqus, Reinforced Concrete Wall, Fiber-Reinforced Concrete, Failure.

* Corresponding Author E-mail: drmhparsa@gmail.com

۱. مقدمه

پاسخ سازه در برابر بار انفجار، دینامیکی و تابعی از جرم و سختی المان‌های سازه‌ای است. علاوه بر این، امواج انفجار در مقایسه با دوره تناوب طبیعی کلی سازه در مدت‌زمان بسیار کوتاهی انتشار می‌یابند که منجر به عملکرد ضربه‌ای بارهای انفجار می‌شود. انرژی امواج انفجار به‌صورت انرژی جنبشی و در قالب سرعت اولیه به المان‌های سازه‌ای منتقل می‌گردد. با استفاده از رابطه انرژی جنبشی ($E_k = \frac{1}{2}mv^2$) که با جرم جسم (m) و مجذور سرعت (v^2) رابطه مستقیم دارد، می‌توان به این نتیجه دست یافت که اندازه این سرعت اولیه متناسب با انرژی موج انفجار است و رابطه عکس با جرم سازه دارد [۱]. از این‌رو استفاده از سازه بتنی در برابر بار انفجار به‌علت جرم زیاد آن نتایج بسیار سودمندی دارد. به همین دلیل دیوارهای حائل بتنی به‌منظور ایجاد حریم، حفاظت و نیز نوعی از انسداد کاربرد دارند. این دیوارها ممکن است به‌صورت پیش‌ساخته و یا در جاریز و از نوع بتن آرمه یا بتن الیافی اجرا شوند.

تجزیه و تحلیل رفتار سازه‌های بتن آرمه و بتن الیافی به‌منظور مقاومت در برابر بارهای دینامیکی با مدت‌زمان تأثیر کوتاه، مانند بار انفجار، در دهه‌های گذشته به‌صورت گسترده‌ای مورد مطالعه قرار گرفته است. به‌منظور درک رفتار سازه بتنی در این نوع بارگذاری، آزمایش‌های انفجار در مقیاس کامل مورد نیاز است که به‌دلیل محدودیت‌های امنیتی و منابع قابل توجه مالی مورد نیاز دچار محدودیت‌هایی هستند و در اغلب موارد سازه موردنظر به‌صورت مقیاس‌شده مورد آزمایش قرار گرفته است [۷-۲]. به‌منظور بررسی خرابی سازه‌های بتن آرمه تحت اثر بار انفجار، هم مطالعات آزمایشگاهی و هم شبیه‌سازی‌هایی در نرم‌افزارهای اجزاء محدود صورت گرفته است. در ادامه چند نمونه از کارهای انجام‌گرفته در زمینه انفجار سازه‌های بتنی مورد بررسی قرار می‌گیرد.

سیلوا و همکاران [۸] در کاری آزمایشگاهی، روشی جهت تخمین خسارت ناشی از برخی حالات بارگذاری انفجار ارائه کردند. به این منظور آنان آزمایش‌هایی بر روی دال بتن آرمه با تغییر فاصله انفجار و وزن مواد منفجره انجام دادند. سپس با توجه به نتایج حاصل از آزمایش‌ها، روش پیشنهادی خود را برای تخمین سطح خرابی با توجه به وزن و فاصله ماده منفجره تا سازه بتن آرمه ارائه کردند. لوچینی و همکاران [۹]، در کاری آزمایشگاهی به همراه شبیه‌سازی عددی به بررسی تحلیل رفتار روسازی بتنی در معرض بارهای انفجار پرداختند. در این کار آنان ابتدا به‌صورت آزمایشگاهی دال بتنی را تحت اثر انفجار قرار دادند. سپس نتایج به‌دست‌آمده را با مدل‌سازی مسئله توسط نرم‌افزارهای آتودین و آباکوس مورد صحت‌سنجی قرار دادند. در انتها رابطه‌ای بین قطر حفره ناشی از انفجار، وزن و محل انفجار ارائه کردند.

به‌دلیل خطرناک و پرهزینه بودن آزمایش‌های انفجار، می‌توان با استفاده از نرم‌افزارهای اجزاء محدود پدیده انفجار را شبیه‌سازی و نتایجی مشابه با آزمایش‌های صورت‌گرفته در این زمینه گرفت. از جمله نرم‌افزارهای قدرتمند در زمینه شبیه‌سازی پدیده انفجار، نرم‌افزار آباکوس می‌باشد که محققین مسائل مختلف اثرگذاری انفجار بر اجزای مختلف سازه‌های بتنی و فولادی با استفاده از آن را شبیه‌سازی کرده‌اند [۱۴-۱۰]. در ادامه به بررسی برخی از مقالات موجود در این زمینه پرداخته می‌شود. وانگ و همکاران [۱۵] در مطالعه‌ای به بررسی رفتار دال‌های بتن آرمه یک‌طرفه در معرض بار انفجار از طریق آزمایش و شبیه‌سازی عددی پرداختند و معیار خرابی را برای سطوح مختلف خسارت در اثر تغییر فاصله و وزن انفجار ارائه کردند. همچنین با افزایش بار مواد منفجره در فاصله ثابت از دال، مشاهده کردند که حالت خرابی دال بتن آرمه از خمش کلی به شکست پانچ موضعی تغییر می‌کند. شاشانک و همکاران [۱۶]، در کاری عددی پاسخ دینامیکی دیوار بتن آرمه تحت بار انفجار را مورد بررسی قرار دادند. آنان در این کار دیوار بتنی به همراه میلگردها را توسط نرم‌افزار اجزاء محدود آباکوس شبیه‌سازی و تأثیرات پارامترهای مختلف از قبیل: ضخامت دیوار، مقاومت فشاری بتن، درصد آرماتور، مقاومت کششی آرماتورها، قطر میلگرد و خواص وابسته به نرخ کرنش بتن و فولاد را مورد بررسی قرار دادند. درنهایت پس از تحلیل نتایج حاصل از مدل‌سازی به این نتیجه رسیدند که عمدتاً ضخامت دیوار و درجه بتن نسبت به درصد آرماتور، قطر میلگرد و درجه فولاد، پاسخ انفجار را کنترل می‌کند. همچنین دیوارهای بتن آرمه با مدل‌سازی مشخصات مصالح وابسته به کرنش، جابه‌جایی کمتری نسبت به مشخصات مصالح مستقل از کرنش از خود نشان می‌دهند.

با توجه به تماس خاک با سازه اعم از بتنی و فولادی، تحقیقاتی نیز با در نظر گرفتن برهم‌کنش خاک و سازه تحت اثر بارهای جانبی شامل زلزله و انفجار صورت گرفته است [۲۱-۱۷]. بازیار و همکاران [۲۲] به‌منظور مقایسه عملکرد دیوار حائل وزنی بتنی و خاک مسلح به‌عنوان دیوار محافظ جاده برای جلوگیری از ریزش خاک‌ریز در پشت آن‌ها، با استفاده از نرم‌افزار FLAC-2D تغییرشکل‌های به‌وجود آمده در اثر بارگذاری‌های مختلف انفجار در این دیوارها را بررسی کردند. در این کار آنان انفجار را در فواصل دور از سازه و داخل خاک در نظر گرفتند و بر اساس آن بتن را به‌صورت الاستیک مدل کردند و به پیش‌بینی عملکرد این دیوارها در انفجارها با شدت و فواصل مختلف پرداختند. توی و سویم [۲۳]، با استفاده از نرم‌افزار آتودین به شبیه‌سازی دیوار حائل بتن آرمه به همراه خاک‌ریز پشت آن تحت بار انفجار در دو فاصله مختلف پرداختند. در این پژوهش انفجار در دو فاصله ۴ و ۵/۵ متری از دیوار مدل شد و نتایج جابه‌جایی‌ها و تنش‌های ایجادشده در دیوار با نمودارهای موجود در UFC 3-340-2 و روابط تجربی دیگر محققین بررسی شد. گیوری و همکاران [۲۴]، در کاری

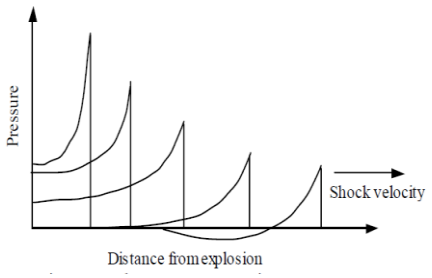
عددی با شبیه‌سازی در نرم‌افزار آباکوس و با تغییر مشخصات خاک پشت دیوار حائل بتنی به بررسی پایداری دیوار حائل تحت بار انفجار در فاصله یک متری از آن پرداختند. در این کار آنان بتن را به‌صورت الاستیک مدل کردند و با تغییر زاویه شکست داخلی و چسبندگی خاک به این نتیجه رسیدند که تغییر پارامترهای مذکور اثر قابل ملاحظه‌ای بر پایداری دیوار حائل ندارد.

پیشرفت‌های انجام‌شده در صنعت ساختمان و مطالعات انجام‌گرفته بر روی بتن، منجر به ظهور انواع مختلفی از بتن الیافی شده است. در این نوع از بتن، الیاف‌های مختلفی به‌صورت ماکروسکوپی و اختلاط فیزیکی به بتن اضافه می‌گردد و منجر به بالا رفتن مقاومت بتن در کشش می‌شود. بتن الیافی به‌دلیل جذب انرژی و مقاومت بالا در برابر بارهای انفجار مورد توجه محققان قرار گرفته است. فوگلار و همکاران [۲۵] در تحقیقی اثر بار انفجار نزدیک بر عرشه پل‌ها را با در نظر گرفتن افزایش الیاف فولادی با عملکرد بسیار بالا بر بتن مورد بررسی قرار دادند. نتیجه کار آنان به این‌صورت بود که افزایش درصد الیاف فولادی با مقاومت بسیار بالا تأثیر بسیار خوبی بر رفتار بتن الیافی در برابر انفجار دارد. همچنین مشاهده کردند که قرار دادن شبکه مش در دال‌ها منجر به بهبود رفتار بتن الیافی در برابر انفجار می‌شود. آبیسینگ و همکاران [۲۶] در تحقیقی به مطالعه آزمایشگاهی بر روی اثر الیاف آرامید بر مقاومت پنل‌های بتن الیافی پرداختند. در این پژوهش چند دال بتن آرمه و بتن الیافی با الیاف آرامید در برابر بار انفجار مورد بررسی قرار گرفتند. با توجه به آزمایش‌های انجام‌گرفته، آنان به این نتیجه رسیدند که استفاده از الیاف آرامید در داخل بتن باعث افزایش جذب انرژی و افزایش مقاومت بتن می‌شود. یو و همکاران [۲۷] در پژوهشی به بررسی عملکرد دال‌های بتن آرمه مجهز به الیاف با عملکرد بسیار بالا پرداختند. در این پژوهش، آزمایش‌هایی بر روی دال‌ها با در نظر گرفتن پارامترهای مختلفی از جمله طول الیاف، جهت الیاف در بتن، بتن با مقاومت بالا و بتن معمولی تحت بارهای انفجار یا ضربه، انجام گرفت. نتیجه این پژوهش نیز همانند سایر مطالعات انجام‌شده مشابه، نشان‌دهنده عملکرد خوب بتن الیافی با مقاومت بسیار بالا نسبت به بتن آرمه بود.

اکثر کارهای انجام‌شده در زمینه بررسی اثر انفجار بر سازه بتنی، بر روی دال‌های بتنی صورت گرفته است. در شبیه‌سازی‌های صورت گفته نیز عمدتاً به بحث انفجار در دیوارهای حائل پرداخته نشده است. در مطالعاتی نیز که بر روی دیوار حائل صورت گرفته، این دیوار به‌صورت دیوار حائل در برابر حرکت خاک‌ریز پشت آن در نظر گرفته شده و با در نظر گرفتن انفجار در فواصل میانی و دور و با الاستیک در نظر گرفتن بتن در مدل‌سازی‌ها به بررسی تغییر شکل‌های خاک، دیوار و پایداری آن پرداخته شده است. به همین جهت در پژوهش حاضر به بررسی اثر انفجار بر سازه دیوار حائل به‌عنوان سازه انسدادی و خرابی‌های ایجادشده در دیوار تحت انفجار در فواصل نزدیک، میانی و دور پرداخته شده است. به این منظور، یک دیوار حائل یکبار از جنس بتن آرمه و بار دیگر از جنس بتن الیافی بدون آرماتور، تحت بارگذاری انفجار در نرم‌افزار آباکوس شبیه‌سازی شده است. سپس با تغییر شدت انفجار و فاصله محل انفجار از دیوار، اثر تخریبی انفجار بر دیوار مورد بررسی قرار گرفته است.

۲. روش تحقیق

انفجار، آزاد شدن ناگهانی انرژی با مدت‌زمان تداوم اندک است [۱]. در لحظه وقوع انفجار مقدار زیادی انرژی به شکل انرژی جنبشی و حرارت در زمان بسیار کوتاهی (در حدود ۰/۰۱ ثانیه) آزاد می‌شود. انرژی آزادشده باعث جلو راندن توده هوای اطراف خود می‌شود که به آن موج انفجار می‌گویند. انرژی آزادشده به‌صورت موج انفجار با ایجاد تغییرات شدید فشار در محیط اطراف خود، ضربه مکانیکی شدیدی به محیط وارد می‌کند [۲۸]. اضافه فشار انفجار[1] مهم‌ترین بخش انفجار است و بیشترین اثر را روی رفتار و پاسخ سازه دارد. بار اضافه فشار به‌علت افزایش فشار ناشی از انبساط توده انفجاری حاصل می‌شود. این بار به‌صورت شکل (۱) با افزایش فاصله از محل انفجار کم می‌شود. با توجه به شکل (۱)، انفجارهایی با فاصله کم دارای بازه کوتاه و فشار بیشتر بر سازه و انفجارهای با فاصله زیاد دارای فشار یکنواخت و کمتر و بازه طولانی‌تری هستند.



شکل ۱. نحوه انتشار موج انفجار [۱۶].

با وقوع انفجار در فاصله مشخص از سازه، موج انفجار در زمان t_A به سازه رسیده و در این لحظه فشار وارد بر سازه از فشار محیط (P_0) به فشار حداکثر (P_{S0}) می‌رسد. فشار وارد بر سازه با سپری شدن زمان $t_A + t_d$ به فشار محیط می‌رسد. این محدوده، فاز مثبت انفجار را در برمی‌گیرد. پس از این لحظه، در سازه مکش یا فاز منفی اتفاق می‌افتد که دارای زمان تداوم بیشتر و قدرتی به‌مراتب کمتر از فاز مثبت است. با گذشت زمان t_d^- از لحظه شروع فاز منفی، فشار موج با فشار محیط متعادل می‌شود و پدیده انفجار پایان می‌یابد (شکل ۲).

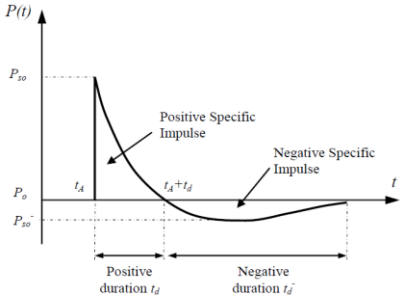
نمودار فشار- زمان امواج انفجاری را می‌توان با یک تابع نمایی به‌صورت رابطه (۱) نمایش داد:

[1] Blast Overpressure

$$P(t) = P_0 + P_{s0}(1-\frac{t}{t_d})e^{-b\frac{t}{t_d}} \quad (۱)$$

در رابطه (۱): t_d مدت‌زمان دوام فاز مثبت و b پارامتر شکل موج نامیده می‌شود که تابعی از فشار حداکثر P_{S0} می‌باشد. مساحت زیر نمودار فشار- زمان، ضربه نامیده می‌شود. ضربه مهم‌ترین عامل ایجاد خسارت در سازه است. بخش اعظم ضربه در فاز مثبت اتفاق می‌افتد که می‌توان به‌صورت رابطه (۲) آن را محاسبه کرد:

$$i_s = \int_{t_A}^{t_A+t_d} P(t)dt \quad (۲)$$



شکل ۲. منحنی تاریخچه زمانی فشار موج انفجار[۲۹].

تمامی پارامترهای موج انفجار را می‌توان بر اساس نمودارهای موجود در آیین‌نامه UFC 3-340-2 [۳۰] با توجه به وزن، فاصله محل انفجار تا سازه، زاویه برخورد موج انفجار به سازه و همچنین نوع انفجار به‌دست آورد. نوع انفجار با توجه به فاصله موج انفجار از زمین به دو صورت کلی انفجار هوایی و سطحی تقسیم می‌شود. انفجار هوایی در بالای سازه اتفاق می‌افتد و میان منبع مواد منفجره و سازه هیچ‌گونه تقویت موج شوک اولیه وجود ندارد. امواج انفجار در این حالت به‌صورت کروی در هوا منتشر می‌شوند. انفجاری که روی سطح زمین یا بسیار نزدیک به سطح زمین رخ می‌دهد، انفجار سطحی نامیده می‌شود. در انفجار سطحی موج اولیه انفجار به نقطه انفجار منعکس شده و با امواج دیگر ناشی از انفجار ادغام شده و یک موج نیمکره‌ای مجزای تقویت‌شده را به‌وجود می‌آورد. انفجار سطحی در بین انواع انفجارها بیشترین احتمال وقوع را دارد و نیروی فشاری ناشی از آن نیز بیشتر از انواع دیگر است.

در آیین‌نامه UFC 3-340-2، وزن شارژ به‌صورت معادل وزنی انرژی TNT مشخص می‌شود تا یک روش مقایسه پیوسته برای تمامی انفجارها ارائه دهد. در صورتی‌که ماده منفجره TNT نباشد، با استفاده از رابطه زیر می‌توان وزن معادل TNT آن را به‌دست آورد [۳۰]:

$$W_E = \frac{H^d_{\exp}}{H^d_{TNT}} \times W_{\exp} \quad (۳)$$

در این رابطه، W_E وزن معادل TNT، $W_{\exp}$ وزن ماده منفجره موردنظر، $H^d_{\exp}$ گرمای انفجار مربوط به ماده منفجره و H^d_{TNT} گرمای انفجار مربوط به TNT می‌باشد. به‌عنوان نمونه گرمای حاصل از انفجار برخی از مواد منفجره در جدول (۱) آورده شده است.

جدول ۱. گرمای انفجار تعدادی از مواد منفجره [۳۰].

ماده منفجره	گرمای انفجار (ft-lb/lb)
TNT	۱/۹۷×۱۰^۶
C4	۲/۲۲×۱۰^۶
RDX	۲/۲۷×۱۰^۶
HMX	۲/۲۷×۱۰^۶
PBX-9407	۲/۲۴×۱۰^۶

سپس به‌منظور لحاظ نمودن هم‌زمان اثر وزن و فاصله انفجار و مقایسه بین حالت‌های ممکن از پارامتر Z به‌صورت رابطه (۴) استفاده می‌شود [۱]:

$$Z = \frac{R}{W^{1/3}} \quad (۴)$$

در این رابطه، R فاصله نقطه انفجار از سازه برحسب فوت (ft) یا متر، W وزن شارژ (انفجار) برحسب پوند (lb) یا کیلوگرم بسته به سیستم یکای مورد استفاده است. با در نظر گرفتن نمودارهای فشار انفجار برحسب فاصله مقیاس شده از UFC 3-340-2 [۱۷]، به‌صورت تقریبی این نتیجه حاصل می‌شود که فشار انفجار دارای رابطه خطی با وزن شارژ و رابطه معکوس با مکعب فاصله نقطه انفجار از سازه می‌باشد [۱]. به این معنی که دو برابر کردن وزن شارژ، تقریباً باعث دو برابر شدن فشار انفجار در فاصله ثابت از سازه می‌شود. همچنین در وزن شارژ ثابت با دو برابر کردن فاصله، فشار موج انفجار تقریباً ۸ برابر کاهش می‌یابد. با توجه به مقدار Z و در نظر گرفتن واحد $\frac{ft}{lb^{1/3}}$ برای آن، می‌توان نوع انفجار را به این‌صورت دسته‌بندی کرد که انفجار دور[1] برای $Z > ۱۰$، انفجار نزدیک[2] برای $۳ < Z < ۱۰$ و انفجار در محل[3] برای $Z < ۳$ را در نظر گرفت [۱]. انفجار دور در اثر انفجار با فاصله به اندازه کافی از ساختمان رخ می‌دهد، به‌طوری‌که موج انفجاری که به ساختمان می‌رسد فشار تقریباً ثابت بر روی عناصر سازه‌ای وارد می‌کند. در انفجار نزدیک به‌علت فاصله کم محل انفجار تا سازه، عناصر سازه‌ای بارگذاری انفجار متغیر را تجربه می‌کنند. انفجار در محل، باعث ایجاد بار انفجار با شدت زیاد و به‌صورت موضعی می‌شود که پاسخ‌های سازه شامل خرد شدن بتن، خرابی مستقیم برشی و پدیده انتشار موج است که می‌تواند باعث شکست کششی در امتداد ضخامت بتن شود [۱].

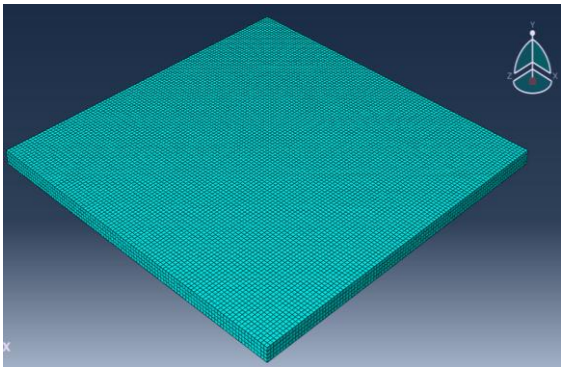
در این تحقیق به‌منظور لحاظ کردن اثر انواع انفجار و خرابی‌های ناشی از آن در دیوار حائل بتنی از نرم‌افزار آباکوس [۳۱] استفاده شده است. آباکوس یکی از قوی‌ترین نرم‌افزارهای عددی با روش حل اجزاء محدود است که قادر به حل مسائلی با

[1] Far field
[2] Near field
[3] Close-in

طیف گسترده از یک تحلیل خطی نسبتاً ساده تا تحلیل‌های غیرخطی بسیار پیچیده است. آباکوس شامل کتابخانه‌ای گسترده از اجزاء مختلف می‌باشد که بر اساس آن می‌توان هر نوع هندسه‌ای را مدل‌سازی کرد. این نرم‌افزار شامل فهرستی از انواع مدل‌های رفتاری مواد مختلف است که در نتیجه آن می‌توان رفتار اغلب مصالح مانند فلزها، لاستیک، پلیمر، کامپوزیت، بتن، خاک، سنگ و غیره را شبیه‌سازی کرد.

۳. صحت‌سنجی

جهت اطمینان از صحت نتایج مدل‌سازی انفجار در آباکوس، کار وانگ و همکاران [۱۵] را که شامل مدل آزمایشگاهی و شبیه‌سازی توسط نرم‌افزار آتودین است در آباکوس مدل‌سازی شده و نتایج حاصل با یکدیگر مقایسه شده‌اند. وانگ و همکاران به‌منظور انجام آزمایش، چهار دال یکسان با ابعاد ۱۰۰۰ در ۱۰۰۰ در ۴۰ میلی‌متر را تحت بارگذاری انفجار قرار دادند. بارگذاری انفجار نیز با مواد منفجره ۰/۲ تا ۰/۵۵ کیلوگرم TNT واقع در ۰/۴ متری بالای دال‌ها رخ داده است. مش‌بندی دال مدل شده در آباکوس در شکل (۳) قرار داده شده است. دال موردنظر بتن آرمه با مصالح بتن با مقاومت فشاری ۳۹/۵ مگاپاسکال و فولاد با تنش تسلیم ۶۰۰ مگاپاسکال است. در جدول‌های (۲) و (۳) مقایسه جابه‌جایی حداکثر در مرکز دال و نیز قطر حفره ایجادشده در هریک از نمونه‌ها آورده شده است. همچنین این نتایج شامل مشاهدات آزمایشگاهی و نتایج شبیه‌سازی در نرم‌افزار آتودین توسط وانگ و همکاران می‌باشد و نتایج شبیه‌سازی انجام‌شده در این پژوهش از نرم‌افزار آباکوس نیز قرار داده شده است. در شکل (۴) نیز کانتور وضعیت خرابی المان‌ها در دال شماره ۴ به همراه عکس دال مورد آزمایش قرار داده شده است. با توجه به نتایج به‌دست‌آمده و اینکه هدف مشاهده خرابی است، خروجی‌های آباکوس همپوشانی خوبی با نتایج آزمایش دارند. از این‌رو با نحوه مدل‌سازی که در بخش ۴ ارائه می‌شود، می‌توان دیوار پیش‌ساخته تحت بار انفجار را مدل‌سازی کرد.



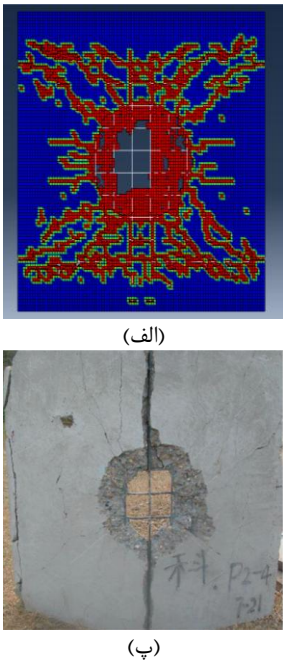
شکل ۳. مش‌بندی صورت گرفته برای دال در آباکوس با ابعاد مش برابر با ۱۰ سانتی‌متر.

جدول ۲. مقایسه نتایج جابه‌جایی مرکز دال در کار وانگ و شبیه‌سازی با آباکوس.

شماره دال	بار انفجار (Kg)	جابه‌جایی آزمایشگاهی (mm)	شبیه‌سازی جابه‌جایی در آتودین (mm)	شبیه‌سازی جابه‌جایی در آباکوس(mm)	درصد خطا با نتایج آزمایشگاهی	درصد خطا با نتایج شبیه‌سازی
۱	۰/۲	۱۰	۸	۱۱/۲	۱۲	۵۰
۲	۰/۳۱	۱۵	۱۳	۱۷	۱۳/۳	۳۱
۳	۰/۴۶	۳۵	۳۲	۳۷/۹	۸/۲	۱۸
۴	۰/۵۵	-	-	-	-	-

جدول ۳. مقایسه نتایج قطر حفره ایجادشده در دال در کار وانگ و شبیه‌سازی با آباکوس.

شماره دال	بار انفجار (Kg)	قطر حفره ایجادشده در آزمایش (mm)	قطر حفره ایجادشده در شبیه‌سازی وانگ (mm)	قطر حفره مدل‌سازی شده (mm)	درصد خطا با نتایج آزمایشگاهی	درصد خطا با نتایج شبیه‌سازی
۱	۰/۲	۰	۰	۰	۰	۰
۲	۰/۳۱	۹۰	۱۰۰	۱۰۰	۱۱/۱	۰
۳	۰/۴۶	۱۲۰	۱۴۰	۱۲۰	۰	۱۴/۳
۴	۰/۵۵	۱۵۰	۱۶۰	۱۵۰	۰	۶/۷



(الف)

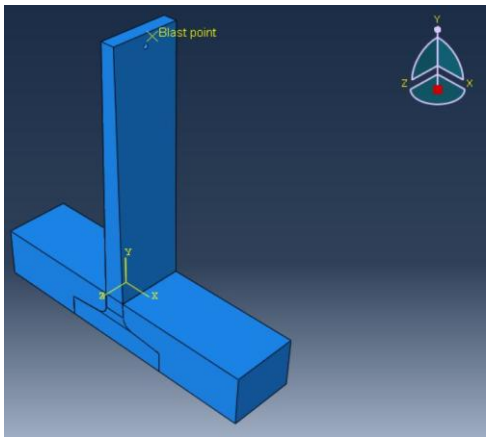
(پ)

شکل ۴. تصاویر دال شماره ۴، (الف) المان‌های تخریب‌شده در آباکوس، (ب) خرابی‌های به‌وجودآمده در دال در آزمایش وانگ [۱۵].

۴. شبیه‌سازی انفجار دیوار حائل بتنی

۴-۱. مدل‌سازی هندسی

دیوار مدل شده در آباکوس دارای ارتفاع کلی ۷ متر، پاشنه ۱/۵ متر در ۲/۵ متر با ضخامت متغیر ۰/۵ متر از لبه تا ۰/۶ متر در محل اتصال با قسمت عمودی دیوار است. ضخامت دیوار نیز به‌صورت متغیر از ۰/۳ متر در انتهای آن تا ۰/۵ می‌باشد. همچنین ۱/۲ متر دیوار را فرض شده که پوشیده از خاک است و طول ۳ متر از خاک در هر طرف دیوار مدل شده است. هندسه کلی دیوار و خاک مدل شده در آباکوس در شکل (۳) آورده شده است.



شکل ۵. هندسه مدل در آباکوس.

در قسمت شرایط تکیه‌گاهی، کف دیوار و خاک به‌صورت گیردار تعریف شده و سطوح کناری خاک متقارن نسبت به محور z و سطوح پشتی خاک متقارن نسبت به محور x مدل شده است. منظور از متقارن نسبت به محور z، مقید کردن جابه‌جایی در راستای محور z و چرخش در راستای محور x و y می‌باشد. منظور از متقارن نسبت به محور x نیز مقید کردن جابه‌جایی در راستای محور x و چرخش در راستای محور z و y می‌باشد.

۴-۲. مشخصات بتن

در آباکوس می‌توان به سه روش مدل بتن ترک‌اندود[1]، مدل آسیب پلاستیسیته بتن[2] و مدل ترک ترد[3] رفتار بتن را وارد کرد. تمامی این مدل‌ها قابلیت مدل‌سازی بتن در انواع سازه شامل تیرها، خرپاها، پوسته‌ها و اعضای توپر را دارند و می‌توانند برای مدل‌سازی بتن مسلح و بتن غیرمسلح استفاده شوند. مدل بتن ترک‌اندود برای کاربردهایی که در آنها بتن در معرض کرنش یکنواخت در فشارهای محدودکننده پائین قرار می‌گیرد طراحی شده است. بنابراین، با توجه به ماهیت غیریکنواخت تنش‌ها و کرنش‌ها در پدیده انفجار، از این مدل نمی‌توان استفاده کرد.

مدل آسیب پلاستیسیته برای کاربردهایی که بتن در معرض بارگذاری‌های یکنواخت، چرخه‌ای و یا دینامیکی قرار می‌گیرد طراحی شده است و در آن می‌توان اثرات سختی حین بارگذاری چرخه‌ای بازیابی کرد. در مدل ترک ترد فرض می‌شود که بتن در ناحیه فشاری در حالت الاستیک قرار دارد و خرابی بتن ناشی از ترک‌خوردگی کششی است. استفاده از این روش در بارگذاری‌های چرخه‌ای مانند زلزله نتایج درستی را نمی‌دهد زیرا در این نوع بارگذاری‌ها سازه متناوباً تحت کشش و فشار قرار می‌گیرد و حتی اگر سازه تحت کشش دچار خرابی هم شده باشد اما باز هم می‌تواند فشار را تحمل کند. بنابراین، در بار انفجار که چرخه‌ای نیست و در مدت‌زمان بسیار کوتاهی نسبت به نوسان طبیعی سازه رخ می‌دهد می‌توان از این روش استفاده کرد. از مزیت‌های این نوع مدل‌سازی، توانایی حذف المان بر اساس معیار گسیختگی ترد می‌باشد.

با توجه به مطالب ذکرشده می‌توان از هر دو مدل آسیب پلاستیسیته بتن و ترک ترد استفاده کرد. با توجه به اینکه هدف اینکار مشاهده خرابی دیوار تحت بارهای انفجار می‌باشد، برای مدل‌سازی بتن از مدل ترک ترد استفاده شده است. در مدل ترک ترد باید محدوده غیرالاستیک بتن، ضریب بقای برش[4] و کرنش شکست ترد[5] بتن در کشش وارد گردد. منظور از ضریب بقای برش، کاهش مقاومت برشی بتن در کشش پس از ترک‌خوردگی است. یکی از راهکارهایی که آباکوس برای وارد کردن این ضریب پیشنهاد می‌دهد در نظر گرفتن رابطه خطی است. به این‌صورت که ضریب بقای برش برابر با یک برای بتن در شروع لحظه ترک‌خورگی و صفر در هنگام شکست، متناظر با کرنش‌های ترک‌خوردگی و شکست در نظر گرفته شود. همچنین در مستندات آباکوس آورده شده است که منظور از کرنش شکست ترد بتن، در واقع همان کرنش ترک‌خوردگی یا حداکثر کرنش الاستیک بتن در کشش است. در فشار نیز فرض می‌گردد بتن در حالت الاستیک است و وارد کردن مدول الاستیسیته و ضریب پواسون کفایت می‌کند.

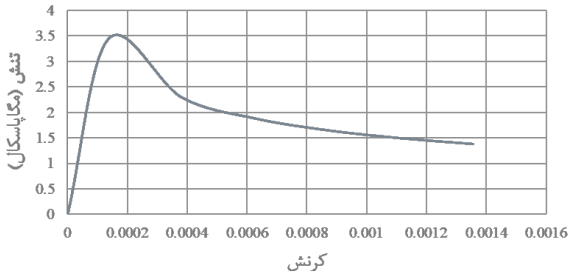
بتن الیافی شبیه‌سازی‌شده در این پژوهش، دارای الیاف فولادی با طول ۶۰ میلی‌متر، قطر ۰/۹۲ میلی‌متر، مقاومت کششی ۱۱۱۶ مگاپاسکال و مدول الاستیسیته ۲۱۰ گیگاپاسکال می‌باشد [۳۲]. همچنین در مدل‌سازی بتن الیافی، الیاف‌های فولادی مدل نشده‌اند ولی اثر آن‌ها در مدول الاستیسیته و نمودار تنش-کرنش بتن الیافی در کشش دیده شده است. مشخصات بتن مورد استفاده در دیوار بتن آرمه و بتن الیافی در دیوار بتنی بدون آرماتور در

[1] Smeared crack concrete model
[2] Concrete damaged plasticity model
[3] Brittle cracking
[4] Shear retention factor
[5] Brittle failure strain

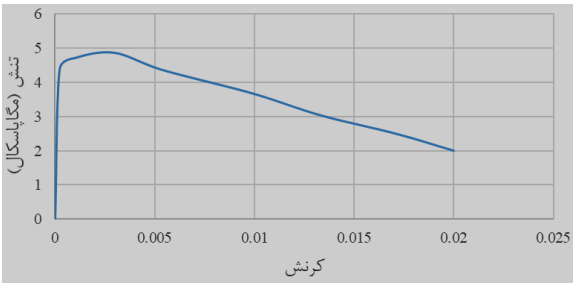
جدول (۴) آورده شده است. همچنین در مدل‌سازی بتن الیافی به‌منظور وارد کردن سایر پارامترهای لازم برای مدل‌سازی بتن، نمودار تنش-کرنش بتن عادی و بتن الیافی در کشش در شکل‌های (۶) و (۷) آورده شده است. بر اساس این شکل‌ها، در جدول (۵)، مشخصات قسمت غیرخطی نمودار تنش-کرنش در کشش و در جدول (۶) ضریب بقای برش و کرنش شکست ترد بتن عادی و الیافی که باید در آباکوس وارد شوند، ارائه شده است.

جدول ۴. مشخصات الاستیک و چگالی بتن عادی [۳۳] و الیافی موردنظر [۳۲].

مصالح	مقاومت فشاری (MPa)	مدول الاستیسیته (MPa)	ضریب پواسون	چگالی (kg/m^3)
بتن عادی	۳۰	۲۵۱۰۰	۰/۲	۲۴۰۰
بتن الیافی	۶۰	۳۲۷۰۰	۰/۲	۲۴۰۰



شکل ۶. منحنی تنش-کرنش بتن عادی در کشش با مقاومت فشاری ۳۰ مگاپاسکال [۳۴].



شکل ۷. منحنی تنش-کرنش بتن الیافی در کشش با مقاومت فشاری ۶۰ مگاپاسکال[۳۲].

همچنین جهت مدل‌سازی بتن از المان‌های هشت‌گرهی (C3D8R) توپر استفاده شده که جزء خانواده تنش سه‌بعدی و تابع شکل با درون‌یابی خطی می‌باشد و نوع انتگرال‌گیری از آن کاهش‌یافته است. این المان از کتابخانه المان‌های با حل صریح است. این نوع المان قابلیت لحاظ کردن تغییرشکل‌های پلاستیک و ترک‌خوردگی در سه جهت متعامد در هر نقطه انتگرال‌گیری را دارا می‌باشد. ابعاد مش در نظر گرفته‌شده برای دیوار نیز ۰/۱ متر می‌باشد.

جدول ۵. مشخصات قسمت غیرخطی نمودار تنش-کرنش بتن عادی و الیافی موردنظر جهت مدل‌سازی رفتار آن‌ها در آباکوس.

بتن الیافی		بتن عادی	
کرنش غیر الاستیک	تنش (MPa)	کرنش غیرالاستیک	تنش (MPa)
۰	۴/۳۹	۰	۳/۴۵
۰/۰۰۲۷۴	۴/۸۶	۰/۰۰۰۲۹	۲/۳
۰/۰۰۵۱۶	۴/۳۶	۰/۰۰۰۵۵	۱/۸۸
۰/۰۰۹۶۳	۳/۶۸	۰/۰۰۰۸۰	۱/۶۵
۰/۰۱۳۱	۳/۰۳	۰/۰۰۱۱	۱/۵
۰/۰۱۹۷۷	۲	۰/۰۰۱۳	۱/۳۸

جدول ۶- ضریب بقای برش و کرنش شکست ترد بتن عادی و الیافی موردنظر جهت مدل‌سازی رفتار آن‌ها در آباکوس.

مصالح	کرنش غیرالاستیک	ضریب بقای برش	کرنش شکست ترد
بتن عادی	۰	۱	۰/۰۰۰۱۳۸
	۰/۰۰۱۳	۰	
بتن الیافی	۰	۱	۰/۰۰۲۹۷
	۰/۰۱۹۷۷	۰	

۴-۳. مشخصات فولاد

در مدل‌سازی فولاد، مدل رفتاری به‌صورت الاستیک- پلاستیک در نظر گرفته شده است. در این مدل، رفتار فولاد قبل از رسیدن به تنش تسلیم به‌صورت کاملاً الاستیک و خطی بوده و پس از آن تا رسیدن به تنش حد گسیختگی به‌صورت پلاستیک و غیرخطی است. مشخصات فولاد مدل شده در آباکوس در جدول‌های (۷) و (۸) آورده شده است. برای تعیین اندرکنش بین میلگردها و بتن در سازه بتن آرمه، میلگردها به‌صورت مدفون[1] در بتن در نظر گرفته شده‌اند. جهت مدل‌سازی آرماتورها از المان‌های دو گرهی میله‌ای B31 با درون‌یابی خطی، استفاده شده است. این المان از کتابخانه المان‌های با حل صریح است. طول مش‌ها نیز ۰/۲ متر می‌باشد.

جدول ۷. مشخصات الاستیک و چگالی فولاد A615 [۳۳].

مصالح	مدول الاستیسیته (GPa)	ضریب پواسون	چگالی (kg/m^3)
فولاد A615	۲۰۰	۰/۳	۷۸۵۰

جدول ۸. مشخصات منحنی تنش-کرنش فولاد A615 در قسمت غیرالاستیک.

کرنش غیرالاستیک	تنش (MPa)
۰	۴۲۰
۰/۰۲۲۴۶	۵۴۶
۰/۰۶۴۳۷	۶۴۴
۰/۱۰۶۴۹	۶۹۸
۰/۱۴۸۶۹	۷۳۷
۰/۱۶۹۸۰	۷۵۴
۰/۲۱۲۰۶	۷۸۲

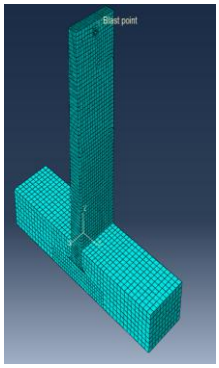
[1] Embedded region

۴-۴. مشخصات خاک

خاک مدل شده در آباکوس، به‌صورت خاک ماسه‌ای در نظر گرفته شده است. برای مدل‌سازی رفتار پلاستیک خاک نیز از معیار مور- کولمب استفاده شده است. در جدول (۹) پارامترهای لازم برای مدل‌سازی خاک در آباکوس آورده شده است. برای تعریف اندرکنش بین خاک و بتن، ضریب اصطکاکی مماسی برابر با ۰/۴۷ و رفتار عمودی بتن و خاک در تماس با یکدیگر به‌صورت تماس جسم سخت تعریف شده است [۳۵]. جهت مدل‌سازی خاک از المان‌های هشت‌گرهی (C3D8R) توپر استفاده شده است. مش‌بندی مدل در شکل (۸) نشان داده شده است. ابعاد مش مورد استفاده برای مدل‌سازی خاک نیز ۰/۱۵ متر می‌باشد.

جدول ۹. مشخصات الاستیک و پلاستیک خاک موردنظر [۳۵].

مصالح	مدول الاستیسیته (MPa)	ضریب پواسون	چگالی (kg/m^3)	زاویه اصطکاک (درجه)	زاویه اتساع (درجه)
خاک	۸۰	۰/۳	۱۸۰۰	۳۵	۵



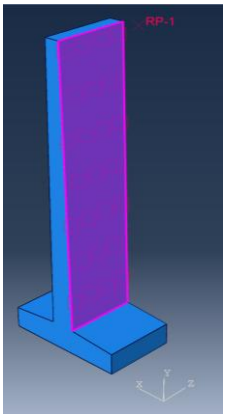
شکل ۸. مش بندی مدل کامل.

۴-۵. مدل‌سازی انفجار

وارد کردن بار انفجار در آباکوس به دو صورت امکان‌پذیر است. در روش اول، بایستی بار انفجار را معادل‌سازی و به‌صورت بار فشاری تبدیل نموده و سپس بر وجه رو به انفجار مدل اعمال کرد. در روش دوم، مقدار TNT به‌صورت مستقیم در نرم‌افزار آباکوس وارد می‌شود. در صورتی‌که ماده منفجره TNT نباشد، بایستی با توجه به جدول (۱) و رابطه (۳) وزن معادل آن را در آباکوس وارد کرد. سپس محل انفجار و وجه رو به انفجار مدل مشخص می‌شود. مزیت این روش، محاسبه فشار انفجار وارد بر سازه توسط نرم‌افزار و امکان تغییر فواصل انفجار از سازه با تغییر مختصات نقطه مرجع[1] (نشان‌دهنده محل اثر بار انفجار) است. در این روش فقط فاز مثبت انفجار در نظر گرفته می‌شود که با توجه به شکل (۲) که بیشتر ضربه وارد بر سازه، مساحت زیر نمودار فشار- زمان، در فاز مثبت رخ می‌دهد، نتایج حاصل از استفاده از این روش همپوشانی خوبی با نتایج آزمایشگاهی دارد. در این پژوهش از روش دوم برای تعریف بار انفجار و اعمال آن به مدل استفاده شده است.

در روش دوم می‌توان دو نوع انفجار در هوا[2] با موج انتشار کروی و انفجار سطحی[3] با موج انتشار نیمکره را مدل‌سازی کرد. در اینکار برای انفجارهای واقع در بالاترین نقطه سازه، انفجار در هوا و انفجارهای واقع بر سطح زمین، انفجار سطحی در نظر گرفته شده است.

در شکل (۹) سطح رو به انفجار و محل انفجار نشان داده شده است. بنابراین، برای مدل‌سازی انفجار در آباکوس، وزن ماده منفجره به همراه نوع انفجار (انفجار در هوا یا سطحی) ابتدا مشخص می‌شود. سپس مطابق شکل (۹) نقطه اثر انفجار و سطح رو به انفجار در دیوار حائل مشخص می‌شود.



شکل ۹. تصویر نمونه از تعیین نقطه اثر انفجار و سطح رو به انفجار دیوار حائل در نرم‌افزار آباکوس.

۴-۶. تجزیه و تحلیل عددی

در این بخش تأثیر مواد منفجره TNT و C4 در فواصل مختلف و با خرج‌های متفاوت بر دیوار حائل بتن آرمه و بتن الیافی با مشخصات ذکرشده بررسی می‌گردد. با توجه به این‌که در آباکوس تنها مدل‌سازی انفجار TNT امکان‌پذیر است، به‌منظور مدل‌سازی ماده منفجره C4 از وزن معادل TNT آن استفاده شده است. برای بررسی تأثیر محل ماده منفجره علاوه بر تغییر فاصله افقی از دیوار، مواد منفجره یکبار در راستای بالاترین نقطه دیوار و بار دیگر در راستای محل اتصال دیوار و زمین در نظر گرفته شده‌اند. در مدل‌سازی آباکوس نیز از معادلات انفجار در هوا برای انفجار در بالاترین نقطه دیوار و معادلات انفجار سطحی برای انفجار در محل اتصال دیوار و زمین استفاده شده است.

تصاویر مربوط به انفجار در فواصل چسبیده به دیوار و یک متری از دیوار در راستای بالاترین نقطه دیوار و محل اتصال دیوار

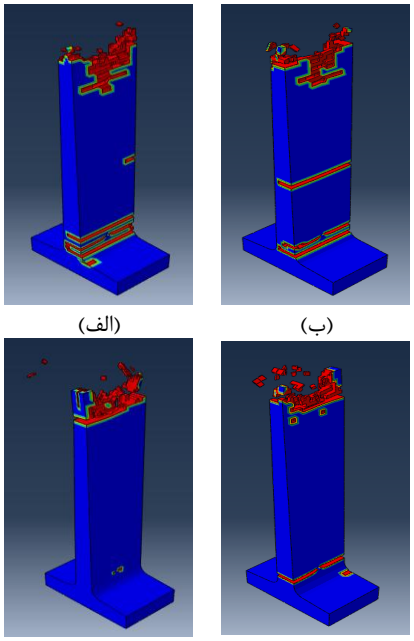
[1] Reference point

[2] Air blast

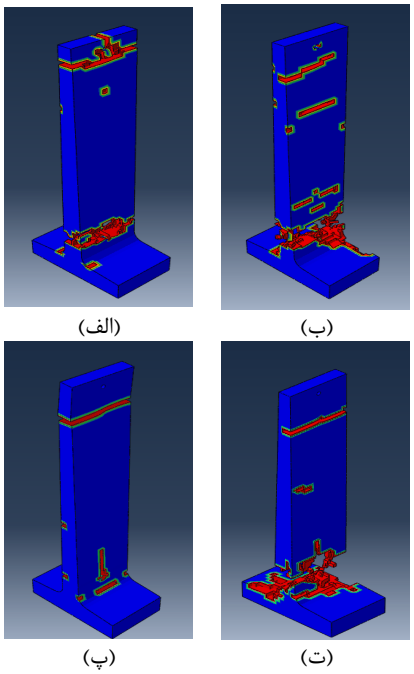
[3] Surface blast

و زمین در شکل‌های (۱۰) تا (۱۳) آورده شده است. با توجه به اینکه در این تحقیق تخریب دیوار حائز اهمیت است، در این شکل‌ها فقط تصاویر دیوار تخریب‌شده نشان داده شده است، رنگ آبی نشان‌دهنده المان‌های سالم، رنگ قرمز المان‌های در حال تخریب است و المان‌های تخریب‌شده نیز با توجه به مدل‌سازی خرابی بتن از روش ترک ترد، توسط نرم‌افزار حذف شده‌اند. در انفجار در فاصله ده متری از دیوار برخلاف انفجار چسبیده و در فاصله یک متری دیوار، خرابی‌های جزئی رخ نمی‌دهد. برش پایه زیادی در محل اتصال دیوار به پاشنه وارد می‌شود و سازه دیوار دچار تغییرشکل‌های زیادی می‌گردد. به همین دلیل در این بخش تصاویر مربوط به انفجار در فاصله ده متری آورده نشده است و در بخش ۵ با توجه به سطح عملکردی دیوار، خرابی آن بررسی می‌شود.

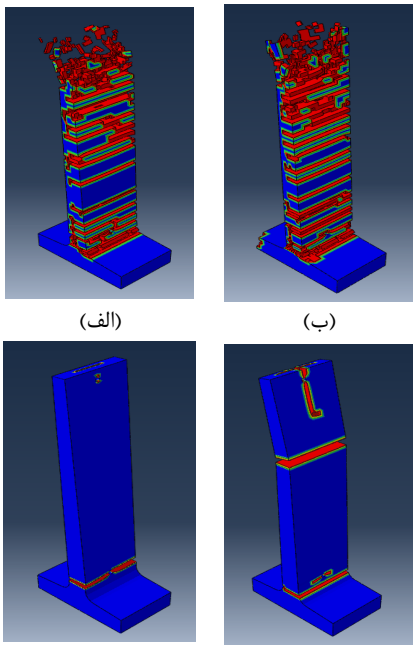
در شکل (۱۰) تصاویر خرابی‌های دیوار بتن آرمه و بتن الیافی تحت بارهای انفجاری C4 و TNT تخریب‌کننده دیوار در انفجار در بالاترین نقطه دیوار و چسبیده به آن آورده شده است. با توجه به اینکه در این حالت ماده منفجره به دیوار چسبیده است، همان‌گونه که از شکل‌ها مشخص است، تخریب به‌صورت موضعی و در محل انفجار رخ می‌دهد و همچنین به‌علت برش پایه وارد بر دیوار در اثر انفجار، در محل اتصال دیوار به پاشنه نیز خرابی جزئی به‌صورت ترک‌خوردگی و از بین‌رفتن المان‌ها رخ می‌دهد. در شکل (۱۱) نیز تصاویر خرابی‌های دو دیوار موردنظر تحت بارهای انفجاری C4 و TNT منجر به تخریب آن‌ها در انفجار در محل اتصال دیوار و زمین و چسبیده به آن آورده شده است. در این حالت خرابی در محل اتصال دیوار و پاشنه و انتهای دیوار رخ می‌دهد. در شکل‌های (۱۲) و (۱۳) مشابه با شکل‌های (۱۰) و (۱۱)، تصاویر خرابی‌های دیوار تحت انفجار C4 و TNT به ترتیب در بالاترین نقطه دیوار و محل اتصال دیوار و زمین در فاصله یک متری از دیوارها آورده شده است. با توجه به این شکل‌ها می‌توان به این نتیجه رسید که خرابی‌های دیوار بتن آرمه در فاصله یک متری، به‌دلیل وجود آرماتورها به‌صورت خرد شدن به قطعات کوچک در کل ارتفاع دیوار رخ می‌دهد. در دیوار بتن الیافی دیوار به‌صورت قطعات درشت تخریب می‌شود، چرا که هرچند الیاف فولادی مانع از تشکیل ترک‌های ریز در کل دیوار بتن الیافی می‌شود ولی به‌دلیل عدم وجود آرماتور در دیوار این نوع تخریب رخ می‌دهد. با توجه به شکل‌های (۱۰) تا (۱۳) این نتیجه حاصل می‌شود که دیوار بتن آرمه هرچند مقاومت کمتری نسبت به دیوار بتن الیافی در انفجار دارد، اما به‌دلیل وجود آرماتور در آن شکل‌پذیری بیشتری داشته و در انفجار به قطعات ریزتری تقسیم می‌شود.



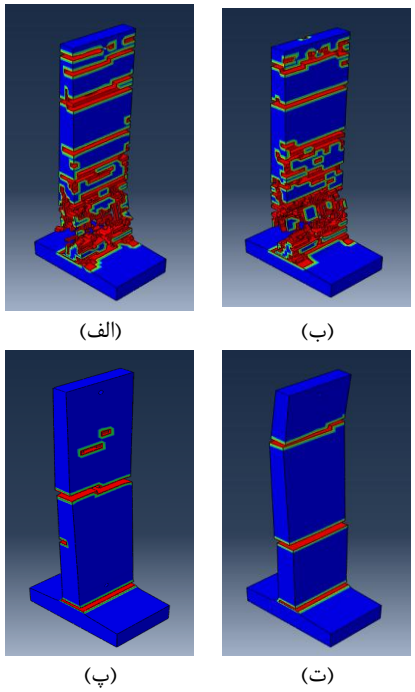
شکل ۱۰. تصاویر تخریب دیوار حائل در انفجار در بالاترین نقطه دیوار و فاصله چسبیده آن: (الف) دیوار بتن آرمه تحت بار ۱۵ کیلوگرم C4، (ب) تخریب دیوار بتن آرمه تحت بار ۱۵ کیلوگرم TNT، (پ) دیوار بتن الیافی تحت بار ۱۵ کیلوگرم C4، (ت) دیوار بتن الیافی تحت بار ۲۰ کیلوگرم TNT.



شکل ۱۱. تصاویر تخریب دیوار حائل در انفجار در محل اتصال دیوار و زمین و فاصله چسبیده آن: (الف) دیوار بتن آرمه تحت بار ۵ کیلوگرم C4، (ب) دیوار بتن آرمه تحت بار ۱۰ کیلوگرم TNT (پ) دیوار بتن الیافی تحت بار ۵ کیلوگرم C4، (ت) دیوار بتن الیافی تحت بار ۱۰ کیلوگرم TNT.



شکل ۱۲. تصاویر تخریب دیوار حائل در انفجار در بالاترین نقطه دیوار و فاصله یک متری: (الف) دیوار بتن آرمه تحت بار ۲۰ کیلوگرم C4، (ب) دیوار بتن آرمه تحت بار ۲۰ کیلوگرم TNT، (پ) دیوار بتن الیافی تحت بار ۲۰ کیلوگرم C4، (ت) دیوار بتن الیافی تحت بار ۲۵ کیلوگرم TNT.

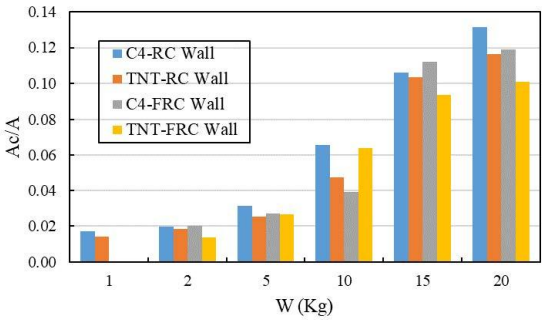


شکل ۱۳. تصاویر تخریب دیوار حائل در انفجار در محل اتصال دیوار و زمین و فاصله یک متری: (الف) تخریب دیوار بتن آرمه تحت بار ۱۵ کیلوگرم C4، (ب) تخریب دیوار بتن آرمه تحت بار ۱۵ کیلوگرم TNT، (پ) تخریب دیوار بتن الیافی تحت بار ۱۵ کیلوگرم C4، (ت) تخریب دیوار بتن الیافی تحت بار ۱۵ کیلوگرم TNT.

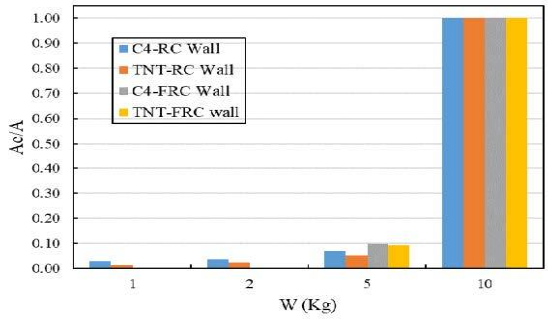
۵. نتایج و بحث

پس از مدل‌سازی و گرفتن خروجی‌های آباکوس، نتایج به دو بخش تقسیم می‌گردند. در بخش اول برای انفجارهای مختلف در فواصل چسبیده به دیوار و یک متری از دیوار، نتایج بر اساس نسبت مساحت تخریب‌شده به مساحت کل ارائه شده است. این نتایج برای ماده منفجره چسبیده به دیوار در شکل‌های (۱۴) و (۱۵)، به ترتیب برای انفجار واقع در بالاترین نقطه دیوار و انفجار واقع در محل اتصال دیوار و زمین ارائه شده است. در شکل‌های (۱۶) و (۱۷) نیز برای ماده منفجره در فاصله یک متری از دیوار، نتایج به ترتیب برای انفجار واقع در بالاترین نقطه دیوار و انفجار واقع در محل اتصال دیوار و زمین آورده شده است. در این شکل‌ها محور قائم بیانگر نسبت مساحت تخریب‌شده به مساحت سطح رو به انفجار دیوار (A_c/A) است. محور افقی نیز بیانگر وزن ماده منفجره برحسب کیلوگرم است.

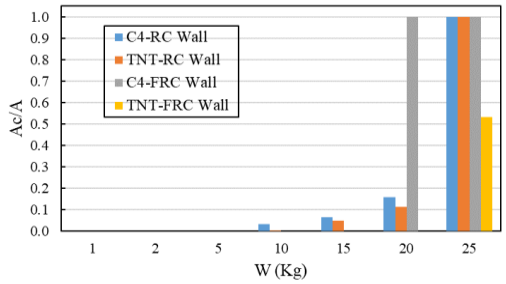
در این قسمت بار انفجاری که منجر به خرابی (نسبت مساحت تخریب‌شده به مساحت کل) بیش از ده درصد شود، به‌عنوان عامل تخریب دیوار در نظر گرفته شده است.



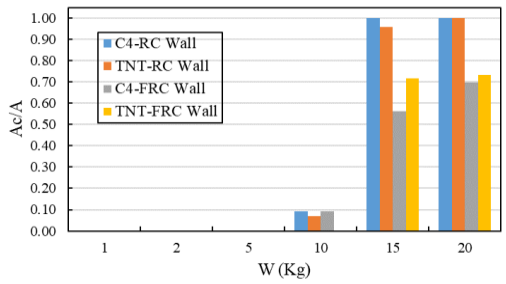
شکل ۱۴. نتایج انفجار در بالاترین نقطه دیوار و در فاصله چسبیده به آن بر اساس، نسبت مساحت تخریب‌شده به مساحت کل (A_c/A) و تغییر خرج انفجار (W).



شکل ۱۵. نتایج انفجار در محل اتصال دیوار و زمین و در فاصله چسبیده به آن، بر اساس نسبت مساحت تخریب‌شده به مساحت کل (A_c/A) و تغییر خرج انفجار (W).



شکل ۱۶. نتایج انفجار در بالاترین نقطه دیوار و در فاصله یک متری، بر اساس نسبت مساحت تخریب‌شده به مساحت کل (A_c/A) و تغییر خرج انفجار (W).



شکل ۱۷. نتایج انفجار در محل اتصال دیوار و زمین و در فاصله یک متری، بر اساس نسبت مساحت تخریب‌شده به مساحت کل (A_c/A) و تغییر خرج انفجار (W).

با توجه به نمودارهای شکل‌های (۱۴) تا (۱۷)، این نتیجه حاصل می‌شود که انفجار در محل اتصال دیوار و زمین اثر تخریبی بیشتری نسبت به انفجار در بالاترین نقطه سازه دارد و همچنین دیوار بتن الیافی مقاومت بیشتری نسبت به دیوار بتن آرمه در برابر انفجار دارد.

در بخش دیگر، نتایج خرابی و سطح عملکردی دیوار حائل تحت بارهای انفجار مختلف در فاصله ۱۰ متری از دیوار بر اساس کتاب اسمیت [۱] ارائه شده است. این کار به این دلیل انجام شده که انفجار در فاصله ۱۰ متری از دیوار برخلاف انفجار چسبیده به دیوار و در فاصله یک متری به‌صورت موضعی عمل نمی‌کند و تخریب جزئی در بر ندارد. در این انفجار، برش پایه زیادی به دیوار وارد شده و تغییرشکل‌های بسیار بزرگی در دیوار اتفاق می‌افتد. به همین دلیل سطح عملکردی دیوار به‌منظور تعیین خرابی در نظر گرفته شده است.

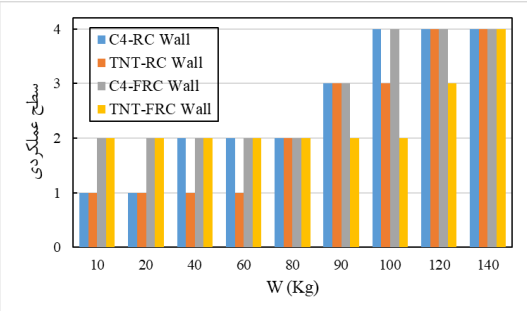
بر این اساس با توجه به آنکه دیوار حائل به‌صورت طره‌ای است، عملکرد دیوار حائل تحت انفجار به‌صورت تیر بتنی در معرض خمش فرض شده است و جدول (۱۰) به‌عنوان معیار بررسی خرابی بر اساس کتاب اسمیت [۱] در نتایج این بخش استفاده شده است. همچنین در جدول (۱۱) سطوح عملکردی متناظر با نوع خرابی سازه آورده شده است. نتایج مربوط به سطح عملکردی دیوار در اثر قرارگیری ماده منفجره در فاصله ۱۰ متری از دیوار در شکل‌های (۱۸) و (۱۹) به ترتیب برای انفجار در بالاترین نقطه دیوار و انفجار در محل اتصال دیوار و زمین آورده شده است. در این شکل‌ها با توجه به جدول (۱۱)، عدد ۱ بیانگر سطح عملکردی استفاده بی‌وقفه، عدد ۲ بیانگر ایمنی جانی، عدد ۳ بیانگر آستانه فروریزش و عدد ۴ بیانگر سطح عملکردی لحاظ نشده است. در این تحقیق مقدار ماده منفجره به‌وجود آورنده سطح عملکردی لحاظ نشده به‌عنوان عامل تخریب دیوار در نظر گرفته شده است.

جدول ۱۰. دسته‌بندی انواع خرابی در تیر بتنی تحت خمش بر اساس کتاب اسمیت [۱].

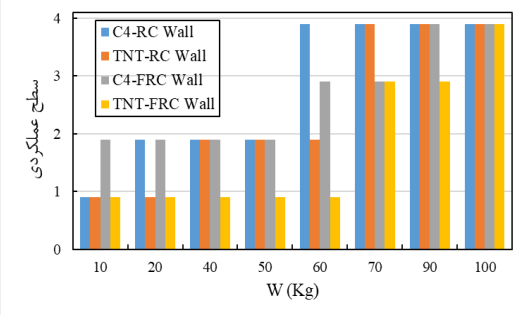
نوع خرابی	چرخش حداکثر (درجه)	شکل‌پذیری حداکثر
سطحی	–	۱
میانه	۲	–
سنگین	۵	–
لحاظ نشده	۱۰	–

جدول ۱۱. دسته‌بندی سطوح عملکردی بر اساس کتاب اسمیت [۱].

خرابی	سطح عملکردی	عدد متناظر با سطح عملکردی
سطحی	استفاده بی‌وقفه	۱
میانه	ایمنی جانی	۲
سنگین	آستانه فروریزش	۳
خطرناک	لحاظ نشده	۴



شکل ۱۸. نتایج انفجار در بالاترین نقطه دیوار و در فاصله ده متری بر اساس سطح عملکردی با افزایش وزن ماده منفجره.



شکل ۱۹. نتایج انفجار در محل اتصال دیوار و زمین و در فاصله ده متری بر اساس سطح عملکردی با افزایش وزن ماده منفجره.

با توجه به شکل (۱۸)، بار انفجار ۱۲۰ کیلوگرم TNT و ۱۰۰ کیلوگرم C4 منجر به تخریب دیوار بتن آرمه در فاصله ده متری و در بالاترین نقطه دیوار شده است. بار انفجار ۱۴۰ کیلوگرم TNT و ۱۰۰ کیلوگرم C4 نیز منجر به تخریب دیوار بتن الیافی شده است. با توجه به شکل (۱۹) نیز بار انفجار ۷۰ کیلوگرم TNT و ۶۰ کیلوگرم C4 در دیوار بتن آرمه و بار انفجار ۱۰۰ کیلوگرم TNT و ۹۰ کیلوگرم C4 نیز منجر به تخریب دیوار بتن الیافی در انفجار در فاصله ده متری و در راستای محل اتصال دیوار و زمین شده است. در انفجار در فاصله ده متری نیز مشابه با انفجار در فاصله چسبیده به دیوار و یک متری، انفجار سطحی (در راستای محل اتصال دیوار و زمین) با ماده منفجره کمتری منجر به تخریب دیوار شده است. همچنین ماده منفجره C4 با توجه به گرمای آزاد شده انفجار بیشتر نسبت به TNT اثر تخریب بیشتری دارد و با وزن کمتری نسبت به TNT قابلیت تخریب دیوار را دارد.

با توجه به نتایج به‌دست‌آمده می‌توان به این نتیجه رسید که استفاده از دیوار بتن الیافی با مسلح کردن آن به آرماتورهای فولادی، باعث افزایش مقاومت دیوار در برابر انفجار می‌شود. دلیل این امر نیز افزایش مقاومت بتن در کشش با استفاده از الیاف و جلوگیری از خرد شدن بتن به قطعات بزرگ به‌علت استفاده از آرماتورهای طولی و عرضی فولادی است. همچنین با توجه به تخریب دیوار در محل اتصال به پاشنه در انفجارهای مختلف در فاصله ده متری، می‌توان با استفاده از درصد آرماتورهای طولی و عرضی بیشتر در این ناحیه، دیوار حائل انسدادی را در برابر انفجار تقویت کرد.

۶. نتیجه‌گیری

در این پژوهش دیوار حائل بتن آرمه و بتن الیافی تحت اثر بار انفجار در فواصل مختلف مورد بررسی قرار گرفت. به این منظور در سه فاصله چسبیده به دیوار، یک متری و ده متری از دیوار با تغییر راستا و خرج انفجار، اثر تخریبی مواد منفجره TNT و C4 مورد بررسی قرار گرفت و نتایج زیر حاصل گردید:

۱) بارهای منجر به تخریب دیوار بتن آرمه در بالاترین نقطه سازه و در فواصل چسبیده به دیوار، ۱ متری و ۱۰ متری برای ماده منفجره TNT به ترتیب برابر ۱۵، ۲۰ و ۱۲۰ کیلوگرم و برای ماده منفجره C4 به ترتیب برابر ۱۵، ۲۰ و ۱۰۰ کیلوگرم می‌باشد.

۲) بارهای منجر به تخریب دیوار بتن آرمه در راستای محل اتصال دیوار و زمین و در فواصل چسبیده به دیوار، ۱ متری و ۱۰ متری به ترتیب برابر با ۱۰، ۱۵ و ۷۰ کیلوگرم برای ماده منفجره TNT و به ترتیب برابر ۵، ۱۵ و ۶۰ کیلوگرم برای ماده منفجره C4 می‌باشد.

۳) بارهای منجر به تخریب دیوار بتن الیافی بدون آرماتور در بالاترین نقطه سازه در فواصل چسبیده به دیوار، ۱ متری و ۱۰ متری به ترتیب برابر ۲۰، ۲۵ و ۱۴۰ کیلوگرم برای ماده منفجره TNT و به ترتیب برابر با ۱۵، ۲۰ و ۱۰۰ کیلوگرم برای ماده منفجره C4 می‌باشد.

۴) بارهای منجر به تخریب دیوار بتن الیافی بدون آرماتور در انفجار در محل اتصال دیوار و زمین در فواصل چسبیده به دیوار، ۱ متری و ۱۰ متری به ترتیب برابر ۱۰، ۱۵ و ۱۰۰ کیلوگرم برای ماده منفجره TNT و ۵، ۱۵ و ۹۰ کیلوگرم ماده منفجره C4 می‌باشد.

۵) بر اساس نتایج به‌دست‌آمده، انفجار در فواصل چسبیده به دیوار و یک متری به‌صورت موضعی عمل کرده و تخریب موضعی در پی دارد. انفجار در فاصله ده متری از دیوار، برخلاف انفجار در فواصل چسبیده به دیوار و یک متری، در دیوار خرابی موضعی ایجاد نمی‌کند و باعث تخریب دیوار در محل اتصال به پاشنه می‌شود.

۶) انفجار در راستای محل اتصال دیوار و زمین به‌علت انتشار نیم‌کره‌ای امواج انفجار نسبت به انفجار در بالاترین نقطه سازه به‌دلیل انتشار کروی امواج انتشار اثر تخریبی بیش‌تری دارد.

۷) در فاصله چسبیده به دیوار، خرج لازم برای تخریب دیوار بتن الیافی بین ۱ تا ۱/۳ برابر دیوار بتن آرمه است. در فاصله یک متری از دیوار، خرج لازم برای تخریب دیوار بتن الیافی بین ۱ تا ۱/۲۵ برابر دیوار بتن آرمه است. در فاصله ده متری از دیوار، خرج لازم برای تخریب دیوار بتن الیافی بین ۱ تا ۱/۵ برابر دیوار بتن آرمه است. در نتیجه دیوار بتن الیافی در پدیده انفجار، عملکرد بهتری نسبت به دیوار بتن آرمه از خود نشان می‌دهد. علت عملکرد بهتر دیوار بتن الیافی نسبت به بتن آرمه نیز، بهبود عملکرد بتن در کشش با اضافه کردن الیاف به آن و در نتیجه اضافه شدن مقاومت کششی بتن در تمامی قسمت‌های دیوار بتن الیافی و جلوگیری نسبی از رشد ترک‌ها و کنترل خرابی به‌وسیله الیاف‌های به‌کاررفته در بتن است.

۸) در دیوار بتن آرمه با تغییر فاصله محل انفجار از چسبیده به دیوار به فاصله یک متری، خرج لازم برای

تخریب دیوار بین ۱/۳ تا ۲ برابر با تغییر ماده منفجره و راستای انفجار افزایش می‌یابد. با تغییر فاصله محل انفجار از یک متری به ده متری دیوار، خرج لازم برای تخریب دیوار بین ۳ تا ۵ برابر افزایش می‌یابد.

۹) در دیوار بتن الیافی با جابجا کردن محل انفجار از فاصله چسبیده به دیوار به یک متری، خرج لازم برای تخریب دیوار بین ۱/۲۵ تا ۲ برابر افزایش می‌یابد. با تغییر محل انفجار از فاصله یک متری به ده متری، خرج لازم برای تخریب دیوار بین ۴ تا ۸ برابر افزایش می‌یابد.

۷. مرجع‌ها

[1] Smith, S. J.; McCann, D. M.; Kamara, M. E. "Blast Resistant Design Guide for Reinforced Concrete Structures"; Portland Cement Association, 2009.

[2] Mays, G. C.; Hetherington, J. G.; Rose, T. A. "Response to Blast Loading of Concrete Wall Panels With Openings"; J. Struct. Eng. 1999, 125, 1448–1450.

[3] Lok, T. S.; Xiao, J. R. "Steel Fibre Reinforced Concrete Panels Exposed to Air Blast Loading"; Proc. Inst. Civ. Eng. Build. 1999, 134, 319–331.

[4] Mosalam, K. M.; Mosallam, A. S. "Nonlinear Transient Analysis of Reinforced Concrete Slabs Subjected to Blast Loading and Retrofitted With CFRP Composites"; Compos. Part B Eng. 2001, 32, 623–636.

[5] Li, J.; Wu, C.; Hao, H. "Investigation of Ultra-High Performance Concrete Slab and Normal Strength Concrete Slab Under Contact Explosion"; Eng. Struct. 2015, 102, 395–408.

[6] Wang, W.; Zhang, D.; Lu, F.; Wang, S. C.; Tang, F. "Experimental Study on Scaling the Explosion Resistance of a One-Way Square Reinforced Concrete Slab Under Close-in Blast Loading"; Int. J. Impact Eng. 2012, 49, 158–164.

[7] Wu, C.; Oehlers, D. J.; Rebentrost, M.; Leach, J.; Whittaker, A. S. "Blast Testing of Ultra-High Performance Fibre and FRP-Retrofitted Concrete Slabs"; Eng. Struct. 2009, 31, 2060–2069.

[8] De Silva, R. V.; Pathegama Gamage, R.; Perera, A.; Samintha, M. "An Alternative to Conventional Rock Fragmentation Methods Using SCDA: A Review"; Energies. 2016, 9, 958-989.

[9] Luccioni, B. M.; Luege, M. "Concrete Pavement Slab Under Blast Loads"; Int. J. Impact Eng. 2006, 32, 1248–1266.

[10] Kamgar, R.; Shams, G. R. "Effect of Blast Load in Nonlinear Dynamic Response of the Buckling Restrained Braces Core"; J. Adv. Def. Sci. Technol. 2019, 9, 107–118 (In Persian).

[11] Lezgi, L. M.; Izadifard R. "Evaluation of Nonlinear Response of Reinforced Concrete Frames Designed According to Earthquake Codes and Subjected to Blast Loading"; J. Adv. Def. Sci. Technol. 2017, 8, 201–212 (In Persian).

[12] Kamgar, R.; Majidi, N.; Heidarzadeh, H. "Optimum Layout of Mega Buckling-Restrained Braces to Optimize the Behavior of Tall Buildings Subjected to Blast Load"; J. Adv. Def. Sci. Technol. 2020, 11, pp. 211–230 (In Persian).

[13] Tavakoli, R.; Kamgar, R.; Rahgozar, R. "The Best Location of Belt Truss System in Tall Buildings Using Multiple Criteria Subjected to Blast Loading,"; Civ. Eng. J. 2018, 4, 1338–1353.

[14] Sadrnejad, S. A.; Ziaei, M. "Behavior of Beam-Column Bolted End-Plate Connections Under Blast,"; J. Adv. Def. Sci. Technol. 2013, 4, 93–101(In Persian).

[15] Wang, W.; Zhang, D.; Lu, F.; Wang, S.; Tang, F. "Experimental Study and Numerical Simulation of the Damage Mode of Square Reinforced Concrete Slab Under Close-in Explosion"; Eng. Fail. Anal. 2013, 27, 41–51.

[16] Jain, S.; Tiwari, R.; Chakraborty, T.; Matsagar, V. "Dynamic Response of Reinforced Concrete Wall Under Blast Loading"; Indian Concr. J. 2015, 89, 27–41.

[17] Tavakoli, R.; Kamgar, R.; Rahgozar, R.; "Seismic Performance of Outrigger-Belt Truss System Considering Soil-Structure Interaction,"; Int. J. Adv. Struct. Eng. 2019, 11, 45–54.

[18] Kamgar, R.; Khatibinia, M.; "Optimization Criteria for Design of Tuned Mass Dampers Including Soil-structure Interaction Effect"; Int. J. Optim. Civil Eng. 2019, 9, 213–232.

[19] Kamgar, R.; Gholami, F.; Sanayei, H. R. Z.; Heidarzadeh, H.; "Modified Tuned Liquid Dampers for Seismic Protection of Buildings Considering Soil-Structure Interaction Effects"; Iran. J. Sci. Technol. Trans. Civ. Eng. 2020, 44, 339–354.

[20] Heidarzadeh, H.; Kamgar, R.; "Evaluation of the Importance of Gradually Releasing Stress Around Excavation Regions in Soil Media and the Effect of Liners Installation Time on Tunneling"; Geotech. Geol. Eng. 2020, 38, 2213–2225.

[21] Tavakoli, R.; Kamgar, R.; Rahgozar, R.; "Optimal Location of Energy Dissipation Outrigger in High-Rise Building Considering Nonlinear Soil-Structure Interaction Effects"; Period. Polytech. Civ. Eng. 2020.

[22] Baziar, M. H.; Rabeti Moghadam, M.; Gholipour, S; "Numerical Investigation of Gravity and Reinforced Soil Wall Performance Under Blast Loading,"; J. Adv. Def. Sci. Technol. 2012, 3, 259–267 (In Persian).

[23] Toy, A. T.; Sevim, B.; "Numerically and Empirically Determination of Blasting Response of a RC Retaining Wall Under TNT Explosive"; Adv. Concr. Constr. 2017, 5, 493–512.

[24] GuhaRay, A.; Mondal, S.; Mohiuddin, H. H.; "Reliability Analysis of Retaining Walls Subjected to Blast Loading By Finite Element Approach"; J. Inst. Eng. Ser. A. 2018, 99, no. 95–102.

[25] Foglar, M.; Hajek, R.; Fladr, J.; Pachman, J.; Stoller, J. "Full-Scale Experimental Testing of the Blast Resistance of HPFRC and UHPFRC Bridge Decks"; Constr. Build. Mater. 2017, 145, 588–601.

[26] Abeysinghe, T. M.; Tanapornraweekit, G.; Tangtermsirikul, S.; Pansuk, W.; Nuttayasakul, N. "Performance of Aramid Fiber Reinforced Concrete Panels Under Blast Loads"; Fourth Asian Conf. on Defence Technology-Japan 2017, 1–6.

[27] Yoo, D. Y.; Banthia, N. "Mechanical and Structural Behaviors of Ultra-High-Performance Fiber Reinforced Concrete Subjected to Impact and Blast"; Constr. Build. Mater. 2017, 149, 416–431.

[28] Dusenberry, D. O. "Handbook for Blast Resistant Design of Buildings"; John Wiley & Sons, 2010.

[29] Ngo, T.; Mendis, P.; Gupta, A.; Ramsay, J. "Blast Loading and Blast Effects on Structures: An Overview"; Electron. J. Struct. Eng. 2007, 7, 76–91.

[30] Unified Facilities Criteria (UFC 3-340-02) “Structures to Resist the Effects of Accidental Explotions”; US Department of Defence, Washington DC. 2008.

[31] Abaqus/Explicit V6.13. “User Manual”; Providence, RI, USA. Abaqus Inc. DS Simulia. 2013.

[32] Kwan, A. K. H.; Chu, S. H.; “Direct Tension Behaviour of Steel Fiber Reinforced Concrete Measured by a New Test Method”; Eng. Struct. 2018, 176, 324–336.

[33] A. C. I. Committee and I. O. for Standardization; “Building Code Requirements for Structural Concrete (ACI 318-08) and Commentary,”; 2008.

[34] Belarbi, T. H. A.; “Constitutive Laws of Concrete in Tension and Reinforcing Bars Stiffened by Concrete,”; Struct. J. 1994, 91.

[35] Helwany, S. “Applied Soil Mechanics With Abaqus Aapplications”; John Wiley & Sons, 2007.

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۳۸۹-۳۸۳

«علمی- پژوهش»

ارزش‌گذاری خطوط سامانه‌های توزیع برق جهت تسریع روند بازیابی و بهبود شاخص تاب‌آوری با در نظر گرفتن تولیدات پراکنده

حمیدرضا شریف مقدم[۱]، رضا دشتی[۲*]

۱- کارشناسی‌ارشد، ۲- استادیار، دانشگاه علم و صنعت ایران

(دریافت: ۹۸/۰۴/۳۰، پذیرش: ۹۸/۱۲/۱۹)

چکیده

برای افزایش میزان تاب‌آوری سامانه توزیع در برابر مخاطرات باید قبل از حادثه، ارزش دارایی‌های سامانه تحت کنترل با در نظر گرفتن فاکتورهای مختلف مشخص باشد تا در زمان بحران بازیابی بارهای ازدست‌رفته با سرعت و کیفیت بهتری انجام پذیرد. در این مقاله اساس مدل‌سازی بر مبنای قیمت است که در آن ارزش بار، جهت درنظر گرفتن اهمیت سمت تقاضا؛ نرخ خرابی، جهت بررسی دسترس‌پذیری خط؛ ارزش ذاتی خطوط، جهت درنظر گرفتن هزینه سرمایه‌گذاری و همچنین فاکتور توپولوژی، جهت تأکید بر آرایش شبکه مدنظر قرار داده شد. همچنین برای مشاهده تأثیر DG در ارزش‌گذاری خطوط شبکه، در دو حالت شبکه با DG و بدون DG مورد بررسی قرار گرفته شد. نتایج حاصل علاوه برنشان دادن حساسیت شبکه به عوامل اثرگذار، نشان می‌دهد اضافه کردن تولیدات پراکنده این پتانسیل رادار است تا رتبه‌بندی ارزش‌گذاری را تغییر دهد و در بهبود روند بازیابی شبکه توزیع مفید واقع شود.

کلیدواژه‌ها: تاب‌آوری، سامانه‌های توزیع، ارزش‌گذاری دارایی‌ها، پدافند غیرعامل، تولیدات پراکنده

Valuation of Distribution System Lines to Improve the Restoration Process and Enhance the Resilience Index with Considering DGs

H. Sharifmoghadam, R. Dashti*
Iran University of Science and Technology.
(Received: 21/07/2019; Accepted: 09/03/2020)

Abstract

In order to increase the resilience of distribution system against natural disaster and human attacks, before the events, the value of the monitored system assets should be identified according to different factors so that during the crisis, restoring of lost loads be done faster and qualitatively better. This paper is based on price-based modeling in which load value, to consider the importance of demand side; failure rate, line availability; intrinsic value of lines, to consider investment cost, as well as topology factor, to emphasize The configuration of grid was taken into consideration. In order to observe the impact of DG on the grid lines evaluation, it was investigated in two states: with and without DGs. The results, in addition to demonstrating the network sensitivity to the influential factors, show that distributed generation has a potential to change ranking of valuation and to help improve the process of restoring the distribution system.

Keywords: *Resilience, Distributed Networks, Asset Evaluation, Passive Defense, Distributed Generation.*

*Corresponding Author E-mail: rdashti@iust.ac.ir

۱. مقدمه

در دهه‌های گذشته پیشرفت‌های قابل‌توجهی در پیشبرد روش‌های تحلیل مسائل مرتبط با بلایای طبیعی در سامانه‌های قدرت انجام‌شده است. هم‌زمان، به سبب پیچیدگی و ماهیت بین‌رشته‌ای مسئله، فعالیت‌های تحقیقاتی پراکنده‌ای در حوزه‌های مختلف انجام‌شده است. مدل‌های مختلفی برای کاهش تأثیرگذاری شدید رویدادهای آب و هوایی بر سامانه‌های قدرت ارائه‌شده است؛ عملیات اصلاحی و پاسخ اضطراری، مقاوم‌سازی و مدل‌های آماده‌سازی قبل از طوفان و مدل‌های بازیابی که فعالیت‌های در حین و بعد از وقوع حوادث طبیعی را سازمان‌دهی می‌کند ازاین‌دست مدل‌ها هستند. ارزیابی تاب‌آوری یک سامانه توزیع قدرت برای اندازه‌گیری توانایی آن سامانه در پاسخ کارآمد و مؤثر ، پس از هر رویداد شدید آب و هوایی است. این رویدادهای شدید احتمالی و غیرقابل‌پیش‌بینی و دینامیک، عواقب پیچیده و دینامیکی نیز به دنبال خواهند داشت[۲-۱]. بااین‌حال رسیدن به یک اجماع در مورد تعریف و محدوده مفهوم تاب‌آوری مشکل است[۳]. طیف وسیعی از حوزه‌های که در آن مفهوم تاب‌آوری بررسی شده است، در منابع [۵-۴] آمده است.

در به‌کارگیری شاخص تاب‌آوری در شبکه‌ها، هر دو ویژگی توپولوژی شبکه و روند اولویت‌بندی بازیابی سامانه‌های توزیع، بر تاب‌آوری سامانه تأثیرگذار است[۷-۶]. علاوه بر این، پس از رخ دادن حادثه شدید، در بازیابی سامانه‌های توزیع و اولویت‌بندی تعمیر، تمایل به سمتی است که استراتژی بازیابی به دنبال جست‌وجوی بهترین گزینه، هم از منظر فنی و هم از دیدگاه اقتصادی باشد[۹-۸]. در مرجع[۱۰]، یک معیار وابسته به زمان از تاب‌آوری ارائه‌شده است که چندین طرح اولویت‌بندی بازیابی را موردبررسی قرار می‌دهد، این معیارهای تاب‌آوری برای ارزیابی رویه‌های کاهش شدت حادثه، تطبیق و یا استراتژی‌های مقاوم‌سازی در سامانه‌های توزیع قدرت در برابر حوادث شدید آب و هوایی به‌کاربرده شده است، در مرجع ذکرشده به‌منظور ارزش‌گذاری و انتخاب بهترین استراتژی بازیابی و سایر سرمایه‌گذاری‌های اقتصادی از یک مسئله بهینه‌سازی صحیح-مختلط بهره برده شده است. این مطالعه [۱۱] یک رویکرد مدل‌سازی عامل(ABM[1]) برای بهینه‌سازی روند بازیابی پس از طوفان است. ABM قادر به بازیابی پس از طوفان است و می‌تواند سناریوهای آینده را آزمایش کند. نویسندگان این مقاله دریافتند که پارامترهایی مانند تعداد قطع، محدوده زمانی تعمیر و تعداد کارکنان می‌تواند تا حد قابل‌توجهی بر زمان برآورد شده تا بازسازی(ETR[2]) تأثیر بگذارد، همچنین پارامترهای دیگر مانند مکان شروع به کار کارکنان و سرعت جابه‌جایی، تأثیرات جزئی بر روی ETR داشتند.

این مرجع [۱۲] یک استراتژی تقویت تاب‌آوری سامانه پس از رخداد شدید را با توجه به تعمیر قطعات آسیب‌دیده و دیسپاچینگ عملیاتی سامانه پیشنهاد می‌دهد. با توجه به نتایج حاصل از ارزیابی میزان آسیب وظایف مربوط به تعمیر، خروجی واحد و برنامه کلید زنی طراحی می‌شود. با ترکیب مسئله مسیریابی خودرو (VRP[3]) و مدل پخش بارDC به‌منظور کاهش تلفات خاموشی و ذخیره سریع منابع تأمین بار یک مسئله بهینه‌سازی صحیح- مختلط پیشنهاد می‌دهد.

اهمیت زمان در هنگام وقوع حادثه برای مدیریت هرچه بهتر بحران‌های آب و هوایی و تلاش برای به حداقل رساندن آسیب‌ها به مشترکین با در نظر گرفتن ملاحظات اقتصادی بر کسی پوشیده نیست. این مقاله اولویت دادن به خطوط شبکه‌های توزیع را مورد هدف قرار داده است تا با در نظر گرفتن پارامترهای فنی و اقتصادی اقدام به ارزش‌گذاری خطوط در دو حالت شبکه بدون تولیدات پراکنده و شبکه با تولیدات پراکنده کند. پیشرفت و حضور غیرقابل‌اجتناب تولیدات پراکنده نیز انگیزه‌ای بود تا تأثیرگذاری این تولیدات در ارزش‌گذاری خطوط به نمایش گذارده شود.

۲. روش تحقیق

اساس مدل‌سازی در اینجا بر مبنای قیمت است تا به هر خط ارزشی داده شود، این ارزش‌گذاری حاوی فاکتورهایی است که در ادامه به هر یک اشاره می‌شود.

۲-۱. ارزش بار

$$v_i = L(i) \times 8760 \times l_f(i) \times voll \qquad (۱)$$

در رابطه فوق L میزان بار مصرفی باسی است که به خط i متصل است، l_f شاخص ضریب بار است و $voll$ ارزش بار از دست رفته است.

۲-۲. نرخ خرابی یا تعمیر

خطوط توزیع برق از منظر دسترس‌پذیری نیز می‌بایست موردتوجه قرار گیرند. احتمالات مربوط به تعمیرات برنامه‌ریزی‌شده و

[1] Agent Based Modeling

[2] Estimated Time to Restoration

[3] Vehicle Routing Problem

خطاهای سالانه در این بخش موردتوجه قرار می‌گیرد. مجموعه این عوامل در رابطه (۲) نشان داده شده است، که دسترس‌ناپذیری یک خط با U_A نشان داده می‌شود.

$$U_A = \frac{f(i) \times r(i) + M_p(i)}{8760} \quad (۲)$$

در این رابطه، f نرخ خرابی در یک دوره یک‌ساله است، r مدت‌زمان میانگین تعمیر برحسب ساعت در طول یک دوره یک‌ساله و M_p مدت‌زمان تعمیرات برنامه‌ریزی‌شده برحسب ساعت است. با توجه به رابطه فوق دسترس‌پذیری خطوط از رابطه (۳) به‌دست می‌آید:

$$U_d = 1 - U_A \quad (۳)$$

۲-۳. ارزش ذاتی خطوط

ارزش ذاتی خطوط یا میزان سرمایه‌گذاری جهت احداث خط، یکی دیگر از عوامل تأثیرگذار در ارزش‌گذاری خطوط است. رابطه (۴) عوامل مؤثر بر این شاخص را به نمایش می‌گذارد.

$$int(i) = \frac{mv(i) \times cl(i)}{lt(i)} \quad (۴)$$

که در آن، intارزش ذاتی خط، mv هزینه سرمایه‌گذاری به ازای هر کیلومتر خط، cl طول هر خط برحسب کیلومتر و lt طول عمر خط برحسب ساعت است.

۲-۴. توپولوژی

می‌توان ادعا کرد که در این مقاله اساسی‌ترین شاخص در تعیین ارزش‌گذاری خطوط موقعیت خط در یک شبکه است، طبق مدل‌سازی، خطوطی که در بالادست قرار دارند ارزش تمامی خطوط پایین‌دستی خود را نیز دارا هستند و ازاین‌جهت توپولوژی شبکه بسیار تأثیرگذار است.

۲-۵. فرمول پیشنهادی

با استفاده از فرمول پیشنهادی زیر ارزش هر خط به‌دست می‌آید.

$$v_l(i) = v_i + \sum_{j \in A} (U_d(j) \times v_j) + int(i) \quad (۵)$$

که در آن A مجموعه خطوطی است که در صورت قطعی خط i از دسترس خارج می‌شوند و درواقع حیات این خطوط و ارزش آن‌ها درگرو در دسترس بودن خط i است.

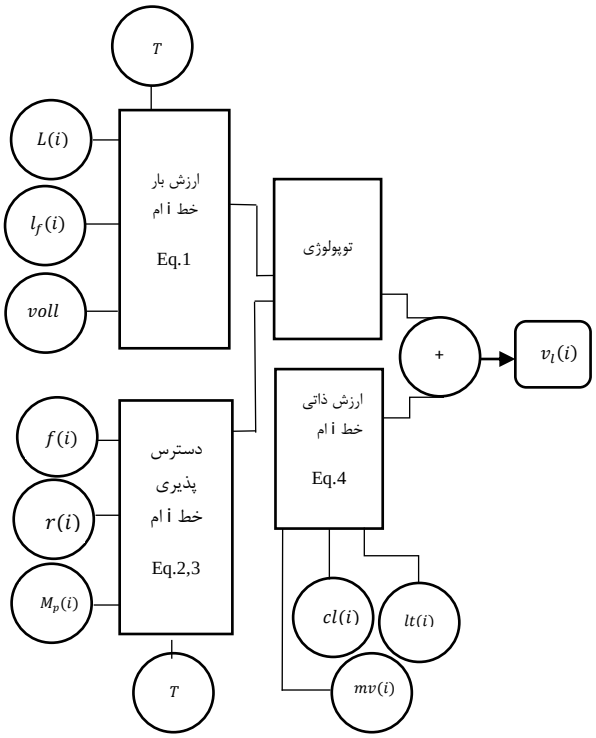
۲-۶. شاخص تاب‌آوری خطوط

ارزش خطوط به‌عنوان معیاری از حساسیت شبکه نسبت به هر مخاطره‌ای در نظر گرفته می‌شود. هر چه خطوط شبکه در این ارزش‌گذاری، مقدار کمتری به خود اختصاص دهند، این حساسیت به درجه پایین‌تری نزول می‌کند و به تعبیری، خطوط در رتبه‌بندی تاب‌آوری، تاب‌آوری بیشتری خواهند داشت. ازاین‌رو این مفهوم در رابطه (۶) نمایش داده شد و به‌عنوان شاخصی برای قیاس تاب‌آوری خطوط شبکه‌ها در نظر گرفته می‌شود.

$$R_G = \sum_{i=1}^{n_G} v_l(i) \quad (۶)$$

که در آن، R_G شاخص تاب‌آوری خطوط شبکه، و n_G تعداد خطوط شبکه است.

۲-۷. فلوچارت مدل پیشنهادی



شکل ۱. فلوچارت مدل پیشنهادی

۲-۸. مطالعات عددی

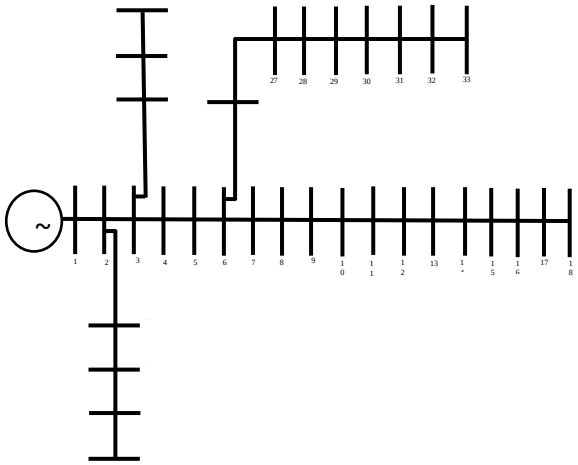
در یک سامانه استاندارد۳۳ شینه IEEE بررسی و ارزش‌گذاری خطوط صورت می‌پذیرد، اثربخشی حضور DG در شبکه، برای دو حالت: آ) شبکه بدون تولید پراکنده و ب) شبکه با تولید پراکنده بررسی می‌شود.

۳. نتایج و بحث

در این بخش با توجه به مدل پیشنهادی و در نظر گرفتن دو حالت شبکه بدون تولیدات پراکنده و در حضور تولیدات پراکنده نتـایج و مشاهدات به بحث گزارده می‌شود.

۳-۱. شبکه بدون DG

شکل (۲) شبکه موردنظر را نشان می‌دهد.



شکل ۲. شبکه استاندارد IEEE ۳۳ شینه

مشخصات توان حقیقی دریـافتی سـامانه فـوق در جـدول (۱) شرح داده شد. سایر مشخصات موردنیاز ۳۳ خط مورد ارزیـابی در جدول (۲) نشان داده شده است.

جدول ۱. مشخصات توان دریافتی شین‌ها

S. bus	R. bus	L	S. bus	R. bus	L	S. bus	R. bus	L
۱	۲	۱۰۰	۱۲	۱۳	۶۰	۲۳	۲۴	۴۲۰
۲	۳	۹۰	۱۳	۱۴	۱۲۰	۲۴	۲۵	۴۲۰
۳	۴	۱۲۰	۱۴	۱۵	۶۰	۶	۲۶	۶۰
۴	۵	۶۰	۱۵	۱۶	۶۰	۲۶	۲۷	۶۰
۵	۶	۶۰	۱۶	۱۷	۶۰	۲۷	۲۸	۶۰
۶	۷	۲۰۰	۱۷	۱۸	۹۰	۲۸	۲۹	۱۲۰
۷	۸	۲۰۰	۲	۱۹	۹۰	۲۹	۳۰	۲۰۰
۸	۹	۶۰	۱۹	۲۰	۹۰	۳۰	۳۱	۱۵۰
۹	۱۰	۶۰	۲۰	۲۱	۹۰	۳۱	۳۲	۲۱۰
۱۰	۱۱	۴۵	۲۱	۲۲	۹۰	۳۲	۳۳	۶۰
۱۱	۱۲	۶۰	۳	۲۳	۹۰	-	-	-

جدول ۲. مشخصات خطوط شبکه

Num.l	l_f	$voll$	f	r	M_p	cl	mv	lt
۱	۰/۸	۳۲۰۰	۰/۰۵	۴	۵	۲۰	۵۰	۱۷۵۲۰۰
۲	۰/۹	۳۲۰۰	۰/۰۵	۵	۶	۲۰	۵۰	۱۷۵۲۰۰
۳	۰/۸۵	۳۲۰۰	۰/۰۵	۶	۴	۲۰	۵۰	۱۷۵۲۰۰
۴	۰/۸۸	۳۲۰۰	۰/۰۵	۴	۶	۲۰	۵۰	۱۷۵۲۰۰
۵	۰/۸۹	۳۲۰۰	۰/۰۵	۴	۷	۲۰	۵۰	۱۷۵۲۰۰
۶	۰/۹۱	۳۲۰۰	۰/۰۵	۶	۷	۲۰	۵۰	۱۷۵۲۰۰
۷	۰/۸	۳۲۰۰	۰/۰۵	۵	۵	۲۰	۵۰	۱۷۵۲۰۰
۸	۰/۹	۳۲۰۰	۰/۰۵	۴	۶	۲۰	۵۰	۱۷۵۲۰۰
۹	۰/۸۵	۳۲۰۰	۰/۰۵	۴	۴	۲۰	۵۰	۱۷۵۲۰۰
۱۰	۰/۸۸	۳۲۰۰	۰/۰۵	۵	۶	۲۰	۵۰	۱۷۵۲۰۰
۱۱	۰/۸۹	۳۲۰۰	۰/۰۵	۴	۵	۲۰	۵۰	۱۷۵۲۰۰
۱۲	۰/۹۱	۳۲۰۰	۰/۰۵	۴	۵	۲۰	۵۰	۱۷۵۲۰۰
۱۳	۰/۸	۳۲۰۰	۰/۰۵	۶	۴	۲۰	۵۰	۱۷۵۲۰۰
۱۴	۰/۹	۳۲۰۰	۰/۰۵	۵	۵	۲۰	۵۰	۱۷۵۲۰۰
۱۵	۰/۸۵	۳۲۰۰	۰/۰۵	۷	۶	۲۰	۵۰	۱۷۵۲۰۰
۱۶	۰/۸۸	۳۲۰۰	۰/۰۵	۴	۵	۲۰	۵۰	۱۷۵۲۰۰
۱۷	۰/۸۹	۳۲۰۰	۰/۰۵	۶	۵	۲۰	۵۰	۱۷۵۲۰۰
۱۸	۰/۸	۳۲۰۰	۰/۰۵	۴	۵	۲۰	۵۰	۱۷۵۲۰۰
۱۹	۰/۹	۳۲۰۰	۰/۰۵	۵	۶	۲۰	۵۰	۱۷۵۲۰۰
۲۰	۰/۸۵	۳۲۰۰	۰/۰۵	۶	۴	۲۰	۵۰	۱۷۵۲۰۰
۲۱	۰/۸۸	۳۲۰۰	۰/۰۵	۴	۶	۲۰	۵۰	۱۷۵۲۰۰
۲۲	۰/۸۹	۳۲۰۰	۰/۰۵	۴	۷	۲۰	۵۰	۱۷۵۲۰۰
۲۳	۰/۹۱	۳۲۰۰	۰/۰۵	۶	۷	۲۰	۵۰	۱۷۵۲۰۰
۲۴	۰/۸	۳۲۰۰	۰/۰۵	۵	۵	۲۰	۵۰	۱۷۵۲۰۰
۲۵	۰/۹	۳۲۰۰	۰/۰۵	۴	۶	۲۰	۵۰	۱۷۵۲۰۰
۲۶	۰/۸۵	۳۲۰۰	۰/۰۵	۴	۴	۲۰	۵۰	۱۷۵۲۰۰
۲۷	۰/۸۸	۳۲۰۰	۰/۰۵	۵	۶	۲۰	۵۰	۱۷۵۲۰۰
۲۸	۰/۸۹	۳۲۰۰	۰/۰۵	۴	۵	۲۰	۵۰	۱۷۵۲۰۰
۲۹	۰/۹۱	۳۲۰۰	۰/۰۵	۴	۵	۲۰	۵۰	۱۷۵۲۰۰
۳۰	۰/۸	۳۲۰۰	۰/۰۵	۶	۴	۲۰	۵۰	۱۷۵۲۰۰
۳۱	۰/۹	۳۲۰۰	۰/۰۵	۵	۵	۲۰	۵۰	۱۷۵۲۰۰
۳۲	۰/۸۵	۳۲۰۰	۰/۰۵	۷	۶	۲۰	۵۰	۱۷۵۲۰۰
۳۳	۰/۸۸	۳۲۰۰	۰/۰۵	۴	۵	۲۰	۵۰	۱۷۵۲۰۰

با توجه به رابطه (۵) و بـا در نظـر گـرفتن توپولـوژی شـبکه، شبیه‌سازی با استفاده از نرم‌افزار متلـب صـورت گرفـت و نتـایجی به‌دست آمد که این نتایج به ترتیب ارزش بیشتر در جدول (۳) به نمایش در آمده است.

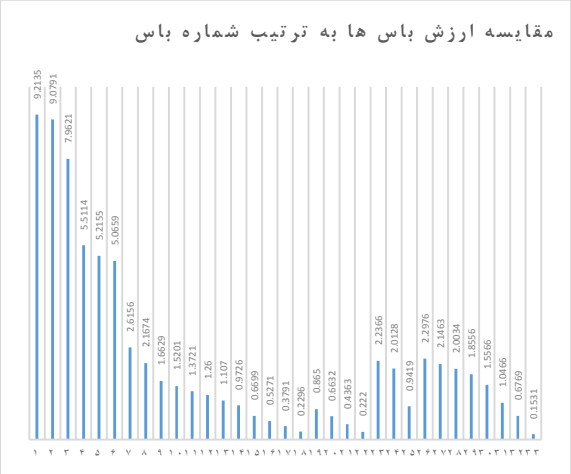
جدول ۳. نتایج شبیه‌سازی در حالت اول

شماره خط	ارزش (×10^{10})	رتبه ارزش‌گذاری	شماره خط	ارزش (×10^{10})	رتبه ارزش‌گذاری	شماره خط	ارزش (×10^{10})	رتبه ارزش‌گذاری
۲۵	۰/۹۴۱۹	۲۳	۲۴	۲/۰۱۲۸	۱۲	۱	۹/۲۱۳۵	۱
۱۹	۰/۸۶۵۰	۲۴	۲۸	۲/۰۰۳۴	۱۳	۲	۹/۰۷۹۱	۲
۳۲	۰/۶۷۶۹	۲۵	۲۹	۱/۸۵۵۶	۱۴	۳	۷/۹۶۲۱	۳
۱۵	۰/۶۶۹۹	۲۶	۹	۱/۶۶۲۹۳	۱۵	۴	۵/۵۱۱۴	۴
۲۰	۰/۶۶۳۲	۲۷	۳۰	۱/۵۵۶۶	۱۶	۵	۵/۲۱۵۵	۵
۱۶	۰/۵۲۷۱	۲۸	۱۰	۱/۵۲۰۱	۱۷	۶	۵/۰۶۵۹	۶
۲۱	۰/۴۳۶۳	۲۹	۱۱	۱/۳۷۲۱۱	۱۸	۷	۲/۶۱۵۶	۷
۱۷	۰/۳۷۹۱	۳۰	۱۲	۱/۲۶۰۰	۱۹	۲۶	۲/۲۹۷۶	۸
۱۸	۰/۲۲۹۶	۳۱	۱۳	۱/۱۰۷۰	۲۰	۲۳	۲/۲۳۶۶	۹
۳۴	۰/۲۲۲۰	۳۲	۳۱	۱/۰۴۶۶	۲۱	۸	۲/۱۶۷۵	۱۰
۳۳	۰/۱۵۳۱	۳۳	۱۴	۰/۹۷۲۶	۲۲	۲۷	۲/۱۴۶۳	۱۱

با دانستن این نکته که شماره باس دریافت‌کننده، نشان‌دهنده شماره خط موردنظر است، موارد مطرح‌شده در ادامه چالش‌برانگیز است:

خطوط شماره ۱ تا ۷ به خاطر موقعیت توپولوژیکی خود دارای بیشترین ارزش می‌باشند، هرچند که به‌خودی‌خود بار زیادی را تأمین نمی‌کنند، حتی دراین‌بین خط شماره ۷ از خط شماره ۲۳ که ۲ بار ۴۲۰ کیلوواتی را تأمین می‌کند دارای ارزش بالاتری است.

خطوط ۲۶ و ۲۳ در رتبه‌های ۸ و ۹ ارزش‌گذاری قرار دارند، این در حالی است که باوجوداینکه خط شماره ۸ باعث دسترس‌پذیر بودن تعداد خطوط بیشتری است، در جایگاه دهم قرار دارد که نشان‌دهنده ارجحیت بار تأمین‌شده در برابر توپولوژی شبکه است. در ادامه خط شماره ۸ در رقابت با خط شماره ۲۷ ارزش بالاتری را از شبیه‌سازی‌ها می‌گیرد و درواقع در اینجا توپولوژی بر تأمین بار ترجیح داده می‌شود. ارزش‌گذاری نسبتاً پراکنده در بیشتر اوقات بر لزوم توجه به اکیپ‌های تعمیراتی اشاره دارد که می‌بایست به‌سرعت جابه‌جا شوند تا روند بازیابی بار برای رسیدن به سطح تاب آور اولیه با سرعت بیشتری انجام پذیرد. شکل (۳) مقایسه‌ای از ارزش‌گذاری صورت گرفته روی باس‌ها را نشان می‌دهد، از این نمودار به‌وضوح می‌توان به چالش برنامه‌ریزی صحیح برای تعمیرات در حین و پس از حوادث غیرقابل‌پیش‌بینی را مشاهده کرد.



شکل ۳. مقایسه ارزش باس‌ها به ترتیب شماره باس

در این شبکه با توجه به رابطه (۶) تاب‌آوری خطوط به قرار زیر به‌دست می‌آید.

$$R_{G_1} = \sum_{i=1}^{33} v_l(i) = 75.644638 \times 10^{10}$$

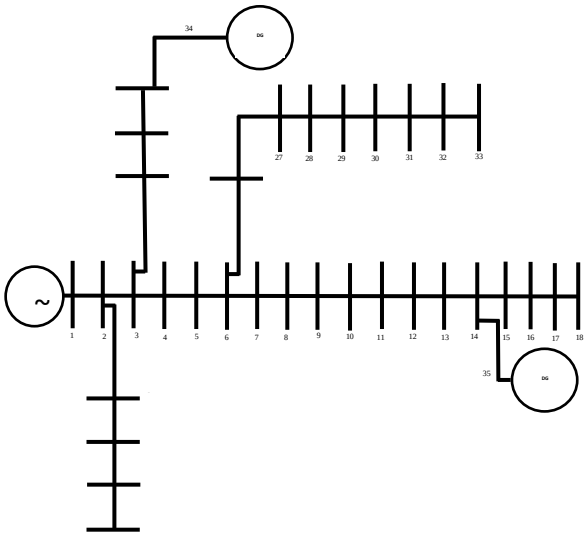
۳-۲. شبکه با DG

در این بخش از دو DG جهت بررسی اثر حضور تولیدات پراکنده در ارزش‌گذاری خطوط شبکه استفاده شده است. در مورد مکان تولیدات پراکنده، روش‌های متنوعی برای مکان‌یابی وجود دارد [۱۳] که مورد بحث در اینجا نیست. در این مقاله با استفاده از ترکیب احتمال، این دو DG در ۳۳ شین موجود در تمامی حالات ممکن قرار داده و در هر حالت ارزش کل خطوط موجود محاسبه شد و سپس در یک جدول به ترتیب از کمترین ارزش خطوط به بیشترین ارزش خطوط مرتب شد. واضح است که حالت‌هایی که ارزش مجموع خطوط در میزان کمتری قرار می‌گرفت، اثر حضور تولیدات پراکنده پررنگ‌تر بود. در مجموع ۵۲۸ حالت برای قرار گیری تولیدات پراکنده وجود داشت که پنج سناریوی برتر و بدترین سناریو را در جدول (۴) مشاهده می‌کنید.

جدول۴. سناریوهای مکان قرار گیری تولیدات پراکنده

مکان قرار گیریDG ها	ارزش (× 10^{10})	سناریو
باس‌های ۱۴ و ۲۵	۷۵/۶۴۱۷۰۵	سناریو ۱(برتر)
باس‌های ۱۸ و ۲۵	۷۵/۶۴۱۷۴۴	سناریو ۲
باس‌های ۸ و ۲۵	۷۵/۶۴۱۷۷۹	سناریو ۳
باس‌های ۷ و ۲۵	۷۵/۶۴۲۱۰۸	سناریو ۴
باس‌های ۲۲ و ۲۵	۷۵/۶۴۲۲۴۲	سناریو ۵
باس‌های ۱ و ۲	۷۵/۶۴۴۴۶۵	بدترین سناریو

با توجه به توضیحات مذکور و جدول (۴) سناریوی برتر یعنی قرار گیری تولیدات پراکنده در باس‌های ۱۴ و ۲۵ در نظر گرفته شد. فرض بر این است که این تولیدات پراکنده همواره قابل‌راه‌اندازی و وصل شدن به شبکه هستند و توانایی تأمین بارهای موردنظر را دارند. برای انجام شبیه‌سازی، خطوط متصل به باس‌های ذکرشده، خطوط شماره ۳۴ و ۳۵ در نظر گرفته می‌شوند.



شکل ۴. شبکه ۳۳ شینه IEEE با درنظر گرفتن تولیدات پراکنده

اطلاعات مربوط به خطوط تولیدات پراکنده در جدول (۵) آورده شده است.

جدول ۵. اطلاعات خطوط تولید پراکنده

Num.l	f	r	M_p	cl	mv	lt
۳۴	./۰۵	۲	۲	۲۵	۶۰	۱۷۵۲۰۰
۳۵	./۰۵	۳	۳	۲۵	۶۰	۱۷۵۲۰۰

اثر حضور تولیدات پراکنده به این صورت است که در زمان در دسترس نبودن خطوط ۱۴ و ۲۵ ، وظیفه تأمین بار این خطوط را بر عهده می‌گیرند. با توجه به فرمول ارائه‌شده (۵) ارزش خطوط تولیدات پراکنده (خطوط ۳۴ و ۳۵) به‌صورت زیر به‌دست می‌آیند:

$$v_l(34) = (U_d(25) \times v_{25}) + int(34) \quad (۷)$$

$$v_l(35) = (U_d(14) \times v_{14}) + int(35) \quad (۸)$$

دیگر اثر حضور تولیدات پراکنده در خطوط بالادستی آن‌هاست، به‌واقع حضور ضریب $(U_d(DG) \times V_j)$ (که V_j ارزش بار تأمین‌شده باسی است که DG به آن وصل شده است.) سبب می‌شود ارزش خطوط بالادستی کمتر شود و این کاهش در شبیه‌سازی‌ها نیز به‌دست می‌آید.

نتایج حاصل از ارزش‌گذاری در شبکه جدید در جدول (۶) آورده شده است.

جدول ۶. نتایج شبیه‌سازی در حالت دوم(شبکه با DG)

شماره خط	ارزش ($\times 10^{10}$)	رتبه ارزش گذاری	شماره خط	ارزش ($\times 10^{10}$)	رتبه ارزش گذاری	شماره خط	ارزش ($\times 10^{10}$)	رتبه ارزش گذاری
۱۹	۰/۸۶۵۰	۲۵	۲۸	۲/۰۰۳۴	۱۳	۱	۹/۲۱۳۱	۱
۳۲	۰/۶۷۶۹	۲۶	۲۹	۱/۸۵۵۶	۱۴	۲	۹/۰۷۸۷	۲
۱۵	۰/۶۶۹۹	۲۷	۹	۱/۶۶۲۸	۱۵	۳	۷/۹۶۱۷	۳
۲۰	۰/۶۶۳۲	۲۸	۳۰	۱/۵۵۶۶	۱۶	۴	۵/۵۱۱۲	۴
۱۶	۰/۵۲۷۱	۲۹	۱۰	۱/۵۱۹۹	۱۷	۵	۵/۲۱۵۳	۵
۲۱	۰/۴۳۶۳	۳۰	۱۱	۱/۳۷۲۰	۱۸	۶	۵/۰۶۵۷	۶
۱۷	۰/۳۷۹۱	۳۱	۱۲	۱/۲۵۹۸	۱۹	۷	۲/۶۱۵۴	۷
۳۵	۰/۳۰۲۶	۳۲	۱۳	۱/۱۰۶۸	۲۰	۲۶	۲/۲۹۷۶	۸
۱۸	۰/۲۲۹۶	۳۳	۳۱	۱/۰۴۶۶	۲۱	۲۳	۲/۲۳۶۳	۹
۲۲	۰/۲۲۲۰	۳۴	۱۴	۰/۹۷۲۴	۲۲	۸	۲/۱۶۷۳	۱۰
۳۳	۰/۱۵۳۱	۳۵	۲۵	۰/۹۴۱۶	۲۳	۲۷	۲/۱۴۶۳	۱۱
–	–	۳۶	۳۴	۰/۹۴۱۴	۲۴	۲۴	۲/۰۱۲۵	۱۲

چنان‌که از نتایج برمی‌آید خطوطی که در آن بودن یا نبودن تولیدات پراکنده در ارزش‌گذاری آن‌ها بی‌تأثیر است، نسبت به حالت قبل ثابت ماندند. از سوی دیگر، حضور تولیدات پراکنده در تمامی خطوطی که ارزش آن‌ها با توجه به توپولوژی شبکه مرتبط با خطوطی است که تولیدات پراکنده به آن متصل شده است، کاهش ارزش خط را به همراه داشته است.

این شبکه با توجه به رابطه (۶) تاب‌آوری خطوط به قرار زیر به‌دست می‌آید:

$$R_{G_2} = \sum_{i=1}^{33} v_l(i) = 75.641705 \times 10^{10}$$

۴. نتیجه‌گیری

ارزش‌گذاری دارایی‌ها و در این مقاله ارزش‌گذاری خطوط جهت واکنش سریع به رویدادهای شدید آب و هوایی در بازیابی از حالت بحرانی امری اجتناب‌ناپذیر و ضروری است.

این مقاله اساس مدل‌سازی برمبنای قیمت را در دستور کار خود قرار داد که در آن ارزش بار، جهت درنظر گرفتن اهمیت سمت تقاضا؛ نرخ خرابی، جهت بررسی دسترس‌پذیری خط؛ ارزش ذاتی خطوط، جهت درنظر گرفتن هزینه سرمایه‌گذاری و همچنین فاکتور توپولوژی، جهت تأکید بر آرایش شبکه مدنظر قرار داده شد. در این کار تغییر توپولوژی شبکه با قرار دادن تولیدات پراکنده در شبکه مورد بررسی قرار گرفت و اثربخشی حضور DGها در ارزش‌گذاری و اولویت‌بندی خطوط مشاهده شد. همچنین با ارایه ی معیاری برای سنجش تاب‌آوری خطوط بر مبنای قیمت، شبکه را در دو حالت با DG و بدون DG مقایسه کرد.

جدول (۷) ارزش‌گذاری در دو حالت شبکه را نشان می‌دهد.

جدول ۷. مقایسه ارزش خطوط در دو حالت

شماره خط	حالت دوم ($\times 10^{10}$)	حالت اول ($\times 10^{10}$)	رتبه ارزش‌گذاری	حالت دوم ($\times 10^{10}$)	شماره خط	حالت اول ($\times 10^{10}$)	رتبه ارزش گذاری
۱۲	۱/۲۵۹۸	۱/۲۶۰۰	۱۹	۹/۲۱۳۱	۱	۹/۲۱۳۵	۱(کاهش)
۱۳	۱/۱۰۶۸	۱/۱۰۷۰	۲۰	۹/۰۷۸۷	۲	۹/۰۷۹۱	۲(کاهش)
۳۱	۱/۰۴۶۶	۱/۰۴۶۶	۲۱	۷/۹۶۱۷	۳	۷/۹۶۲۱	۳(کاهش)
۱۴	۰/۹۷۲۴	۰/۹۷۲۶	۲۲	۵/۵۱۱۲	۴	۵/۵۱۱۴	۴(کاهش)
۲۵	۰/۹۴۱۶	۰/۹۴۱۹	۲۳	۵/۲۱۵۳	۵	۵/۲۱۵۵	۵(کاهش)
۱۹/۳۴	۰/۹۴۱۴	۰/۸۶۵۰	۲۴	۵/۰۶۵۷	۶	۵/۰۶۵۹	۶(کاهش)
۳۲/۱۹	۰/۸۶۵۰	۰/۶۷۶۹	۲۵	۲/۶۱۵۴	۷	۲/۶۱۵۶	۷(کاهش)
۱۵/۳۲	۰/۶۷۶۹	۰/۶۶۹۹	۲۶	۲/۲۹۷۶	۲۶	۲/۲۹۷۶	۸(کاهش)
۲۰/۱۵	۰/۶۶۹۹	۰/۶۶۳۲	۲۷	۲/۲۳۶۳	۲۳	۲/۲۳۶۶	۹(کاهش)
۱۶/۲۰	۰/۶۶۳۲	۰/۵۲۷۱	۲۸	۲/۱۶۷۳	۸	۲/۱۶۷۵	۱۰(کاهش)
۲۱/۱۶	۰/۵۲۷۱	۰/۴۳۶۳	۲۹	۲/۱۴۶۳	۲۷	۲/۱۴۶۳	۱۱(کاهش)
۱۷/۲۱	۰/۴۳۶۳	۰/۳۷۹۱	۳۰	۲/۰۱۲۵	۲۴	۲/۰۱۲۸	۱۲
۱۸/۱۷	۰/۳۷۹۱	۰/۲۲۹۶	۳۱	۲۸	۲/۰۰۳۴	۲/۰۰۳۴	۱۳
۳۲/۳۵	۰/۳۰۲۶	۰/۲۲۲۰	۳۲	۲۹	۱/۸۵۵۶	۱/۸۵۵۶	۱۴
۳۳/۱۸	۰/۲۲۹۶	۰/۱۵۳۱	۳۳	۹	۱/۶۶۲۸	۱/۶۶۲۹۳	۱۵(کاهش)
۲۲	۰/۲۲۲۰	–	۳۴	۳۰	۱/۵۵۶۶	۱/۵۵۶۶	۱۶
۳۴	۰/۱۵۳۱	–	۳۵	۱۰	۱/۵۱۹۹	۱/۵۲۰۱	۱۷(کاهش)
–	–	–	–	۱۱	۱/۳۷۲۰	۱/۳۷۲۱۱	۱۸

در جدول (۷) ردیف هایی که با رنگ سبز به نمایش در آمده انـد، نشان دهنده تغییر رتبـه ارزش‌گـذاری در دو حالـت اسـت کـه در ستون مربوط به شماره خط، عدد اول مربوط به شماره خط شبکه اول(بدون تولیدات پراکنده) و عـدد دوم مربـوط بـه شـماره خـط شبکه دوم (با تولیدات پراکنده) است.

۵. مرجع‌ها

[1] Billinton, R.; Wu.; Singh,G. “Extreme adverse weather modeling in transmission and distribution system reliability evaluation”; Power Syst. Comput. Conf.(PSCC), Spain. 2002, 65, p. 66.

[2] Haimes, Y. Y. “On the definition of resilience in systems”; Risk Anal. An Int. J. 2009, 29, 498-501.

[3] Hosseini, S. ;Barker.K.; Ramirez-Marquez, J. E. “A review of definitions and measures of system resilience”; Reliab. Eng. Syst. Saf. 2016, 145, 47-61.

[4] Francis, R.; Bekera,B. “A metric and frameworks for resilience analysis of engineered and infrastructure systems”; Reliab. Eng. Syst. Saf. 2014, 121, 90-103.

[5] Righi, A. W.; Saurin, T. A.; Wachs, P. “A systematic literature review of resilience engineering: Research areas and a research agenda proposal”; Reliab. Eng. Syst. Saf. 2015, 141, 142-152.

[6] Maliszewski, P. J.; Perrings, C. “Factors in the resilience of electrical power distribution infrastructures”;Appl. Geogr. 2012, 32, 668-679.

[7] Nan, C.; Sansavini, G. “A quantitative method for assessing resilience of interdependent infrastructures”; Reliab. Eng. Syst. Saf. 2017, 157, 35-53.

[8] Ouyang, M.; Duenas-Osorio, L. “Multi-dimensional hurricane resilience assessment of electric power systems”; Struct. Saf. 2014, 48, 15-24.

[9] Cadini, F.; Agliardi, G. L.; E. Zio. “A modeling and simulation framework for the reliability/availability assessment of a power transmission grid subject to cascading failures under extreme weather conditions”; Appl. Energy. 2017, 185, 267-279.

[10] Figueroa-Candia, M.; Felder, F. A.; Coit, D. W. “Resiliency-based optimization of restoration policies for electric power distribution systems”; Electr. Power Syst. Res. 2018, 161, 188-198.

[11] Walsh, T.; Layton, T.; Wanik, D.; Mellor, J. “Agent based model to estimate time to restoration of storm-induced power outages”. Infrastructures. 2018, 3, p. 33.

[12] Zhang, H.; Bie, Z.; Yan, C.; Li, G. “Post-disaster Power System Resilience Enhancement Considering Repair Process”; 2018 China Int. Conf. Electr. Distrib., 2018, 1550-1554.

[13] Alizade, M.; Khosravi, M. “Provide a practical approach in planning and placement of distributed generation sources based on multi-objective genetic algorithms” .Adv. Defence Sci & Technol, pp. 267-277, 2019.

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۴۰۱-۳۹۱

«علمی- پژوهش»

ارائه الگوریتمی جهت شناسایی آسیب‌پذیرترین شین در شبکه هوشمند برق در حمله سایبری مبتنی بر تخمین حالت

امیرحسین طیبی[۱]، رضا شریفی[۲*]، امیرحسین سالمی[۳]، فرامرز فقیهی[۴]

۱- دانشجوی دکتری تخصصی، گروه مهندسی برق، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران ۲- استادیار، گروه مهندسی برق، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران ۳- استادیار، گروه مهندسی برق، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران ۴- استادیار، گروه مهندسی برق، واحد علوم تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

(دریافت: ۹۸/۱۱/۰۶، پذیرش: ۹۹/۰۲/۲۲)

چکیده

با توجه به خودکارسازی شبکه‌های قدرت و مبادله داده‌ها در یک زیرساخت مخابراتی، احتمال طرح‌ریزی حمله سایبری بسیار بالا است. در این راستا بهینه‌سازی بودجه‌های حمله و دفاع در حمله سایبری در شبکه قدرت از اهمیت خاصی برخوردار است. در این مقاله در راستای فاز تهاجم سایبری به شبکه قدرت، انتخاب آسیب‌پذیرترین شین عملیاتی با استفاده از فن تخمین حالت طی الگوریتم جدیدی تحلیل و شبیه‌سازی‌شده است. برای این منظور تزریق داده غلط به اطلاعات ارسالی از PMU به‌گونه‌ای که قابل‌تشخیص برای بهره‌بردار شبکه تحت تهاجم نباشد صورت می‌پذیرد. به‌عنوان یک مطالعه موردی پیاده‌سازی الگوریتم پیشنهادی برای یک شبکه ۱۴ شینِ IEEE انجام‌شده است و بهترین شین ازنظر قرارگیری تحت تهاجم شناسایی‌شده است. عملکرد این الگوریتم مبنی بر نتایج حاصل از تخمین حالت شبکه پس از رخداد حمله سایبری بر روی شین‌های مختلف است. درنهایت قسمتی از شبکه که تخریب اطلاعات در آن بخش بیشترین آسیب را به شبکه وارد می‌کند مشخص می‌شود.

کلیدواژه‌ها: تزریق داده غلط، حمله غیرقابل تشخیص، سامانه قدرت، تخمین حالت، بردار اندازه‌گیری

Presentation of an Algorithm for Identification of the Most Vulnerable Bus in Electric Smart Grid Through Cyber-Attack Based on State Estimation

A. H. Tayebi, R. Sharifi*, A. H. Salemi, F. Faghihi
Faculty of Electrical Engineering, West Tehran Branch, Islamic Azad University, Tehran, Iran
(Received: 26/01/2020; Accepted: 11/05/2020)

Abstract

Considering the power grids automation and network data transferring in telecommunication infrastructure, the possibility of planning a cyber-attack grows up intensively. In this regard, the optimization of the budget for attack (BA) and budget for defense (BD) in a power network through cyber-attack is so crucial. In this paper, regarding the cyber invasion phase, the choice of the most vulnerable operating bus using the state estimation technique through a new algorithm is analyzed and simulated. For this purpose, false data injection is performed on the data sent from the PMU in such a way that it is not detectable to the network dispatching operator under the invasion. As a case study implementation of the suggested algorithm for a 14 IEEE bus network is carried out and the best bus in terms of exposure under attack is identified. The performance of this algorithm is based on the results obtained from state estimating of the grid after occurring a cyber-attack on different buses. Finally, the part of the grid, which the destruction of information in that part leads to the most damage to the grid, is determined.

Keywords: False Data Injection, Undetectable Attack, Power System, State Estimation, Measurement Vector.

*Corresponding Author E-mail: Sharifi.r@wtiau.ac.ir

۱. مقدمه

شبکه‌های هوشمند یکی از مهم‌ترین ساختارهای مبتنی بر دستگاه‌های سایبر-فیزیکی می‌باشند. به همین خاطر این شبکه‌ها دارای قابلیت اطمینان بالا و کارایی بیشتر در زمان افزایش مصرف می‌باشند. ادوات ارتباط داخلی از قبیل واحدهای اندازه‌گیری فازور PMU (Phasor measurement units) و اندازه‌گیرهای هوشمند ازجمله زیرساخت‌های مهم این شبکه‌ها برای رسیدن به اهدافشان به‌حساب می‌آیند. این زیرساخت‌های سایبری با بالا بردن دسترسی و انتقال اطلاعات در سامانه، از طریق ادغام ارتباطات، محاسبات و فناوری‌های پیشرفته کنترل، وضعیت سامانه را کنترل می‌کنند. درواقع سامانه‌های سایبر- فیزیکی نسل جدیدی از سامانه‌ها هستند که منابع محاسباتی، وسایل ارتباطی عملیات فیزیکی را شامل می‌شوند. ازجمله کاربردهایی که این سامانه‌ها دارند تخمین حالت سامانه با استفاده از اطلاعات به‌دست‌آمده از این سامانه‌ها است. تخمین حالت درواقع پروسه تخمین متغیرهای حالت نامعلوم با استفاده از مقادیر اندازه‌گیری شده توسط اندازه‌گیرها در شبکه است. تخمین حالت یکی از مهم‌ترین ابزارهای مدیریت انرژی سامانه است. تخمین حالت سامانه وضعیت فیزیکی سامانه را مشخص می‌کند (البته باوجود نویز) که می‌توان با استفاده از این اطلاعات دستورات لازم را به سامانه‌های فیزیکی ارسال کرد. پس تخمین حالت سامانه از لوازم مهم کنترل سامانه است.

امنیت شبکه‌های برق یکی از عواملی است که در کنترل این سامانه‌ها نقش اساسی دارد. یکی از راه‌کارهای مقابله با هر مجموعه‌ای از بین بردن این امنیت و درنتیجه ایجاد اخلال در سامانه برق‌رسانی آن مجموعه است. مهاجمین برای از کار انداختن شبکه‌های قدرت دست به حمله به این شبکه‌ها برای از کار انداختن عملکرد صحیح آن‌ها می‌زنند. پس یکی از راه‌کارهای آسیب رساندن به دشمن ایجاد اختلال در شبکه‌های برق‌رسانی و درنتیجه ایجاد خاموشی در شبکه‌های برق است. این اختلال را می‌توان به طرق مختلف ایجاد کرد. یکی از راه‌های اختلال در شبکه‌های قدرت حمله فیزیکی به این شبکه‌ها و از بین بردن زیرساخت‌های انتقال برق از قبیل خطوط انتقال یا ترانسفورماتورها است؛ اما روش دیگری که برای ایجاد اختلال در شبکه‌های قدرت وجود دارد حملات سایبری به زیرساخت‌های سایبری- فیزیکی این شبکه‌ها است.

حملات سایبری می‌توانند سامانه‌های کنترل‌کننده شبکه‌های الکتریکی را تضعیف کنند یا حتی به‌طورکلی از بین ببرند. درگذشته تصور می‌شد که حملات سایبری نمی‌توانند امنیت سامانه‌های برق صنعتی را تهدید کنند؛ اما در سال‌های گذشته حملات سایبری تأثیر بسیار مهمی در مسائل امنیتی چه در بحث صنعتی و چه از دیدگاه تأمین‌کنندگان انرژی داشته‌اند. مثلاً در سال ۲۰۰۰ سامانه SCADA (Supervisory Control and Data Acquisition) فاضلاب شهری یکی از ایالت‌های استرالیا موردحمله قرار گرفت. در سال ۲۰۰۳ به سامانه‌های کامپیوتری یکی از نیروگاه‌های اتمی یکی از ایالت‌های امریکا توسط حملات سایبری نفوذ کردند. همچنین در سال ۲۰۱۰ نیز یک حمله سایبری به تأسیسات اتمی نطنز صورت گرفت.

در سال‌های اخیر حملات سایبری به تهدیدی مهم برای یکپارچگی سامانه‌های تخمین حالت سامانه تبدیل‌شده است. حملات سایبری که به‌خوبی برنامه‌ریزی‌شده باشند می‌توانند اثرات فاجعه باری بر روی سامانه بگذارند تا حدی که ممکن است منجر به خاموشی سراسری در شبکه گردند. یکی از انواع متداول این حملات، حمله از طریق تزریق اطلاعات غلط به سامانه است. در این نوع حمله دشمن با تزریق اطلاعات غلط تخمین حالت سامانه را با خطا مواجه می‌کند که این عمل منجر به تصمیم‌گیری غلط از طریق سامانه‌های کنترلی می‌گردد.

در این سال‌ها مقالات زیادی به بررسی حملات سایبری بر روی شبکه‌های برق پرداخته‌اند. این حملات از جهت‌های مختلفی موردبررسی و تحلیل قرارگرفته‌اند. در [۲-۱] به بررسی و تحلیل حملات از نوع تزریق اطلاعات غلط بر روی شبکه‌های هوشمند پرداخته شده است. در این مقالات روش‌ها و تحلیل‌هایی برای شناسایی و تشخیص این حملات ارائه شده است. همچنین روش‌هایی ارائه‌شده که میزان خسارات ناشی از این حملات کاهش یابد.

یکی از مواردی که بر روی میزان اثرگذاری حملات و همچنین نوع راهبرد حمله تأثیرگذار است، مکان قرار گرفتن واحدهای اندازه‌گیری (PMUها) است. این اندازه‌گیرها انواع متفاوتی دارند. یکی از راهبردهای دفاع در برابر حملات سایبری ارتقا امنیت این اندازه‌گیرها به نحوی است که دشمن قابلیت نفوذ به آن‌ها را نداشته باشد؛ اما همان‌طور که اشاره شد نحوه قرارگیری این اندازه‌گیرها در شبکه بر روی تأثیرگذاری حمله دشمن مؤثر است.

در [۴-۳] به بررسی مسئله جایابی بهینه PMUها پرداخته شده است. این جایابی بهینه با در نظر گرفتن شرایط اضطراری در شبکه انجام‌شده و درنهایت بهترین حالت قرارگیری PMU ها با توجه به انواع مختلف خطاهایی که ممکن است در شبکه وجود داشته باشد، مشخص می‌شود. در [۵] با توجه به این‌که شبکه مورد یک حمله سایبری از نوع تزریق اطلاعات غلط قرارگرفته، راه‌کاری ارائه‌شده که در این شرایط وضعیت ادوات سایبری- فیزیکی سامانه به‌درستی تخمین زده شود.

یکی دیگر از مباحث مرتبط با حملات سایبری بحث دفاع در برابر این حملات است؛ یعنی پس از تشخیص اتفاق افتادن حمله سایبری، باید راه‌کارهایی ارائه شود که بتوان از این شبکه‌ها در برابر این حملات دفاع کرد. در [۶] به بررسی دفاع در برابر حملات از نوع تزریق داده غلط بر روی تخمین متغیرهای حالت سامانه پرداخته‌شده است. ازجمله مسائل مهمی که در این مقاله موردبررسی قرارگرفته این است که کدام‌یک از اندازه‌گیرها محافظت شوند تا سامانه آسیب کمتری ببیند. همچنین مسئله تأثیر انتخاب PMU محافظت‌شده بر روی بودجه دفاعی سامانه موردبررسی قرارگرفته. به این معنی که کدام‌یک از PMU ها محافظت شود تا بودجه دفاعی افزایش کمتری داشته باشد.

در این مقاله بر روی ساختار حملات سایبری غیرقابل تشخیص بحث شده است. درنتیجه حمله‌ای که در اینجا موردبررسی قرارگرفته یک حمله از نوع تزریق داده غلط به شکلی است که مدافع قابلیت تشخیص این حمله را نداشته باشد. پس ابتدا در مورد نحوه انجام یک حمله سایبری غیرقابل تشخیص بحث شده است. بحث حمله سایبری در اینجا از دیدگاه مهاجم مطرح‌شده است؛ یعنی سعی بر این است که حمله سایبری ترتیب داده شود که بدون اینکه مدافع متوجه آن بشود (بدون اینکه تغییر یا تناقضی در مقادیر متغیرهای حالت یا پارامترهای اندازه‌گیری شده وجود داشته باشد) مقادیر اندازه‌گیری شده PMU ها و درنتیجه حالت‌های تخمین زده‌شده تخریب شوند. یکی از اطلاعاتی که مهاجم برای انجام چنین حمله‌ای به آن نیاز دارد، اطلاعات کامل نسبت به ساختار شبکه مدافع است. پس باید به این نکته توجه کرد که برای انجام حمله غیرقابل تشخیص به یک شبکه نیاز به داشتن اطلاعات از آن شبکه است.

یکی از مواردی که در تعیین میزان اثرپذیری حمله مؤثر است منطقه حمله است. این بدان معنی است که کدام‌یک از اندازه‌گیرهای سامانه تخریب شود تا بیشترین تأثیر مخرب را بر روی شبکه مدافع بگذارد. در این مقاله الگوریتمی ارائه‌شده که با استفاده از آن می‌توان بهترین ناحیه برای دستیابی به بیشترین آسیب را مشخص نمود. شبیه‌سازی‌هایی انجام‌شده تا تأثیر این حملات در شرایط مختلف حمله موردبررسی قرار گیرد.

۲. روش تحقیق

تخمین حالت سامانه یکی از موارد مهم در مدیریت انرژی یک سامانه است. برای دست‌یابی به این مهم مرکز کنترل سامانه قدرت اطلاعات اندازه‌گیری شده را از RTUها (Terminal Unit Remote) دریافت می‌کنند. اطلاعاتی که RTUها به ما می‌دهند شامل توان اکتیو و راکتیو تزریقی به شین‌ها، توان اکتیو و راکتیو جاری بین خطوط و ولتاژ و زاویه ولتاژ شین اصلی می‌شود. اطلاعات این اندازه‌گیرها در تخمین حالت سامانه مورداستفاده قرار می‌گیرند. اطلاعات اندازه‌گیری که از این RTUها به‌دست می‌آیند، ممکن است حاوی خطاهای ناشی از اندازه‌گیری باشند. این خطاهای اندازه‌گیری اغلب به شکل تصادفی هستند که منشأ به وجود آمدن آن‌ها می‌تواند نویزهای موجود یا عملکرد غلط ادوات اندازه‌گیری باشد. همان‌طور که مشخص است اگر چنین خطاهایی وجود داشته باشد، این خطاها به یکدیگر وابسته نبوده و روش‌های تخمین حالت می‌توانند حالت سامانه را به‌درستی تخمین بزنند. گذشته از این خطاهای کوچک، ممکن است در مواقعی که اشکالات ارتباطی در سامانه به وجود می‌آید خطاهای بزرگ‌تری نیز وجود داشته باشد. این خطاها نیز به یکدیگر وابسته نبوده و توسط روش‌های تشخیص خطای موجود قابل شناسایی هستند.

در این مقاله بر روی حملات سایبری از نوع تزریق اطلاعات غلط بحث شده که سامانه‌های تشخیص خطا قابلیت شناسایی آن‌ها را ندارند. درواقع این نوع اطلاعات به شکلی هماهنگ شده به سامانه تزریق می‌شوند که سامانه تشخیص خطا را دور می‌زنند. در مقابله با این حملات کارهای متفاوتی انجام می‌شود. در [۷] به بررسی اثرات ناشی از حملات تزریق اطلاعات غلط بر روی سامانه‌ها و نحوه نجات سامانه در برابر این حملات پرداخته‌شده است.

۲-۱. تخمین حالت DC

تخمین حالت DC بر اساس معادله خطی (۱) انجام می‌شود.

$$z = Hx + e \qquad (۱)$$

در این رابطه، $z = (z_1, z_2, \dots, z_m)^T$ بردار اندازه‌گیری است که شامل m اندازه‌گیر است. این اندازه‌گیری‌ها شامل تزریق توان اکتیو به شین‌ها و توان اکتیو جاری بین خطوط انتقال می‌شود. $x = (x_1, x_2, \dots, x_n)^T$ بردار حالت صحیح سامانه است که باید تخمین زده شود. درنتیجه تعداد متغیرهای حالت n متغیر در نظر گرفته‌شده است. H یک ماتریس ژاکوبی $m \times n$ است که تابع خطی اندازه‌گیری نام دارد. H بر اساس ساختار شبکه به‌دست می‌آید. $e = (e_1, e_2, \dots, e_m)^T$ بردار خطای اندازه‌گیری است و R ماتریس قطری است که کوواریانس خطای اندازه‌گیری را نشان می‌دهد.

اگر تعداد اندازه‌گیرها برای تخمین حالت کافی باشد، شبکه قدرت یک شبکه رؤیت پذیر است. الگوریتم‌های متفاوتی برای جایابی اندازه‌گیرها وجود دارد که شبکه را رؤیت‌پذیر کند [۸]. اصولاً تعداد اندازه‌گیرهایی که در شبکه وجود دارد بیش از آن

تعدادی است که برای رؤیت پذیر شدن شبکه موردنیاز است (اغلب $m > n$). در تخمین حالت DC فرض می‌شود که دامنه ولتاژ شین‌ها برابر ۱ است. همچنین ادمیتانس‌های موازی و مقاومت خطوط قابل صرف‌نظر هستند. توان اکتیو جاری بین دو شین از رابطه $P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}}$ قابل‌محاسبه است که در آن X_{ij} راکتانس شاخه بین i و j و همچنین θ_i و θ_j زاویه فاز شین‌های i و j هستند.

$\hat{x}$ که همان حالت تخمین زده‌شده سامانه است به روش DC از کمینه کردن تابع معادله (۲) به‌دست می‌آید.

$$F(x) = (z - Hx)^T R^{-1} (z - Hx) \quad (۲)$$

بردار $\hat{x}$ که تابع بالا را حداقل می‌کند از رابطه (۳) به‌دست می‌آید [۹].

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \quad (۳)$$

۲-۲. تشخیص داده بد و حملات از نوع تزریق داده غلط

ازجمله روش‌هایی که می‌توان برای تشخیص حمله استفاده کرد این است که مقدار باقیمانده $r = z - H\hat{x}$ را به‌دست آورد. برای تشخیص اینکه حمله‌ای اتفاق افتاده یا خیر می‌توان این مقدار باقیمانده را با یک مقدار مشخصی که از قبل با توجه به شرایط مختلف مشخص‌شده مقایسه کرد. این روش به روش تشخیص داده بد مرسوم است. اگر از دید حمله‌کننده نگاه شود، باید حمله به شکلی اتفاق بیفتد که توسط این روش قابل‌تشخیص نباشد. برای انجام چنین حمله‌ای باید اولاً ساختار شبکه مدافع برای حمله‌کننده شناخته‌شده و دقیقاً مشخص باشد (حمله‌کننده از H اطلاعات داشته باشد) و ثانیاً مهاجم قابلیت این را داشته باشد که به‌طور هم‌زمان چند اندازه‌گیر را تخریب کند [۱۰]. اگر مهاجم بتواند بردار اندازه‌گیری را به شکل $z_b = z + a$ تغییر دهد، در صورتی می‌شود سامانه تشخیص مدافع را از کار انداخت که $a = Hc$ باشد. در این رابطه a داده مخربی است که به اندازه‌گیرها اضافه‌شده و c خطای تزریق‌شده به حالت سامانه است. همان‌طور که مشاهده می‌شود مقدار بردار اندازه‌گیری در این حالت تغییر کرده است اما بعد از اعمال شدن این داده مخرب، حالت سامانه‌ای که توسط روش تخمین DC تخمین زده می‌شود به شکل $\hat{x}_{bad} = \hat{x} + c$ تغییر می‌کند. با استفاده از این بردار تخمین حالت مقدار باقیمانده که روش تشخیص حمله از آن استفاده می‌کند به شکل رابطه (۴) به‌دست می‌آید [۱۱].

$$r_{bad} = z_{bad} - H\hat{x}_{bad} = z + a - H(\hat{x} + c) = z - H\hat{x} = r \quad (۴)$$

همان‌طور که مشاهده می‌شود رابطه به‌دست‌آمده برای مقدار باقیمانده با توجه به بردار تخمین حالت پس از حمله با مقدار آن قبل از انجام حمله یکسان است. پس با این روش حمله‌ای اتفاق افتاده که سامانه تشخیص حمله مدافع قابلیت تشخیص آن را ندارد.

۲-۳. تخمین حالت AC و تزریق داده غلط در این حالت

در این حالت برخلاف تخمین حالت DC یک تابع غیرخطی بین اندازه‌گیری‌ها و حالت سامانه وجود دارد. این تابع به شکل (۵) است.

$$z = h(x) + e \quad (۵)$$

در این رابطه، h یک تابع غیرخطی بین بردار اندازه‌گیری (z) و بردار حالت سامانه (x) است. در این حالت بردار x شامل اندازه ولتاژ شین‌ها و زاویه فاز آن‌ها است. در این حالت مهاجم برای اینکه سامانه تشخیص حمله مدافع را بی‌اثر کند باید برداری به شکل $a = h(\hat{x} + c) - h(\hat{x})$ را به بردار اندازه‌گیری اضافه کند. در حالت AC هریک از متغیرهای حالت می‌توانند بر روی مقادیر چهار اندازه‌گیری که ممکن است در اطراف آن‌ها وجود داشته باشد، تأثیر بگذارد. این چهار اندازه‌گیر شامل حس‌گرهای اندازه‌گیری توان اکتیو و راکتیو شین مربوط به آن متغیر حالت و حس‌گرهای اندازه‌گیری توان اکتیو و راکتیو جاری بین آن شین و شین‌های مجاور است. پس نکته مهم در این حالت این است که برای هدف قرار دادن یک متغیر حالتی که مربوط به شین i می‌باشد، اندازه‌گیری‌هایی که باید تخریب شوند P_i، Q_i، P_{ij} و Q_{ij} است که j مجموعه شین‌های متصل به شین i است.

اگر حمله‌کننده بخواهد هم‌زمان چند متغیر حالت را تغیر دهد، نیاز به تخریب تعداد بیشتری کنتور هست. مثلاً اگر حمله‌کننده بخواهد مجموعه K متغیر حالت را تغییر دهد، توان اکتیو و راکتیو تزریقی به این شین‌ها و توان اکتیو و راکتیو بین این شین‌ها و شین‌های اطرافشان باید تخریب شود. به همین خاطر حمله به بیش از یک متغیر حالت ازنظر اقتصادی به‌صرفه نیست، خصوصاً اگر این متغیرها مربوط به دو شینی باشد که فاصله آن‌ها از هم زیاد است. درنتیجه اگر تصمیم بر حمله به بیش از یک متغیر باشد تا حد امکان شین‌هایی انتخاب می‌شود که به هم نزدیک باشند [۱۲].

در انجام یک حمله غیرقابل تشخیص دو چیز باید مشخص شود. در مرحله اول باید مشخص شود که کدام‌یک از اندازه‌گیرها باید تخریب شود و در مرحله دوم مقادیر این تغییرات مشخص می‌شوند. در تخمین حالت AC همه اندازه‌گیرهایی که با شین تخریب‌شده در ارتباط هستند، باید تخریب شوند. در حالت DC ماتریس H ماتریسی بود که نشان می‌داد کدام اندازه‌گیری با کدام متغیر حالت در ارتباط است. در تخمین حالت AC همان‌طور که

اشاره شد رابطه بین متغیرهای حالت و مقادیر اندازه‌گیری شده یک رابطه غیرخطی است. در اینجا ماتریس ژاکوبی $h(x)$ که به شکل (۶) تعریف می‌شود مشخص می‌کند که کدام‌یک از اندازه‌گیرها به کدام‌یک از متغیرهای حالت وابسته است. به این شکل که اگر اندازه‌گیری به متغیر حالتی وابسته باشد، سطر مربوط به آن اندازه‌گیر در ستون آن متغیر حالت غیر صفر است؛ یعنی اگر اندازه‌گیری به متغیر حالتی وابسته نباشد، درایه مربوط به آن در ماتریس برابر صفر است [۱۳].

$$J_h = \begin{bmatrix} {dh_1}/{dx_1} & {dh_1}/{dx_2} & \cdots & {dh_1}/{dx_n} \\ \vdots & \vdots & \ddots & \vdots \\ {dh_m}/{dx_1} & {dh_m}/{dx_2} & \cdots & {dh_m}/{dx_n} \end{bmatrix} \quad (۶)$$

با بررسی این ماتریس می‌توان با توجه به مقادیر غیر صفر هر ستون متوجه شد که برای تغییر در یک متغیر حالت حداقل چه تعداد اندازه‌گیر باید تخریب شود (درواقع به تعداد عناصر غیر صفر موجود در هر ستون). بعدازاینکه مشخص شد که کدام اندازه‌گیرها باید تغییر کنند سؤال مهم دیگری که وجود دارد این است که مقادیر جدید آن‌ها چه مقداری باید باشد.

مقادیر توان اکتیو (P_{ij}) و راکتیو (Q_{ij}) جاری در خطوط از معادلات (۷) و (۸) قابل‌دستیابی است.

$$P_{ij} = V_i^2.g_{ij} - V_iV_jg_{ij}\cos(\theta_i-\theta_j) - V_iV_jb_{ij}\sin(\theta_i-\theta_j) \quad (۷)$$

$$Q_{ij} = -V_i^2.(b_{ij}+b_{ij}^{sh}) + V_iV_jb_{ij}\cos(\theta_i-\theta_j) - V_iV_jg_{ij}\sin(\theta_i-\theta_j) \quad (۸)$$

در این روابط V_i ولتاژ شین iام که به‌عنوان شین مبدأ در نظر گرفته‌شده و V_j ولتاژ شین jام که شین مقصد خط انتقال است در نظر گرفته‌شده است. همچنین g_{ij} و b_{ij} پارامترهای مربوط به ادمیتانس سری خطوط انتقال و b_{ij}^{sh} پارامتر مربوط به ادمیتانس موازی خط انتقال می‌باشد. θ_i و θ_j نیز به ترتیب مقادیر اندازه فاز شین‌های مبدأ و مقصد هستند. همچنین مقادیر توان اکتیو و راکتیو تزریقی به شین‌ها از روابط (۹) و (۱۰) محاسبه می‌شوند.

$$P_i = \sum_{j\in\vartheta_i} P_{ij} \quad (۹)$$

$$Q_i = \sum_{j\in\vartheta_i} Q_{ij} \quad (۱۰)$$

در این روابط ϑ_i مجموعه شین‌های متصل به شین i می‌باشد. مشابه حالت DC انتخاب ستون و اندازه‌گیری که باید تنظیم شود، متغیر حالتی که باید تخریب شود را تعیین می‌کند. فرض شود که مهاجم برای تخریب V_i به‌عنوان متغیر حالت سعی می‌کند که توان انتقالی بین شین‌های i و j را تغییر دهد، در این صورت معادله (۱۱) باید حل شود تا مشخص شود که دامنه ولتاژی که به توان جاری مدنظر منجر می‌شود چقدر است.

$$P_{ij} = V_{i,a}^2.g_{ij} - V_{i,a}V_j.g_{ij}\cos(\theta_i-\theta_j) - V_{i,a}V_j.b_{ij}\sin(\theta_i-\theta_j) \quad (۱۱)$$

در این رابطه زیر وند a متغیر حالتی را نشان می‌دهد که توسط حمله‌کننده تحت تأثیر قرار می‌گیرد. معادله (۱۱) یک معادله درجه دوم است که دو جواب دارد. در اغلب موارد فقط یکی از پاسخ‌ها با توجه به شرایط قابل‌پذیرش هستند. در آنالیز DC مهاجم نیازی به دانستن مقادیر متغیرهای حالت ندارد اما در حالت AC این‌گونه نیست؛ یعنی علاوه بر اینکه باید معادله (۱۱) را حل کند باید مقادیر V_j و $\theta_i-\theta_j$ را نیز تخمین بزند.

با مشخص شدن مقدار $V_{i,a}$ مقادیر دیگر اندازه‌گیرها نیز توسط روابط (۷) و (۸) قابل‌دستیابی هستند. در آنالیز AC یک گزینه دیگری که وجود دارد این است که θ_i به‌عنوان متغیر حالتی در نظر گرفته شود که باید تخریب شود. با توجه به این حقیقت که حساسیت توان‌های جاری در خطوط و توان‌های تزریقی به شین‌ها نسبت به زاویه ولتاژ بیشتر از اندازه ولتاژ است، با ایجاد تغییرات کمتر در زاویه ولتاژ، تأثیر بیشتری روی توان جاری در خطوط گذاشته می‌شود. طبیعتاً اگر هر دو آن‌ها (هم‌اندازه و هم زاویه ولتاژ) به‌عنوان متغیر حالت تخریب‌شده در نظر گرفته شوند، مجموعه جواب‌های ممکن بزرگ‌تر می‌شود. در این حالت برای اینکه تغییرات اندازه‌گیرهایی که در مرحله اول گفته شد منجر به یک حمله مخفی (غیرقابل تشخیص) شود باید شرایط معادله (۱۲) را داشته باشد. در این شرایط سامانه تشخیص اطلاعات غلط نمی‌تواند انجام حمله را تشخیص دهد [۱۴].

$$\|z_{bad}-h(\hat{x}_{bad})\| = \|z+a-h(\hat{x}+c)\| = \left\|\begin{pmatrix} z_1 \\ z_2+a_2 \end{pmatrix} - \begin{pmatrix} h_1(\hat{x}) \\ h_2(\hat{x}_1,\hat{x}_2+c) \end{pmatrix}\right\| = \left\|\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} - \begin{pmatrix} h_1(\hat{x}) \\ h_2(\hat{x}_1,\hat{x}_2) \end{pmatrix}\right\| = \|z-h(\hat{x})\| < \tau \quad (۱۲)$$

در این رابطه متغیرهایی که زیر وند ۱ دارند مربوط به اندازه‌گیری‌ها و متغیرهای حالتی هستند که توسط مهاجم تغییر داده نشده‌اند. متغیرهایی که زیر وند ۲ دارند آن‌هایی هستند که تخریب‌شده‌اند. بردار a مربوط به تغییرات موردنیاز در اندازه‌گیرهای موردحمله قرارگرفته و بردار c مربوط به تغییرات در متغیرهای حالت تخمین زده‌شده می‌باشند.

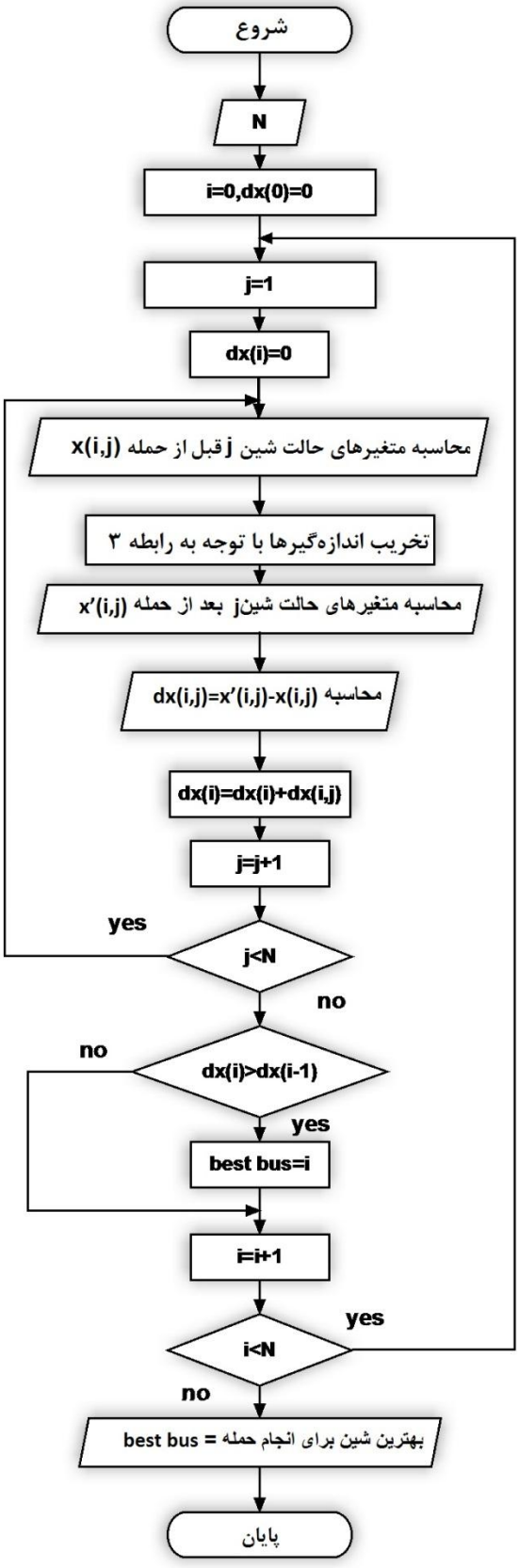
از معادله (۱۲) نتیجه می‌شود که بردار تغییر در اندازه‌گیری که نتیجه آن حمله غیرقابل تشخیص است به شکل (۱۳) می‌باشد.

$$a_2 = h_2(\hat{x}_1,\hat{x}_2+c) - h_2(\hat{x}_1,\hat{x}_2) \quad (۱۳)$$

درنتیجه در حالت AC مهاجم باید مقادیر تخمین زده‌شده برای مجموعه متغیرهای حالتی که در h_2 وجود دارد را بداند.

۲-۴. ارائه الگوریتم شناسایی آسیب‌پذیرترین شین

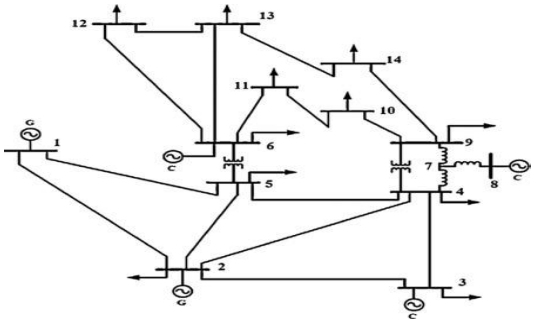
شکل حمله به یک شبکه قدرت می‌تواند اثرات مختلفی بر روی شبکه بگذارد. یکی از مواردی که در میزان اثرگذاری یک حمله سایبری مؤثر است قسمتی از شبکه است که تحت حمله قرار می‌گیرد. در این بررسی فرض بر این است که هیچ‌یک از شین‌های شبکه تحت مطالعه (به‌جز شین شماره ۱) شین‌های حفاظت‌شده نیستند (منظور شین‌هایی هستند که کنترل‌گر شبکه مدافع از صحت اطلاعات ارسالی توسط آن‌ها اطمینان دارد). درنتیجه تزریق داده غلط به‌منظور تخریب بردار اندازه‌گیری می‌تواند بر روی هر یک از شین‌ها اتفاق افتد. سؤالی که مطرح می‌شود این است که حمله سایبری بر روی کدام شین اتفاق افتد که بیشترین مقدار آسیب را به شبکه مدافع وارد کند. البته نکته مهم دیگری که وجود دارد این است که منظور از بیشترین آسیب چیست. بیشترین آسیب می‌تواند از دو دیدگاه در نظر گرفته شود که به هدف مهاجم برمی‌گردد. در برخی انواع حمله‌ها هدف مهاجم تعداد متغیر حالت تخریب‌شده بیشتر نیست و فقط دامنه تغییر یک متغیر حالت مدنظر است؛ یعنی در این حالت مهاجم از بین گزینه‌های مختلف حمله به شین‌ها به دنبال آن شینی می‌گردد که بیشترین تغییر را در یک متغیر حالت ایجاد می‌کند؛ اما در حالت کلی و ازنظر کنترل شبکه بیشترین تخریب زمانی در شبکه مدافع ایجاد می‌شود که بیشترین تعداد متغیر حالت دچار بیشترین تغییر شود. پس در این مقاله بدین منظور الگوریتمی ارائه‌شده که از بین شین‌های مختلف یک شبکه، شینی که حمله به آن باعث بیشترین تغییر کلی در مقادیر متغیرهای حالت شبکه می‌شود را مشخص می‌کند. ذکر این نکته نیز مهم است که در این محاسبه نوع حمله به‌تمامی شین‌ها یکسان در نظر گرفته می‌شود. همچنین فرض شده که ازنظر محدودیت یا هزینه انجام حمله هیچ تفاوتی بین شین‌های مختلف شبکه وجود ندارد. اگر میزان هزینه حمله به شین‌های مختلف شبکه برای ایجاد تغییر یکسان در متغیرهای حالت آن‌ها متفاوت باشد باید هزینه حمله نیز در الگوریتم در نظر گرفته شود. الگوریتم انتخاب بهترین شین در جهت ایجاد بیشترین آسیب در شبکه مدافع در شکل (۱) نشان داده‌شده است. تصمیم‌گیری این الگوریتم بر اساس اطلاعات به‌دست‌آمده پس از انجام تخمین حالت در سامانه به‌دست‌آمده است. منظور از تخمین حالت در اینجا همان تخمین حالت AC است.



شکل ۱. الگوریتم شناسایی آسیب‌پذیرترین شین شبکه مدافع در جهت تخریب مقادیر متغیرهای حالت

۳. نتایج و بحث

در این مقاله یک شبکه ۱۴ شینِ IEEE برای انجام شبیه‌سازی مورداستفاده قرار می‌گیرد. ساختار چنین ریز شبکه‌ای در شکل (۲) نشان داده‌شده است. اطلاعات فنی مربوط به این ریزشبکه در [۱۵] ارائه شده است. شین‌های ۱ تا ۵ به ژنراتورها متصل هستند که می‌توانند یکی از انواع منابع تولید پراکنده در نظر گرفته شوند. در ابتدا با توجه به مقادیر توان اکتیو و راکتیو ارسالی از اندازه‌گیرها مقادیر متغیرهای حالت سامانه تخمین زده می‌شود. توان‌های اکتیو و راکتیو تزریقی به شین‌های ۳، ۴، ۸، ۱۰، ۱۱، ۱۲ و ۱۴ توسط اندازه‌گیرهای این شین‌ها در دسترس هستند. شماره اندازه‌گیرهای توان اکتیو در بردار اندازه‌گیری از ۳ تا ۹ و شماره اندازه‌گیرهای توان راکتیو از ۱۰ تا ۱۶ است. همچنین اندازه‌گیرهایی در این شبیه‌سازی بر روی خطوط (۱ و ۲)، (۲ و ۳)، (۴ و ۲)، (۴ و ۷)، (۵ و ۲)، (۶ و ۱۳)، (۱۱ و ۶) و (۱۲ و ۱۳) قرارگرفته و توان‌های اکتیو و راکتیو جاری بین خطوط را اندازه‌گیری می‌کنند. شماره اندازه‌گیرهای توان اکتیو این خطوط از ۱۷ تا ۲۴ و اندازه‌گیرهای توان راکتیو از ۲۵ تا ۳۲ در بردار اندازه‌گیری می‌باشد. اندازه‌گیرهای شماره ۱ و ۲ نیز بر روی شین یک برای اندازه‌گیری اندازه و زاویه ولتاژ قرار دارد.



شکل ۲. ساختار ریز شبکه استاندار ۱۴ شین IEEE [۱۵]

یکی از مسائلی که در بحث حملات سایبری می‌تواند موردتوجه قرار گیرد مکان‌های قرارگیری این اندازه‌گیرها است. درواقع از دید مدافع با تغییر جایگاه این اندازه‌گیرها می‌توان در برابر حملات سایبری احتمالی به تخریب‌های کمتر دست‌یافت. پس یکی از مباحثی که می‌تواند موردتوجه قرار گیرد کمینه کردن اثر یک حمله خاص بر روی شبکه با تغییر آرایش قرارگیری PMU ها است. چون در این مقاله منافع مهاجم مدنظر قرارگرفته شده و انجام یک حمله با حداکثر میزان تخریب در شبکه مدافع مدنظر است، با در نظر گرفتن مکان‌های متفاوت برای تخریب داده اثرات حمله‌بر روی شین‌های مختلف بررسی‌شده و بهترین حالت حمله از دید مهاجم به‌دست می‌آید.

در حالت عادی و بدون اتفاق افتادن حمله مقادیری که برای متغیرهای حالت این شبکه با استفاده از اطلاعات PMU ها تخمین زده می‌شود در جدول (۱) نشان داده‌شده است. مقادیر جداول و نتایج همه شبیه‌سازی‌های این مقاله در فضای نرم‌افزار MATLAB انجام‌شده است.

جدول ۱. متغیرهای حالت شبکه بدون اتفاق افتادن حمله

شماره شین	دامنه ولتاژ	اندازه فاز
۱	۱,۰۶۰۰	۰,۰۰۰۰
۲	۱,۰۴۵۰	-۴,۹۸۰۰
۳	۱,۰۱۰۰	-۱۲,۷۲۰۰
۴	۱,۰۱۸۶	-۱۰,۳۲۰۰
۵	۱,۰۲۰۳	-۸,۷۸۰۰
۶	۱,۰۶۹۸	-۱۴,۲۲۰۰
۷	۱,۰۶۱۹	-۱۳,۳۷۰۰
۸	۱,۰۹۰۰	-۱۳,۳۷۰۰
۹	۱,۰۵۶۱	-۱۴,۹۵۰۰
۱۰	۱,۰۵۱۱	-۱۵,۱۰۰۰
۱۱	۱,۰۵۶۹	-۱۴,۸۰۰۰
۱۲	۱,۰۵۵۰	-۱۵,۰۸۰۰
۱۳	۱,۰۵۰۲	-۱۵,۱۶۰۰
۱۴	۱,۰۳۵۶	-۱۶,۰۴۰۰

همچنین در این حالت مقادیر اندازه‌گیری شده PMU ها در جدول (۲) نشان داده شده است.

جدول ۲. مقادیر اندازه‌گیری شده PMUها بدون وجود حمله

شماره PMU	مقدار	شماره PMU	مقدار
۱	۱,۰۶۰۰	۱۷	۱,۵۶۸۳
۲	۰	۱۸	۰,۷۳۱۹
۳	-۰,۹۴۲۰	۱۹	-۰,۵۴۴۶
۴	-۰,۴۷۸۰	۲۰	۰,۲۸۰۹
۵	۰	۲۱	-۰,۴۰۶۱
۶	-۰,۰۹۰۰	۲۲	۰,۱۷۷۴
۷	-۰,۰۳۵۰	۲۳	-۰,۷۲۸
۸	-۰,۰۶۱۰	۲۴	۰,۰۱۶۱
۹	-۰,۱۴۹۰	۲۵	-۰,۲۰۳۹
۱۰	۰,۰۴۳۹	۲۶	۰,۰۳۵۷
۱۱	۰,۰۳۹۰	۲۷	۰,۰۳۳۹
۱۲	۰,۱۷۳۶	۲۸	-۰,۰۹۴۲
۱۳	-۰,۰۵۸۰	۲۹	-۰,۰۱۶۳
۱۴	-۰,۰۱۸۰	۳۰	۰,۰۷۱۶
۱۵	-۰,۰۱۶۰	۳۱	-۰,۰۳۳۵
۱۶	-۰,۰۵۰۰	۳۲	۰,۰۰۷۴

همان‌طور که اشاره شد مهاجم باید نسبت به پارامترها و ساختار شبکه مدافع اطلاعات کامل داشته باشد. همچنین ایجاد

تغییر در این پارامترها با توجه به سامانه‌های امنیتی و حفاظتی مدافع پروسه‌ای هزینه‌بر است. پس مهاجم برای ایجاد تغییر در این پارامترها نیاز به‌صرف هزینه دارد. طبیعتاً هرچه میزان هزینه مدافع در جهت به کار بردن لایه‌های دفاعی بیشتر، مقادیر بالاتری باشد، مهاجم برای انجام حمله و نفوذ در شبکه اطلاعاتی مدافع باید هزینه بیشتری مصرف کند. همچنین میزان تغییر در این پارامترها و تعداد پارامترهای تغییریافته با میزان هزینه لازم جهت حمله نسبت مستقیم دارد. در این مقاله فرض بر این است که مهاجم تنها می‌تواند یکی از متغیرهای حالت را تخریب کند. این بدان معنی است که بردار c که در حالت حمله به بردار $\hat{x}$ افزوده می‌شود فقط دارای یک درایه غیر صفر است.

حمله سایبری در نظر گرفته می‌شود که مقدار مربوط به سطر شماره ۱۰ بردار تخمین حالت را به میزان ده درصد افزایش دهد؛ یعنی بردار c در این حمله به شکل $c = [0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0.1\hat{x}(10)\ 0\ 0\ 0\ 0]$ می‌باشد. مقادیر متغیرهای حالت تخمین زده‌شده پس از انجام این حمله سایبری در جدول (۳) نشان داده شده است. درواقع مقادیر این جدول عناصر بردار $\hat{x}_{bad}$ می‌باشد.

جدول ۳. مقادیر متغیرهای حالت تخمین زده‌شده بعد از حمله سایبری بر روی شین شماره ۱۰

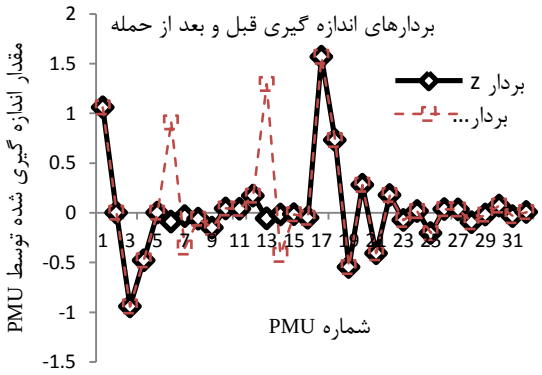
شماره شین	دامنه ولتاژ	اندازه فاز
۱	۱,۰۶۰۰	۰,۰۰۰۰
۲	۱,۰۴۵۰	-۴,۹۸۰۰
۳	۱,۰۱۰۰	-۱۲,۷۲۰۰
۴	۱,۰۱۸۶	-۱۰,۳۲۰۰
۵	۱,۰۲۰۳	-۸,۷۸۰۰
۶	۱,۰۵۶۷	-۱۴,۲۳۰۰
۷	۱,۰۶۱۹	-۱۳,۳۷۰۰
۸	۱,۰۹۰۰	-۱۳,۳۷۰۰
۹	۱,۰۵۶۱	-۱۴,۹۵۰۰
۱۰	۱,۱۳۷۳	-۱۳,۷۸۰۰
۱۱	۱,۰۴۳۶	-۱۴,۸۲۰۰
۱۲	۱,۰۴۱۷	-۱۵,۱۱۰۰
۱۳	۱,۰۳۶۹	-۱۵,۱۹۰۰
۱۴	۱,۰۲۹۷	-۱۶,۰۷۰۰

همچنین بردار اندازه‌گیری که در این حالت به‌دست می‌آید به شکل جدول (۴) است. مقادیر جدول (۴) همان z_{bad} هستند که از روی c و درنتیجه مقدار a به‌دست‌آمده از آن به‌دست‌آمده است. بردار z_{bad} درواقع برداری است که مهاجم باید برای عدم‌تشخیص تغییر متغیر حالت دهم توسط مدافع مقادیر این بردار را تنظیم کند. یعنی بردار اندازه‌گیری z باید توسط مهاجم به z_{bad} تبدیل شود.

جدول ۴. مقادیر اندازه‌گیری شده توسط PMUها بعد از انجام حمله سایبری (این مقادیری است که مهاجم باید برای PMUها تنظیم کند)

شماره PMU	مقدار	شماره PMU	مقدار
۱	۱,۰۶۰۰	۱۷	۱,۵۶۸۳
۲	۰	۱۸	۰,۷۳۱۹
۳	-۰,۹۴۲۰	۱۹	-۰,۵۴۴۶
۴	-۰,۴۷۸۰	۲۰	۰,۲۸۰۹
۵	۰	۲۱	-۰,۴۰۶۱
۶	۰,۹۰۹۱	۲۲	۰,۱۷۷۴
۷	-۰,۳۵۰۶	۲۳	-۰,۷۲۸
۸	-۰,۰۶۱۰	۲۴	۰,۰۱۶۱
۹	-۰,۱۴۹۰	۲۵	-۰,۲۰۳۹
۱۰	۰,۰۴۳۹	۲۶	۰,۰۳۵۷
۱۱	۰,۰۳۹۰	۲۷	۰,۰۳۳۹
۱۲	۰,۱۷۳۶	۲۸	-۰,۰۹۴۲
۱۳	۱,۲۹۴۵	۲۹	-۰,۰۱۶۳
۱۴	-۰,۴۲۳۰	۳۰	۰,۰۷۱۶
۱۵	-۰,۰۱۶۰	۳۱	-۰,۰۳۳۵
۱۶	-۰,۰۵۰۰	۳۲	۰,۰۰۷۴

برای درک بهتر اندازه‌گیرهایی که باید مقادیر آن‌ها تغییر کند این دو بردار در شکل (۳) باهم مقایسه شده‌اند.

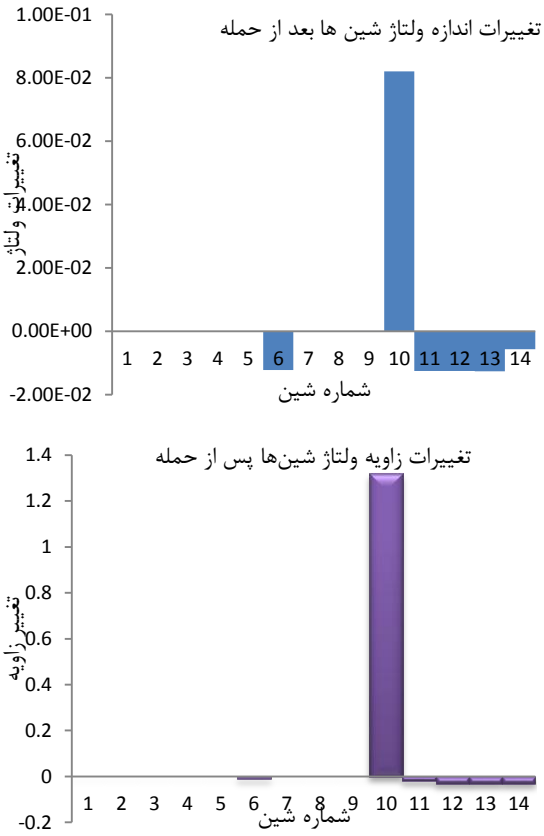


شکل ۳. مقایسه بردار z و z_{bad}

چنانچه مشخص است مهاجم برای انجام حمله اشاره‌شده باید مقدار اندازه‌گیری‌شده توسط ۴ اندازه‌گیر را تخریب کند. درصورتی‌که مهاجم چنین حمله‌ای انجام دهد، در مقادیر متغیرهای حالت تخمین زده‌شده سامانه تغییراتی ایجاد می‌شود. میزان تأثیرگذاری حمله با توجه به میزان انحراف مقادیر متغیرهای حالت تخمین زده‌شده بعد از انجام این تغییرات با مقدار تخمین زده‌شده قبل از حمله آن‌ها مشخص می‌شود.

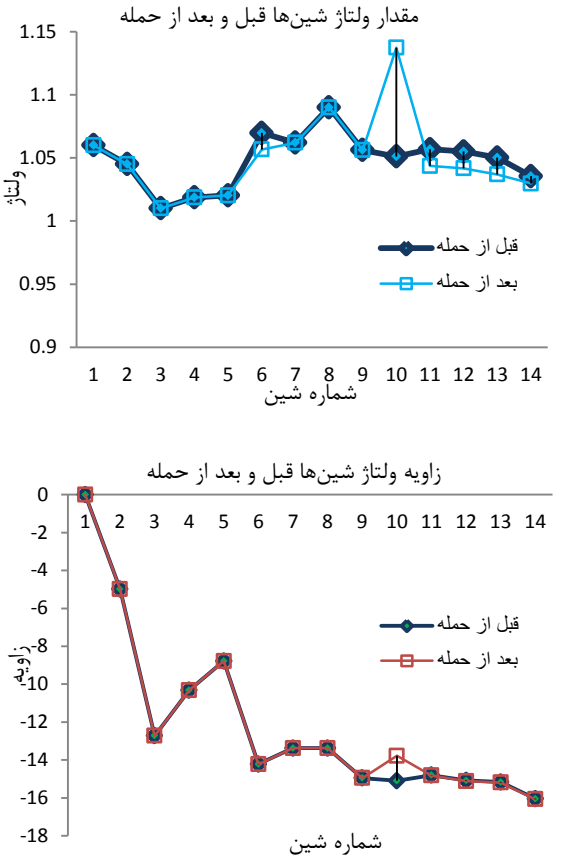
حمله سایبری به شکلی اتفاق می‌افتد که سامانه تشخیص حمله مدافع متوجه اتفاق افتادن این حمله نمی‌شود. میزان تغییرات ولتاژ و زاویه ولتاژ شین‌ها در شکل (۴) نشان داده شده

است. همچنین دیاگرام تغییرات متغیرهای حالت در شکل (۵) نشان داده‌شده است.



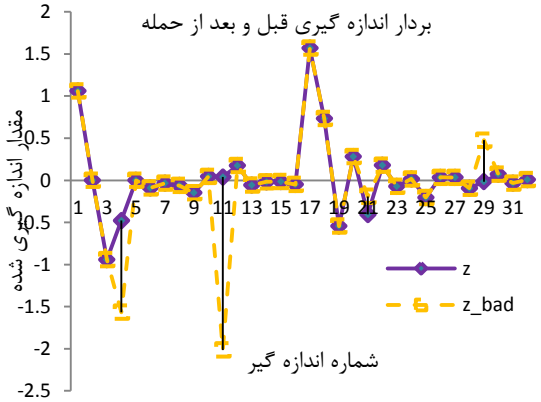
شکل ۴. تغییرات اندازه و زاویه ولتاژ پس از انجام حمله سایبری بر روی شین شماره ۱۰

همان‌گونه که مشخص است علاوه بر شین شماره ۱۰ مقادیر تخمین زده‌شده مربوط به ۵ شین دیگر نیز تخریب‌شده و سامانه مدافع بر اساس این مقادیر برای شبکه تصمیم‌گیری خواهد کرد. با انجام شبیه‌سازی حمله سایبری بر روی همه شین‌های شبکه می‌توان در هر حالت به اطلاعات مشابهی دست‌یافت. با مقایسه این حالت‌ها و استفاده از الگوریتم‌های بهینه‌سازی می‌توان به بهترین شین از دید مهاجم که باید موردحمله قرار گیرد دست‌یافت. قطعاً بهترین حمله از دید مهاجم حمله‌ای است که در آن با تخریب کمترین اندازه‌گیر، بیشترین میزان تغییر در متغیرهای حالت سامانه را ایجاد کند. الگوریتم ارائه‌شده در این مقاله در این زمینه کمک می‌کند که بهترین شین برای حمله را شناسایی کنیم. برای شبکه‌ای با چنین ساختاری حمله به شین شماره ۵ بهترین گزینه برای مهاجم است. اگرچه ازنظر تعداد شین‌هایی که متغیرهای حالتشان تغییر می‌کند و همچنین دامنه تغییرات متغیرهای حالت گزینه‌های بهتری (مثلاً شین شماره ۳) نیز برای حمله وجود دارد اما باید به این نکته توجه شود که با حمله به شین ۵ با تخریب کمترین اندازه‌گیر، بیشترین تغییر قابل‌دست‌یابی خواهد بود.



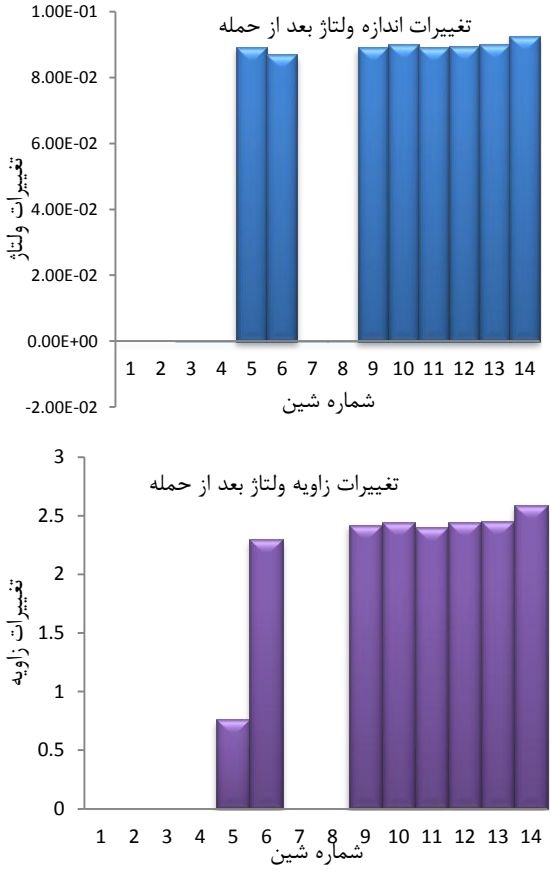
شکل ۵. مقادیر متغیرهای حالت تخمین زده‌شده پیش و پس از انجام حمله سایبری

پس در شرایط یکسان ازنظر میزان تغییر در بردار $\hat{x}$، میزان تخریب شبکه با حمله به شین ۵ چشمگیرتر از حمله به شین شماره ۱۰ می‌باشد.



شکل ۶. اندازه‌گیرهایی که باید توسط مهاجم جهت حمله به شین ۵ تخریب شوند و میزان تغییر آن‌ها

نتایج حمله بر روی شین شماره ۵ در شکل‌های (۶) و (۷) نشان داده‌شده است. شکل (۶) اندازه‌گیرهایی که باید تخریب شوند را نشان می‌دهد. همان‌طور که مشخص است در این حالت نیز مقادیر اندازه‌گیری شده توسط ۴ اندازه‌گیر باید تخریب شوند؛ اما با این تغییر مقادیر متغیرهای حالت تخمین زده‌شده ۸ شین دچار تغییر چشمگیر می‌گردد. این تغییر می‌تواند سامانه‌های کنترلی و حفاظتی شبکه مدافع را به‌طورکلی دچار اختلال و اشتباه کند به‌نحوی‌که پایداری و ثبات شبکه به‌طورکلی از بین برود. در [۱۶] حمله سایبری در دو سناریو مورد بررسی قرار گرفته است. در سناریو اول حمله سایبری مد نظر قرار گرفته که با انجام آن بیشترین هزینه اقتصادی به شبکه مدافع وارد می‌شود. در سناریو دوم، هدف انجام حمله سایبری با بیشترین آسیب به امنیت شبکه و بزرگ‌ترین انحرافات در پخش بار است. در نهایت خطوط انتقالی که انجام حمله بر روی آنها بیشترین آسیب را از این دو منظر به شبکه وارد می‌کنند شناسایی می‌شوند. مشابه مقاله حاضر، نتایج به‌دست‌آمده نشان می‌دهد که بیشترین آسیب زمانی به شبکه مدافع وارد می‌شود که حمله سایبری بیشترین تخریب را در تخمین حالت بیشترین متغیرهای حالت شبکه ایجاد کند.



شکل ۷. تفاوت مقادیر متغیرهای حالت تخمین زده‌شده قبل و بعد از حمله بر روی شین شماره ۵

همان‌طور که مشخص است با توجه به الگوریتم ارائه‌شده بهترین شین جهت انجام حمله شین شماره ۵ بود که بیشترین تغییر را در متغیرهای حالت با کمترین تخریب اندازه‌گیر ایجاد می‌کند.

۴. نتیجه‌گیری

برای ایجاد اختلال در یک شبکه قدرت به‌جای انجام حمله فیزیکی می‌توان از حملات سایبری استفاده کرد. بدین منظور می‌توان از حملات از نوع تزریق داده غلط به شبکه مدنظر استفاده کرد. حمله از نوع تزریق اطلاعات غلط می‌تواند موجب تخمین حالت نادرست و درنتیجه تصمیم‌گیری‌های غلط در شبکه گردد. در این مقاله بر روی حمله سایبری بر روی شبکه قدرت بدون قابلیت تشخیص مدافع بحث شد؛ یعنی حمله از نوع تزریق داده غلطی که سامانه تشخیص حمله مدافع متوجه آن نمی‌شود. درنتیجه در این مقاله منافع مهاجم مدنظر قرارگرفته است. پس از بررسی روش تزریق داده غلط و تغییر متغیرهای حالت سامانه، شبیه‌سازی‌هایی بر روی یک شبکه نمونه صورت گرفت و نتایج این شبیه‌سازی‌ها با تغییر نقطه حمله موردبررسی قرار گرفت. به شکلی که بهترین نقطه برای انجام حمله سایبری بر روی شبکه مدافع مشخص شد. برای تشخیص بهترین نقطه حمله الگوریتمی ارائه شد که این الگوریتم با واردکردن اطلاعات شبکه موردحمله، بهترین شین را جهت حمله معرفی می‌کند. یکی از مواردی که در راستای این مقاله می‌تواند موردبررسی قرار گیرد بحث روش‌های تشخیص حمله و دفاع در برابر حملات سایبری است. درواقع به‌جای در نظر گرفتن منافع حمله‌کننده می‌توان منافع مدافع را در جهت آسیب کمتر در برابر حملات سایبری در نظر گرفت. به‌عنوان‌مثال ازنظر مدافع می‌توان با تغییر مکان قرارگیری اندازه‌گیرهایی که مقادیر اندازه گرفته‌شده توسط آن‌ها مطمئن هستند، می‌توان به بهترین مکان برای قرارگیری آن‌ها در جهت کاهش اثرات حملات سایبری دست‌یافت. با توجه به الگوریتم ارائه‌شده، برای شبکه ۱۴ شین موردبررسی در این مقاله بهترین شین برای انجام حمله شین شماره ۵ است. اگرچه که به‌عنوان‌مثال با تخریب متغیرهای حالت شین شماره ۳ میزان کلی تغییر در متغیرهای حالت تخمین زده‌شده بیشتر است، اما در این حالت تعداد اندازه‌گیرهایی که مقدار آن‌ها باید تغییر کند بیشتر است و درنتیجه انجام حمله هزینه بیشتری خواهد داشت. درنتیجه با استفاده از الگوریتم ارائه‌شده با انجام یک حمله از نوع تزریق داده غلط به‌صورتی که قابلیت تشخیص برای مدافع ندارد می‌توان تأثیرگذارترین حمله به شبکه مدافع را ایجاد کرد.

۵. مرجع‌ها

[1] Wang, Y.; Amin, M. M.; Fu, J.; Moussa, H. B. “A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids”; IEEE Access 2017, 5, 26022-26033.

[2] He, Y.; Mendis, G. J.; Wei, J. “Real-Time Detection of False Data Injection Attacks in Smart Grid: a Deep Learning-Based Intelligent Mechanism”; IEEE Trans. Smart Grid 2017, 8, 2505-2516.

[3] Asgari, A.; Firouzjah, K. G. “Optimal PMU Placement for Power System Observability Considering Network Expansion and$N-1$ Contingencies”; IET Gener. Transm. Distrib. 2018, 12, 4216-4224.

[4] Lu, C.; Wang, Z.; Ma, M.; Shen, R.; Yu, Y. “An Optimal PMU Placement with Reliable Zero Injection Observation”; IEEE Access 2018, 6, 54417-54426.

[5] Guan, Y.; Ge, X. “Distributed Attack Detection and Secure Estimation of Networked Cyber-Physical Systems Against False Data Injection Attacks and Jamming Attacks”; IEEE Trans. Signal Inf. Process. Networks 2018, 4, 48-59.

[6] Deng, R.; Xiao, G.; Lu, R. “Defending Against False Data Injection Attacks on Power System State Estimation,” IEEE Trans. Ind. Inf. 2017, 13, 198-207.

[7] Deng, R.; Xiao, G.; Lu, R.; Liang, H.; Vasilakos, A. V. “False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: a Survey”; IEEE Trans. Ind. Inf. 2017, 13, 411-423.

[8] Monticelli, A. “State Estimation in Electric Power Systems a Generalized Approach”; Kluwer Academic Publishers, 1999.

[9] Huang, Y.; Tang, J.; Cheng, Y.; Li, H.; Campbell, K. A. “Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis”; IEEE Syst. J. 2016, 10, 532-543.

[10] Gaffarpour, R.; Jam, A.; Ranjbar, A. M. “Optimal Mix of Distributed Generation Allocation to Improve the Security of Energy Supply in Defensive Sites Using Principles of Passive Defence”; Advanced Defence Sci. & Tech. 2015, 7, 19-32. (In Persian).

[11] Bi, S.; Zhang, Y. J. “Graphical Methods for Defense against False-Data Injection Attacks on Power System State Estimation”; IEEE Trans. Smart Grid 2014, 5, 1216-1227.

[12] Zamani Gargari, M.; Ghaffarpour, R. “Increasing Energy Security by Using the Concept of Resiliency in Multi-Energy Infrastructures”; Advanced Defence Sci. & Tech. 2019, 10, 419-432.

[13] He, Y.; Mendis, G. J.; Wei, J. “Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism”; IEEE Trans. Smart Grid 2017, 8, 2505-2516.

[14] Mohammadpourfard, M.; Sami, A.; Weng, Y. “Identification of False Data Injection Attacks With Considering the Impact of Wind Generation and Topology Reconfigurations”; IEEE Trans. Sustainable Energy 2018, 9, 1349-1364.

[15] Taher, S. A.; Mahmoodi, H.; Aghaamouei, H. “Optimal PMU Location in Power Systems Using MICA”; Alex. Eng. J. 2016, 55, 399-406.

[16] Liang, G.; Weller, S. R.; Zhao, J.; Luo, F.; Dong, Z. Y. “A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios”; IEEE Trans. Smart Grid 2017, 10, 1704-1712.

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۴۱۴-۴۰۳

«علمی- پژوهش»

یک سامانه حفاظت ویژه جدید جهت جلوگیری از وقوع ناپایداری ولتاژ بلندمدت در مقابل حملات گرافیتی

سیاوش یاری[۱]، حمید خوشخو[۲*]، عرفان اسدی[۳]

۱- کارشناس ارشد، ۲- استادیار، ۳- دانشجوی کارشناسی ارشد، دانشگاه صنعتی سهند

(دریافت: ۹۸/۱۲/۰۹، پذیرش: ۹۹/۰۲/۳۱)

چکیده

بمب‌های گرافیتی از جمله سلاح‌های غیر مخرب مدرن هستند که با ایجاد اتصال کوتاه در سامانه‌های قدرت منجر به وقوع خاموشی سراسری در این شبکه‌ها می‌شوند. هدف اصلی این مقاله ارائه یک سامانه حفاظت ویژه (SPS) جهت جلوگیری از وقوع ناپایداری ولتاژ بلندمدت پس از حملات گرافیتی است. در این سامانه حفاظت ویژه، برای آنکه اقدامات اصلاحی با هماهنگی مناسبی انجام شود و خطر ناپایداری کاهش یابد، با استفاده از مفهوم فاصله الکتریکی، شبکه قدرت به چند ناحیه کنترل ولتاژ (VCA) تقسیم می‌شود. سپس با توجه به وضعیت پایداری ولتاژ در هر ناحیه که به کمک شاخص RPRI تعیین می‌شود، سامانه حفاظت ویژه ارائه شده برای جلوگیری از ناپایداری ولتاژ بلندمدت مورد استفاده قرار خواهد گرفت. در این مقاله، با استفاده از محیط DPL نرم‌افزار DIgSILENT PowerFactory، سامانه حفاظت ویژه پیشنهاد شده بر روی شبکه‌های IEEE 39-Bus و Nordic32 پیاده‌سازی و آزمایش شده است. نتایج شبیه‌سازی‌های انجام شده در شرایط وقوع اغتشاش‌های N-1، N-2 و N-3 مختلف و مقایسه آن‌ها با روش‌های پیشین، تائید کننده عملکرد مناسب روش پیشنهاد شده است.

کلید واژه‌ها: بمب گرافیتی، ناپایداری ولتاژ بلندمدت، سامانه حفاظت ویژه.

A Novel Special Protection System to Prevent Long-Term Voltage Instability against Graffite Attacks

S. Yari, H. Khoshkhoo*, E. Asadi
Sahand University of Technology
(Received: 28/02/2020; Accepted: 20/05/2020)

Abstract

Graffiti bombs are one of the modern non-destructive weapons that by causing short circuit in the power systems result in blackout in these networks. The main purpose of this paper is to propose a Special Protection System (SPS) to prevent long-term voltage instability after graffite attacks. In this SPS, the power grid is divided into several voltage control area (VCAs) in order to carry out corrective actions in a coordinated manner and reduce the risk of the instability. Then, according to the voltage stability status of each area determined by RPRI index, the proposed SPS will be used to prevent long-term voltage instability. In this paper, using the DPL environment of DIgSILENT PowerFactory software, the proposed SPS is implemented and tested on IEEE 39-Bus and Nordic32 networks. The results of simulations performed under different N-1, N-2 and N-3 contingencies and comparison of them with previous ones verify the appropriate performance of the proposed method.

Keywords: Graffite Bombs, Long Term Voltage Stability, Special Protection System.

*Corresponding Author E-mail: khoshkhoo@sut.ac.ir

۱. مقدمه

در سال‌های اخیر، به دلیل افزایش قابل توجه بارگذاری در شبکه قدرت، نقاط کار این شبکه در سراسر جهان به سمت مرزهای پایداری حرکت کرده‌اند که سبب کاهش امنیت سامانه قدرت در مقابل اغتشاشات و حملات شده است [۳-۱]. یکی از حملات مخرب به تجهیزات شبکه قدرت استفاده از بمب گرافیتی است. این بمب که بنا به درخواست نیروی هوایی آمریکا ساخته شده و اثرات نامطلوبی روی انسان ندارد، نوعی مهمات هوا به زمین است که هدف آن غیرعملیاتی کردن ژنراتورهای شبکه قدرت و خطوط انتقال برق است. این بمب با کمک دستگاه ارتفاع‌سنج در ارتفاع خاصی منفجر می‌شود و ابری از گرافیت با وسعت چند صد متر بر فراز تأسیسات تولید انرژی یا مراکز ارتباطی به‌وجود می‌آورد. این ابر گرافیتی به تدریج در محدوده هدف نشست می‌کند و به علت رسانا بودن موجب ایجاد اتصال‌کوتاه در کلیدها و مدارات و سوختن قطعات دستگاه‌ها می‌شود و به این ترتیب، مراکز تولید انرژی و مخابرات را غیرفعال یا ناتوان می‌کند. اولین بار در سال ۱۹۹۹ ، بمب‌های گرافیتی به‌وسیلهٔ هواپیماهای جنگنده آمریکایی علیه مراکز نیروگاهی و سامانه‌های الکتریکی و الکترونیکی یوگسلاوی به‌کار گرفته شد که ضمن خسارات بسیار سنگین، ۷۰ ٪ کشور را در خاموشی فرو برد.

بمب‌های گرافیتی که تاکنون مورد استفاده قرار گرفته و شناسایی شده‌اند از نظر مواد گرافیتی و عملکرد به دو دسته تقسیم می‌شوند:

- بمب گرافیتی الیافی
- بمب گرافیتی پودری

بمب‌های گرافیتی الیافی عموماً دارای وزنی در حدود ۴۵۰ کیلوگرم بوده و از نظر قیمت در مقایسه با بمب‌های جنگی بسیار ارزان قیمت می‌باشند. عملکرد این بمب‌ها به‌طوری است که بعد از رها شدن از هواپیما، پوسته خارجی آن منفجر شده و الیاف درونی آن خارج شده و در فضا منتشر می‌شود و به تدریج بر روی کابل‌های برق فشارقوی در مراکز نیروگاهی فرود می‌آید و با ایجاد اتصال‌کوتاه و آتش‌سوزی باعث خسارات سنگین به این‌گونه مراکز می‌گردد [۴].

در نوع پودری آن، کپسول از دو قسمت تشکیل می‌شود و به‌وسیله چتر فرود می‌آیند و در میانه راه قسمت پایین کپسول جدا شده و پودر زغالی بسیار نرم و سبکی از آن خارج شده که در فضا منتشر می‌شود و به تدریج روی محل اتصالات مراکز نیروگاهی و پست‌های انتقال و فوق توزیع می‌نشیند و منجر به قطع تمام مدارات و جریانات ارتباطی می‌گردد [۴].

تجهیزات غیر عایقی که در فضای باز قرار می‌گیرند (مانند خطوط انتقال) می‌توانند مورد حمله بمب‌های گرافیتی قرار گیرند. این بمب‌ها با ایجاد اتصال الکتریکی بین تجهیزات شبکه قدرت، موجب وقوع اتصال کوتاه بر روی این تجهیزات می‌شوند. ازاین‌رو، عدم وجود یک سامانه حفاظت گسترده مناسب برای جلوگیری از وقوع ناپایداری‌های مختلف در شبکه قدرت، منجر به وقوع خاموشی سراسری خواهد شد. برای مثال در سال ۱۳۸۲ و در پی حمله ایالات متحده آمریکا به کشور عراق، موشک‌های آمریکایی حامل بمب‌های گرافیتی با اصابت به نیروگاه بصره موجب خاموشی سراسری در این کشور گردیدند. بر این اساس، حفظ پایداری و کنترل عملکرد مناسب شبکه با استفاده از روش‌های مؤثر و بهینه، یکی از الزامات مهم جهت مقابله با حملات مختلف متجاوزگران است [۵].

در همین راستا، همواره روش‌های کنترلی مختلفی در جهت جلوگیری از وقوع ناپایداری در شبکه‌های قدرت ارائه شده‌اند [۷-۶]. در بین این راهبردها، روش‌های مبتنی بر سامانه حفاظت ویژه (SPS[1]) به نظر مؤثرتر و کارآمدتر از سایر روش‌ها هستند. براساس تعریف ارائه‌شده توسط NERC[2]، SPS سامانه حفاظت خودکاری است که به‌منظور شناسایی شرایط غیرطبیعی یا از پیش تعیین‌شده شبکه طراحی می‌گردد، تا با انجام اقدامات اصلاحی از قبل مشخص‌شده (به غیر از جداسازی تجهیزات خطادار که توسط سامانه حفاظت معمول انجام می‌شود) پایداری شبکه قدرت را حفظ کند [۸]. الگوریتم‌های مبتنی بر SPS برای جلوگیری از ناپایداری ولتاژ از برخی اقدامات اصلاحی مانند: بهره‌برداری مؤثر از منابع تولید، حذف بار و کنترل تجهیزات شبکه (مانند سامانه‌های OLTC[3]، AVR[4] و ادوات FACTs[5]) بهره می‌برند. این اقدامات اصلاحی می‌تواند پایداری شبکه‌های قدرت را که سامانه‌های بزرگ، پیچیده و غیرخطی هستند بهبود ببخشند [۱۹-۹].

الگوریتم‌های مبتنی بر SPS به‌طورکلی به ۲ دسته تقسیم می‌شوند [۹]:

- SPSهای مبتنی‌بر رخداد (Event-based)
- SPSهای مبتنی‌بر اندازه‌گیری متغیرهای شبکه (Response-based)

در SPSهای مبتنی بر رخداد، روش کنترلی و اقدامات اصلاحی بر اساس وقوع اغتشاش‌های خاصی طراحی می‌شوند تا در هنگام وقوع این اغتشاشات از وقوع ناپایداری در شبکه قدرت

[1] Special Protection System
[2] North American Electric Reliability Corporation
[3] On Load Tap Changer
[4] Automatic Voltage Regulator
[5] Flexible AC Transmission Systems

جلوگیری شود. SPSهای مبتنی بر اندازه‌گیری متغیرهای شبکه، برخلاف روش قبلی، اقدامات اصلاحی مناسب را مبتنی بر رفتار شبکه و اندازه‌گیری متغیرهای سامانه قدرت (از قبیل ولتاژ شین‌ها و ...) اجرا می‌کنند و از این‌رو عملکرد آنها محدود به اغتشاش خاصی نیست [۹].

در این مقاله یک SPS مبتنی بر اندازه‌گیری متغیرهای شبکه (Response-based)، با استفاده از بانک‌های خازنی، ابزار حذف بار، و کنترل عملکرد تپ‌چنجرهای ترانسفورماتورهای شبکه، جهت پیشگیری از ناپایداری ولتاژ بلندمدت ارائه شده است. بر این اساس، در بخش ۲ از این مقاله، ابزارهای مورد نیاز برای روش پیشنهادی ارائه می‌گردد. در این بخش، ناحیه بندی سامانه قدرت به چندین VCA[1]، تعیین شین‌های ضعیف با استفاده از شاخص پایداری شین SVSI[2]، و بررسی توانایی ژنراتورهای سنکرون برای تولید توان راکتیو با استفاده از شاخص RPRI[3] توضیح داده خواهد شد. سپس در بخش ۳، SPS پیشنهادی ارائه شده است. بخش ۴ نتایج شبیه‌سازی‌ها را ارائه می‌دهد و در بخش ۵ نتیجه‌گیری ارائه خواهد شد.

۲. ابزارهای مورد نیاز

۲-۱. ناحیه بندی شبکه قدرت و مفهوم ناحیه کنترل ولتاژ

برای ارزیابی پایداری ولتاژ، تقسیم شبکه به چندین VCA می‌تواند سبب سهولت نظارت بر پایداری شبکه و اجرای روش‌های کنترل ولتاژ شود [۲۰]. در این مقاله، سامانه قدرت با استفاده از مفهوم فاصله الکتریکی (ED[4]) به چندین VCA تقسیم می‌شود. در این‌روش، ED بین شین n و شین m طبق معادله (۱) محاسبه می‌شود:

$$ED_{mn} = ED_{nm} = -log(a_{mn} \times a_{nm}) \qquad (۱)$$

که در آن، a_{mn} و a_{nm} با استفاده از ماتریس ژاکوبین پخش بار [۲۱] یا ماتریس سوسپتانس قابل محاسبه است [۲۲]:

$$a_{mn} = \left(\frac{\partial V_m}{\partial Q_n}\right) / \left(\frac{\partial V_n}{\partial Q_n}\right); a_{nm} = \left(\frac{\partial V_n}{\partial Q_m}\right) / \left(\frac{\partial V_m}{\partial Q_m}\right) \qquad (۲)$$

۲-۲. تعیین محل نصب خازن‌های موازی در شبکه قدرت با استفاده از شاخص SVSI

در این مقاله برای تعیین ضعیف‌ترین شین‌ها شبکه قدرت جهت نصب خازن‌های موازی از شاخص SVSI استفاده شده است. [۲۳]. در این راستا، SVSI برای همه شین‌ها (در هر VCA) با استفاده از معادله (۳) محاسبه می‌شود و شین‌هایی که دارای مقدار SVSI بیشتری باشند به‌عنوان شین‌های ضعیف تعیین می‌گردند [۲۳]:

$$SVSI_i = \frac{\Delta V_i}{\beta \times V_i} = \frac{\left|\vec{V}g - \vec{V}i\right|}{\beta \times V_i} \qquad (۳)$$

که در آن، V_i ولتاژ شین i و V_g ولتاژ ترمینال نزدیک‌ترین ژنراتور به شین i (که توسط ED تعیین می‌شود) و β به‌عنوان ضریب تصحیح به‌صورت رابطه (۴) محاسبه می‌شود [۲۳]:

$$\beta = 1 - (max(|V_m| - |V_l|))^2 \qquad (۴)$$

ضریب تصحیح β بر اساس بیشترین اختلاف ولتاژ بین دو (m و l) شین از شبکه محاسبه می‌گردد.

۲-۳. ارزیابی ژنراتورهای سنکرون با استفاده از شاخص RPRI

در این مقاله، به‌منظور اجرای اقدامات کنترلی موردنیاز برای حفظ پایداری سامانه، وضعیت پایداری ولتاژ و انتخاب اقدامات اصلاحی بهینه بر مبنای قابلیت ژنراتورهای سنکرون در تولید توان راکتیو موردنیاز بارها ارزیابی می‌شود. به این منظور، طبق معادله (۵) می‌توان با استفاده از شاخص RPRI، وضعیت ژنراتورهای سنکرون شبکه را از منظر قابلیت تولید توان راکتیو اضافی بررسی کرد [۲۴]:

$$RPRI = \min_{i \in G}\left(\frac{Q_i^{max} - Q_i}{Q_i^{max}}\right) \qquad (۵)$$

که در آن، Q_i توان راکتیوی است که توسط ژنراتورهای سنکرون تولید می‌شود و Q_i^{max} حداکثر توان راکتیو است که می‌تواند توسط ژنراتور سنکرون تولید شود و بر اساس رابطه (۶) محاسبه می‌گردد [۷]:

$$Q_i^{max} = \frac{V\, E_{FD}^{max}}{x_d} cos(\delta - \theta) - V^2\left(\frac{sin^2(\delta - \theta)}{x_q} + \frac{cos^2(\delta - \theta)}{x_d}\right) \qquad (۶)$$

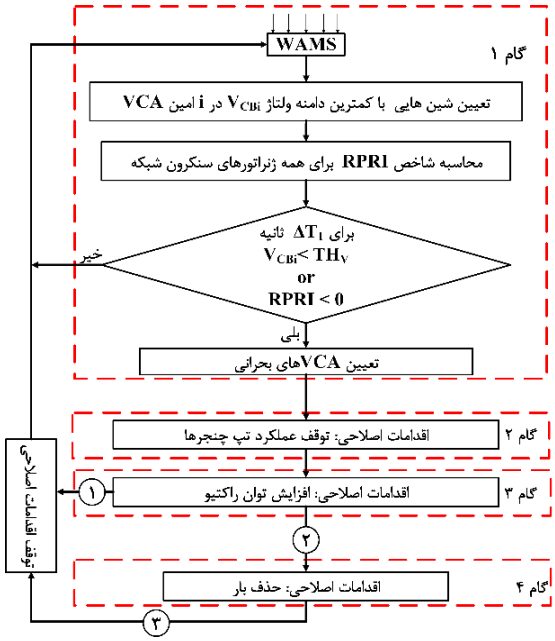
که در آن، V به‌عنوان ولتاژ ترمینال ژنراتور سنکرون، E_{FD}^{max} بیشینه ولتاژ داخلی تولیدشده در ژنراتور، x_d و x_q به‌عنوان راکتانس‌های محور d و q، δ به‌عنوان زاویه روتور و θ به‌عنوان زاویه ولتاژ ترمینال در نظر گرفته شده است. ازاین‌رو، آن دسته از ژنراتورهایی که RPRI آن‌ها به صفر برسد، دیگر نمی‌توانند توان راکتیو تولید کنند و در کنترل پایداری ولتاژ نقش داشته باشند.

۳. سامانه حفاظت ویژه پیشنهادی

در این بخش، برای جلوگیری از ناپایداری ولتاژ بلندمدت، یک الگوریتم مؤثر با بار محاسباتی کم ارائه شده است تا بتواند در زمان کوتاه تصمیمات مناسب برای بهبود پایداری ولتاژ را اتخاذ کند. در این‌روش، سامانه قدرت به چندین VCA تقسیم می‌شود و در هر ناحیه، بر اساس شاخص RPRI و اندازه دامنه ولتاژ

[1] Voltage Control Area
[2] Simple Voltage Stability Index
[3] Reactive Power Reserve Index
[4] Electrical Distance

شین‌ها، وضعیت پایداری شبکه به‌طور مداوم ارزیابی می‌شود. روندنمای SPS پیشنهادی در شکل (۱) نشان داده شده است، که شامل سه گام اصلی است که در ادامه توضیح داده خواهد شد.



شکل ۱. روندنمای SPS پیشنهادی برای جلوگیری از وقوع ناپایداری ولتاژ.

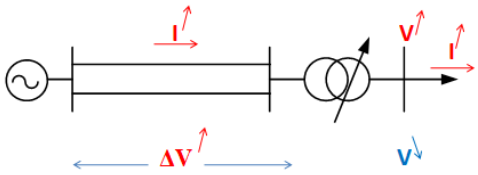
۳-۱. گام ۱ (تحلیل وضعیت پایداری ولتاژ شبکه قدرت)

در هر نقطه کار، داده‌های ارسالی از سوی WAMS[1] دریافت شده و شین‌های بحرانی که دارای حداقل اندازه ولتاژ (V_{CBi}) در i امین VCA هستند، تعیین می‌شوند. علاوه بر این، شاخص RPRI برای هر ژنراتور سنکرون در آن ناحیه محاسبه می‌شود. در این گام، اگر به مدت ΔT_1 ثانیه ژنراتوری وجود داشته باشد که مقدار RPRI آن از صفر کمتر شود (ژنراتورهای بحرانی) یا شینی وجود داشته باشد که اندازه ولتاژ آن از TH_V پایین‌تر بماند (شین بحرانی)، آن VCA به‌عنوان ناحیه بحرانی در نظر گرفته می‌شود. سپس الگوریتم به گام ۲ وارد می‌شود. در غیر این صورت الگوریتم به ابتدای گام ۱ باز می‌گردد.

۳-۲. گام ۲ (توقف عملکرد تپ چنجرها)

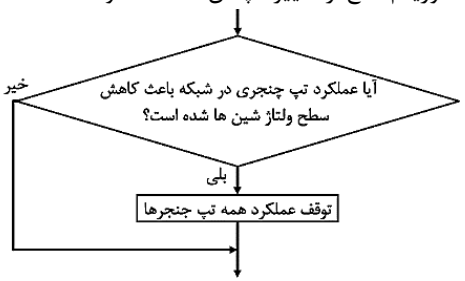
در شبکه قدرت پس از وقوع یک اغتشاش شدید، دامنه ولتاژ شین‌های شبکه دستخوش تغییرات می‌شوند. حال اگر این اغتشاش موجب کاهش بیش از حد ولتاژ شین‌هایی که توسط ترانسفورماتورهای تپ چنجردار (OLTC) کنترل می‌شود گردد، OLTCها در مقابل این کاهش ولتاژ عکس‌العمل نشان می‌دهند تا سطح ولتاژ شین‌ها به محدوده قابل قبول خود بازگردند.

از سوی دیگر، تلاش OLTCها برای افزایش ولتاژ شین‌ها (به‌دلیل آنکه معمولاً بارها وابسته به ولتاژ هستند) سبب افزایش توان و جریان بارها می‌شود که این موضوع سبب افزایش افت ولتاژ در شبکه انتقال خواهد شد (ΔV در شکل (۲)). بنابراین، در شرایط پرباری که شبکه به سختی قادر به تأمین توان مورد نیاز بارها است، ممکن است که افت ولتاژ در سامانه انتقال بر افزایش ولتاژ (ناشی از تغییر تپ OLTC) غلبه کند و تغییر تپ OLTC منجر به کاهش بیشتر ولتاژ شین مورد نظر شود.



شکل ۲. تأثیر نامطلوب عملکرد OLTCها بر کنترل سطح ولتاژ.

از این‌رو، بر اساس شکل (۳)، در این گام اگر عملکرد تپ چنجرهای ترانسفورماتورهای شبکه تأثیر معکوس بر روی وضعیت پایداری شبکه داشته باشند، دستور توقف عملکرد آن‌ها صادر شده و الگوریتم وارد گام سوم می‌شود. در غیر این صورت، الگوریتم وارد گام سوم می‌شود. لازم به ذکر است که این گام به‌طور مستمر اجرا می‌شود. بنابراین، اگر در حین اجرای سایر اقدامات اصلاحی عملکردی نامناسب از سوی هر OLTC مشاهده شود، الگوریتم مانع از تغییر تپ آن OLTC خواهد شد.



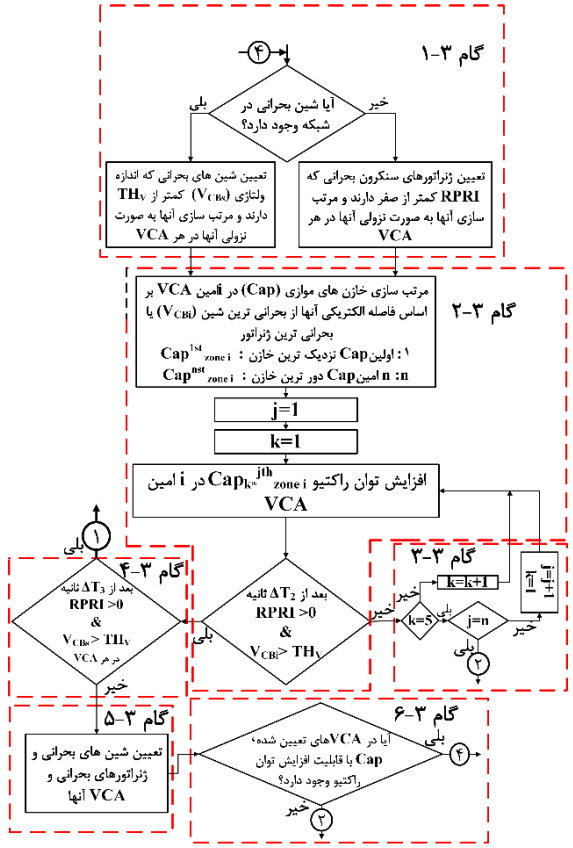
شکل ۳. گام ۲ از SPS پیشنهادی برای جلوگیری از وقوع ناپایداری.

۳-۳. گام ۳ (افزایش توان راکتیو از طریق خازن‌های موازی)

روندنمای این گام، که در VCAهای بحرانی اجرا می‌شود، در شکل (۴) نشان داده شده است. مطابق این شکل:

- گام ۳-۱: اگر در هر یک از VCAها شین بحرانی وجود داشته باشد، این شین‌ها که دارای اندازه ولتاژ کمتر از TH_V هستند، تعیین و به‌صورت نزولی مرتب می‌شوند. همچنین در هر VCA، ژنراتورهای سنکرون با RPRI کمتر از صفر شناسایی می‌شوند و به‌صورت نزولی مرتب می‌شوند. پس از آن الگوریتم وارد گام ۳-۲ می‌شود.

[1] Wide Area Measurement System



شکل ۴. گام ۳ از SPS پیشنهادی برای جلوگیری از وقوع ناپایداری.

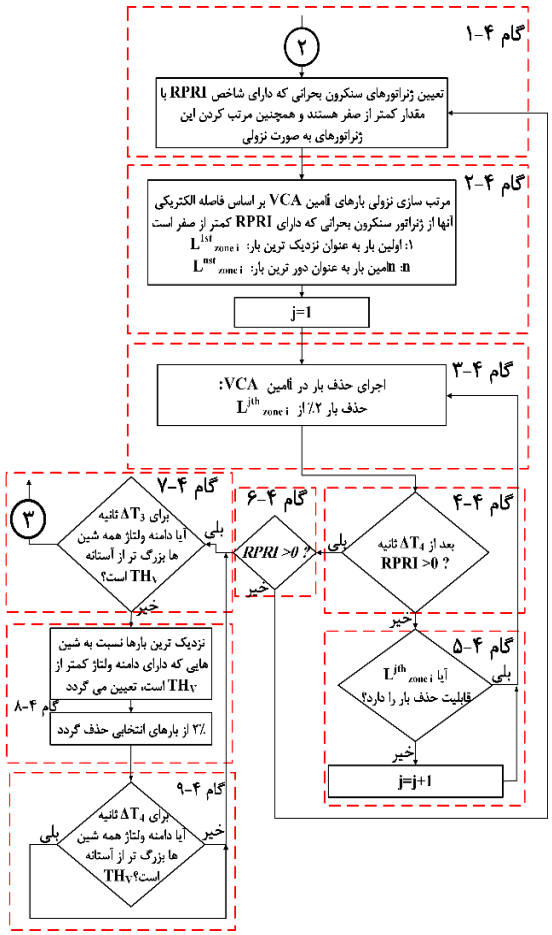
- گام ۳-۲: در این گام، در ابتدا بانک‌های خازنی (Cap) در VCAهای بحرانی که قابلیت افزایش توان راکتیو دارند، بر اساس کمترین فاصله الکتریکی نسبت به بحرانی‌ترین شین مرتب می‌شوند. سپس، افزایش توان راکتیو از نزدیک‌ترین خازن آغاز می‌شود (اگر شین بحرانی وجود نداشته باشد، روند فوق برای بحرانی‌ترین ژنراتور انجام می‌شود). اگر ΔT_2 ثانیه پس از افزایش توان راکتیو خازن انتخاب شده، مقدار دامنه ولتاژ شین بحرانی بیشتر از TH_V شود (و یا مقدار شاخص RPRI برای ژنراتور سنکرون بحرانی بزرگ‌تر از صفر شود)، الگوریتم وارد گام ۳-۴ می‌گردد. در غیر این صورت الگوریتم پیشنهادی وارد گام ۳-۳ می‌شود.
- گام ۳-۳: در این گام، اگر تعداد پله‌های خازن مورد نظر جهت افزایش توان راکتیو به مقدار بیشینه خود نرسیده باشد، پله دیگر برای خازن انتخاب شده و خازن توان راکتیو تزریقی خود به شبکه را افزایش دهد. سپس الگوریتم به گام ۳-۴ وارد می‌شود. در غیر این صورت، خازن بعدی جهت افزایش توان راکتیو انتخاب می‌شود و الگوریتم به گام ۳-۲ باز می‌گردد. همچنین اگر خازن دیگری در ناحیه بحرانی باقی نمانده باشد، الگوریتم وارد گام ۴ خواهد شد.
- گام ۳-۴: اگر بعد از ΔT_3 ثانیه، مقدار دامنه ولتاژ شین‌های بحرانی (V_{CBs}) بیشتر از TH_V شود (در تمام VCAها) و همچنین مقدار شاخص RPRI برای همه ژنراتور سنکرون در همه نواحی کنترل ولتاژ بیشتر از صفر باشد، دستور توقف اقدامات اصلاحی در آن VCA صادر می‌گردد. در غیر این صورت الگوریتم وارد گام ۳-۵ می‌گردد.
- گام ۳-۵: در این گام از الگوریتم پیشنهادی، مجدداً شین‌ها و ژنراتورهای بحرانی و VCAهای آن‌ها تعیین می‌گردد. سپس الگوریتم وارد گام ۳-۶ می‌گردد.
- گام ۳-۶: در این گام، اگر بانک‌های خازنی موجود در VCAهای بحرانی (تعیین‌شده از گام ۳-۵)، قابلیت افزایش توان راکتیو داشته باشند، الگوریتم به گام ۳-۱ باز می‌گردد. در غیر این صورت الگوریتم وارد گام ۴ (که در آن حذف بار انجام خواهد شد) می‌شود.

۳-۴. گام ۴ (حذف بار در شبکه قدرت)

روندنمای این گام در شکل (۵) نشان داده شده است. مطابق این شکل:

- گام ۴-۱: در این گام ابتدا ژنراتورهای سنکرون شبکه که داری شاخص RPRI کمتر از صفر هستند شناسایی شده و به‌صورت نزولی مرتب می‌گردند. سپس الگوریتم وارد گام ۴-۲ می‌شود.
- گام ۴-۲: در این گام، بارهای هر یک از VCAهای بحرانی بر اساس کمترین فاصله الکتریکی نسبت به بحرانی‌ترین ژنراتور سنکرون (که دارای کمترین مقدار شاخص RPRI در آن ناحیه است)، مرتب می‌شوند. سپس اولین بار انتخاب شده و الگوریتم وارد گام ۴-۳ می‌شود.
- گام ۴-۳: در این مرحله حذف بار با مقدار ۲٪ بر روی بار انتخاب‌شده اعمال می‌گردد و سپس الگوریتم پیشنهادی وارد گام ۴-۴ می‌گردد.
- گام ۴-۴: اگر بعد از ΔT_4 ثانیه، مقدار شاخص RPRI برای ژنراتور سنکرون بحرانی بیشتر از صفر شود، الگوریتم وارد گام ۴-۶ می‌شود. در غیر این صورت الگوریتم وارد گام ۴-۵ می‌شود.
- گام ۴-۵: اگر بار انتخاب‌شده قابلیت حذف بار را داشته باشد، الگوریتم به گام ۴-۳ بازمی‌گردد. در غیر این صورت بار بعدی انتخاب شده و سپس الگوریتم به گام

۴-۳ باز می‌گردد.



شکل ۵. گام ۴ از SPS پیشنهادی برای جلوگیری از ناپایداری ولتاژ.

- گام ۴-۶: در این گام، اگر مقدار شاخص RPRI برای تمام ژنراتورهای سنکرون بیشتر از صفر باشد، الگوریتم پیشنهادی وارد گام ۴-۷ می‌گردد. در غیر این صورت الگوریتم به گام ۴-۱ باز می‌گردد.
- گام ۴-۷: در این گام، اگر برای ΔT_3 ثانیه، دامنه ولتاژ همه شین‌های شبکه بیشتر از TH_V باشد، دستور توقف اعمال اصلاحی صادر می‌گردد. در غیر این صورت الگوریتم وارد گام ۴-۸ می‌گردد.
- گام ۴-۸: در این گام، نزدیک‌ترین بارهای شبکه به شین‌هایی که دامنه ولتاژ آن‌ها کمتر از TH_V می‌باشند، تعیین می‌شود و به مقدار ۵٪ حذف بار، بر روی آن‌ها اعمال می‌شود. سپس الگوریتم وارد گام ۴-۹ می‌شود.
- گام ۴-۹: در این گام، اگر برای ΔT_4 ثانیه، ولتاژ همه شین‌های شبکه بزرگ‌تر از TH_V باشد، الگوریتم به گام ۴-۷ بازمی‌گردد.

۴. نتایج شبیه‌سازی‌ها

در این بخش، جهت بررسی عملکرد SPS پیشنهادی در جلوگیری از ناپایداری ولتاژ بلندمدت، از شبکه‌های IEEE 39-Bus و Nordic32 استفاده‌شده است. در این راستا، این شبکه‌ها در نرم‌افزار PowerFactory پیاده‌سازی شده‌اند. همچنین کنترل‌کننده‌های ژنراتورهای سنکرون (AVR، GOV، و PSS[1]) و OLTCها و بارهای وابسته به ولتاژ برای شبیه‌سازی دقیق رفتار دینامیکی شبکه قدرت مدل‌سازی شده‌اند. مقادیر آستانه‌های مورد استفاده در این شبیه‌سازی‌ها در جدول (۱) آورده شده است.

جدول ۱. مقادیر آستانه‌های استفاده شده در SPS پیشنهادی.

آستانه	ΔT_1 ثانیه	ΔT_2 ثانیه	ΔT_3 ثانیه	ΔT_4 ثانیه	TH_V (پریونیت)	
					IEEE-39 bus	Nordic32
مقدار	۱۰	۲	۲۰	۲	۰/۹۶	۱

۴-۱. بررسی عملکرد SPS ارائه‌شده در شبکه IEEE 39-bus

همان‌طور که پیش از این توضیح داده شد، بر اساس روشی که در [۷] توضیح داده شد، این شبکه به سه VCA تقسیم شده است و در هر VCA، از معیار "SVSI> 0.8" [۲۵]، برای تعیین شین‌های ضعیف جهت نصب بانک‌های خازنی استفاده شده است. از آنجا که هیچ شین ضعیفی در VCA1 وجود ندارد، هیچ بانک خازنی در این VCA نصب نمی‌شوند. از این‌رو خازن‌های موازی فقط در VCA 2 و VCA 3 (با حداکثر ۵۰٪ ظرفیت توان راکتیو بار متصل به شینی که خازن به آن متصل شده است) نصب شده‌اند، که در جدول (۲) و شکل (۶) نشان داده شده است (هریک از این خازن ها دارای ۵ پله هستند که قابلیت کلیدزنی دارند). همچنین در این آزمایش سامانه، هر بار از طریق ترانسفورماتورهای OLTC به سامانه انتقال متصل شده است و ترانسفورماتورهای بین bus11-12، bus13-15 ، و bus20-19 نیز دارای OLTC هستند. همچنین بر روی تمام خطوط انتقال رله دیستانس نصب شده است و تأثیر عملکرد رله‌های حفاظتی برای خروج خطوط در هنگام وقوع خطا در نظر گرفته‌شده است.

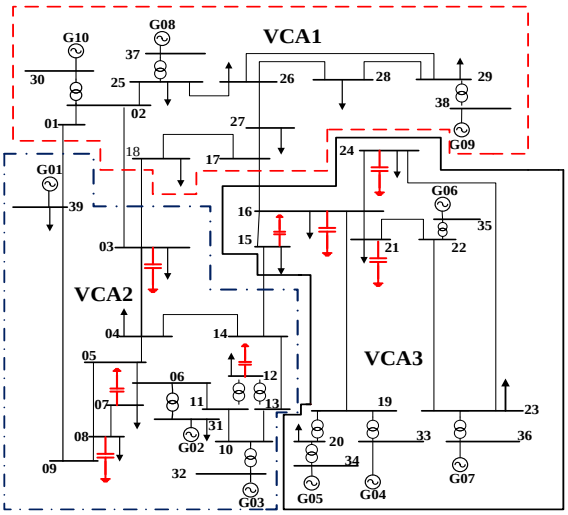
برای ارزیابی عملکرد SPS پیشنهادی، سه سناریو زیر در نظر گرفته‌شده است که در ادامه توضیح داده خواهند شد:

- سناریو ۱: خروج خط انتقال ۲۱-۲۲ از VCA 3
- سناریو ۲: خطوط انتقال ۵-۶ و ۵-۸ از VCA 2
- سناریو ۳: خروج خطوط انتقال ۵-۸، ۴-۵ و ۴-۱۴ از VCA 2

[1] Power System Stabilizer

جدول ۲. شین‌های بحرانی در هر ناحیه (محل نصب خازن‌ها).

ناحیه	شین‌های بحرانی				
VCA2	شین	شین ۱۲	شین ۸	شین ۷	شین ۳
	SVSI	۰/۹۷	۰/۸۹	۰/۸۵	۰/۸۴
VCA3	شین	شین ۱۵	شین ۱۶	شین ۲۱	شین ۲۴
	SVSI	۰/۹۴	۰/۹	۰/۸۹	۰/۸۱

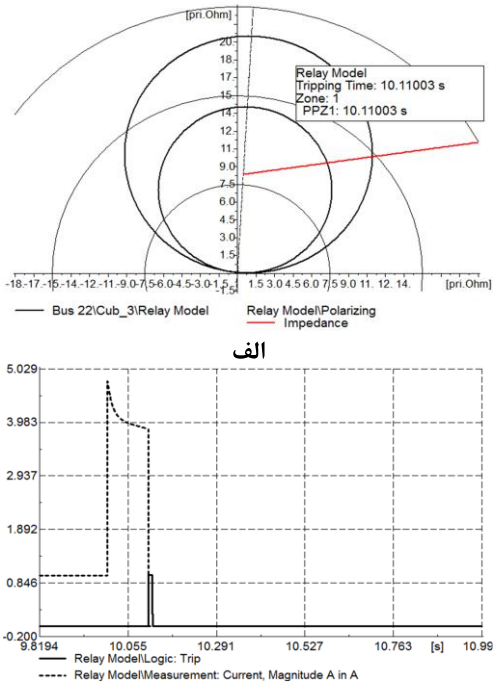


شکل ۶. آزمایش سامانه IEEE 39-Bus، تقسیم‌شده به سه VCA.

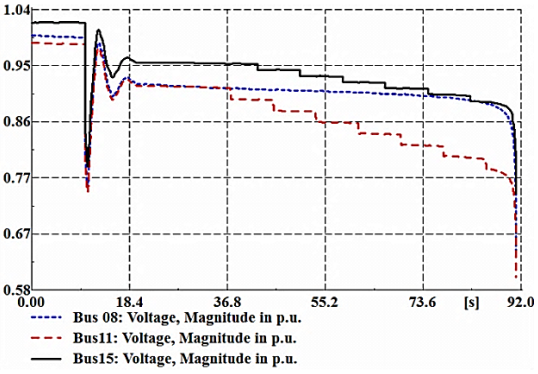
۴-۱-۱. سناریو ۱: خروج خط انتقال ۲۱-۲۲ از VCA3

در این سناریو، در ثانیه ۱۰ از شبیه‌سازی حوزه زمان خطای اتصال‌کوتاه سه فاز بر روی خط ۲۱-۲۲ اتفاق می‌افتد. طبق شکل (۷-الف) این خطای رخ داده‌شده در ناحیه ۱ (zone1) از رله‌های دیستانس خط ۲۱-۲۲ قرارگرفته و این رله‌ها دستور خروج خط ۲۱-۲۲ را ۰/۱۱ ثانیه پس از خطای اتصال کوتاه صادر می‌کنند. در شکل (۷-ب) نحوه ارسال دستور قطع (Trip) خط ۲۱-۲۲ و صفر شدن جریان گذرنده از این خط نشان داده شده است.

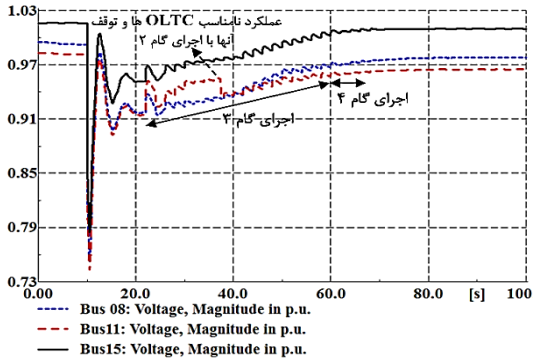
این اغتشاش شدید باعث می‌شود، سامانه قدرت دچار ناپایداری ولتاژ بلندمدت شود، که در شکل (۸) نشان داده شده است. نتایج شبیه‌سازی در این سناریو نشان می‌دهند که خروج خط مذکور سبب فعال شدن محدودکننده سامانه تحریک ژنراتور G05 می‌گردد. همچنین افت ولتاژ در شین‌ها باعث فعال شدن برخی از OLTCها می‌شود تا به‌طور خودکار موقعیت تپ خود را برای بهبود پروفیل ولتاژ تغییر دهند. با این حال، این تغییرات وضعیت را بدتر و افت ولتاژ را بیشتر می‌کند و موجب فعال شدن محدودکننده سامانه تحریک ژنراتور G04 می‌گردد. سرانجام، سقوط ولتاژ در حدود ثانیه ۹۰ از شبیه‌سازی حوزه زمان اتفاق می‌افتد.



شکل ۷. الف: امپدانس اندازه‌گیری شده توسط رله دیستانس در صفحه R-X. ب: عملکرد رله دیستانس در رفع خطا.



شکل ۸. وضعیت ولتاژ شین‌ها بدون در نظر گرفتن SPS در سناریو ۱.

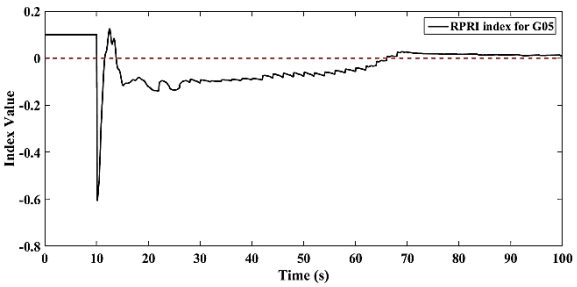


شکل ۹. وضعیت ولتاژ شین‌ها با در نظر گرفتن SPS پیشنهادی در سناریو ۱.

با این حال، طبق شکل (۹)، SPS پیشنهادی مانع از وقوع ناپایداری ولتاژ جلوگیری می‌شود و سبب می‌شود که نقطه کار شبکه به یک نقطه تعادل جدید برسد. همان‌طور که در شکل (۹) نشان داده شده است، بعد از وقوع اغتشاش، دامنه ولتاژ در شین ۱۱ در VCA 2 (در ثانیه ۲۰ از شبیه‌سازی) کمترین مقدار بوده و به همین دلیل این شین به‌عنوان بحرانی‌ترین شین در VCA2 انتخاب می‌گردد. همچنین شین ۱۵ در VCA 3 به‌عنوان بحرانی‌ترین شین در این ناحیه انتخاب می‌شود (دامنه ولتاژ شین‌ها در VCA 1 به TH_V نمی‌رسد). بر این اساس، در ثانیه ۲۰ از شبیه‌سازی، SPS وارد گام ۳ می‌شود. در این گام، نزدیک‌ترین خازن به شین ۱۱ (که در شین ۱۲ نصب شده است) و شین ۱۵ (در شین ۱۵)، توان راکتیو خود را طی ۱۰ ثانیه و ۵ پله افزایش می‌دهند. این اقدام سبب می‌شود که در ثانیه ۳۰ دامنه ولتاژ شین ۱۵ از مقدار آستانه TH_V افزایش پیدا می‌کند. با این حال، همچنان دامنه ولتاژ شین ۱۱ کمتر از مقدار آستانه TH_V است.

همچنین طبق شکل (۱۰)، مقدار شاخص RPRI برای ژنراتور G05 (در VCA3) کمتر از صفر است. بنابراین در ثانیه ۳۰، خازن متصل به شین ۷ (در VCA 2) به‌عنوان نزدیک‌ترین خازن به شین ۱۱ و خازن متصل به شین ۱۶ به‌عنوان نزدیک‌ترین خازن موازی به G05، توان راکتیو خود را افزایش می‌دهند (در مدت ۱۰ ثانیه و در پنج پله). اگرچه این اقدامات سبب بهبود وضعیت پایداری می‌شود، در ثانیه ۳۸، عملکرد نامناسب OLTCها سبب کاهش ولتاژ شین ۱۱ می‌شود که براثر آن، الگوریتم پیشنهادی (طبق گام ۲) توقف عملکرد آن‌ها اجرا می‌کند.

در ادامه این‌روند، در ثانیه ۴۰، خازن شین ۳ (در VCA 2) به‌عنوان نزدیک‌ترین خازن به شین ۱۱ و خازن متصل به شین ۲۱ به‌عنوان نزدیک‌ترین خازن موازی به G05، توان راکتیو خود را افزایش می‌دهند (در مدت ۱۰ ثانیه و در پنج پله). با این حال، مقدار دامنه ولتاژ شین ۱۱ (در VCA2) همچنان کمتر از TH_V و مقدار RPRI برای G05 (در VCA3) کمتر از صفر است.



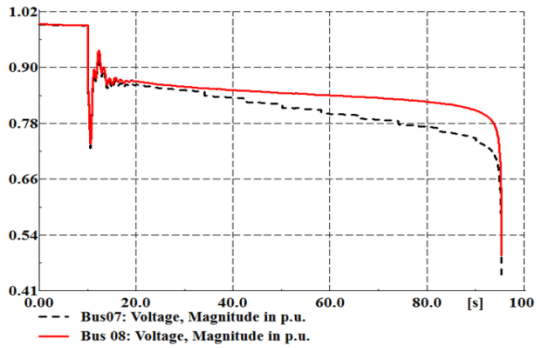
شکل ۱۰. مقدار شاخص RPRI برای ژنراتورهای سنکرون G05.

با این وجود، در ثانیه ۵۰، همچنان مقدار دامنه ولتاژ شین ۱۱ از مقدار آستانه TH_V کمتر است و مقدار RPRI برای G05 نیز کمتر از صفر خواهد بود که سبب می‌شود خازن‌های متصل به شین‌های ۸ (در VCA2) و ۲۴ (در VCA3)، توان راکتیو خود را افزایش می‌دهند. پس از سپری شدن ΔT_2 ثانیه از به مدار آمدن آخرین پله خازن‌های مذکور، ولتاژ کلیه شین‌های شبکه بزرگ‌تر از TH_V است. اما مقدار RPRI برای G05 هنوز کمتر از صفر است و به همین دلیل، SPS وارد گام ۴ می‌شود. در این گام با اعمال ۴ مرتبه حذف بار (به مقدار ۲٪) بر روی نزدیک‌ترین بار به ژنراتور G05 در VCA3 (بار متصل به شین ۲۰) مقدار شاخص RPRI در ثانیه ۶۵ از شبیه سناریو ۱ به مقداری بیش از صفر می‌رسد و از این زمان به بعد، شبکه در یک نقطه تعادل جدید به عملکرد خود ادامه می‌دهد.

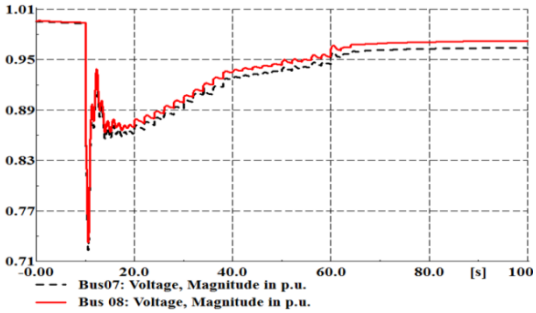
۴-۱-۲. سناریو ۲: خروج خطوط ۵-۶ و ۵-۸ از VCA 2

در این سناریو، در ثانیه ۱۰ از شبیه‌سازی حوزه زمان خطای اتصال کوتاه سه فاز بر روی خطوط ۵-۶ و ۵-۸ اتفاق می‌افتد. خطاهای اتصال کوتاه سه فاز رخ داده شده در ناحیه ۱ (zone1) از رله‌های دیستانس خطوط ۵-۶ و ۵-۸ قرار گرفته و رله‌ها دستور قطع خطوط را حدود ۰/۱۱ ثانیه پس از وقوع اتصال کوتاه صادر می‌کنند.

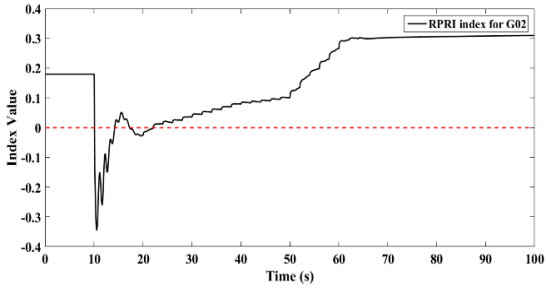
در این سناریو، سامانه قدرت دچار ناپایداری ولتاژ بلند مدت می‌شود (شکل ۱۱). این اغتشاش سبب فعال شدن محدودکننده سامانه تحریک ژنراتور G02 می‌گردد. همچنین افت ولتاژ در شین‌ها باعث فعال شدن برخی از OLTCها می‌شود تا به‌طورخودکار موقعیت تپ خود را برای بهبود پروفیل ولتاژ تغییر دهند. با این حال، این تغییرات افت ولتاژ را بیشتر می‌کند و سرانجام سقوط ولتاژ در ثانیه ۹۵ اتفاق می‌افتد. با این وجود، طبق شکل (۱۲)، SPS پیشنهادی می‌تواند باعث رسیدن نقطه کار شبکه به یک نقطه تعادل شده و از ناپایداری ولتاژ جلوگیری کند. بر اساس شکل (۱۲) با وقوع این اغتشاش‌ها، تنها ولتاژ برخی از شین‌ها در VCA 2 به مقدار کمتر از TH_V رسیده است. همچنین بر اساس شکل (۱۳)، از بین تمام ژنراتورهای شبکه، فقط مقدار RPRI برای G02 به مقداری کمتر از صفر می‌رسد. ازاین‌رو، شین ۰۷ به‌عنوان ضعیف‌ترین شین VCA 2 انتخاب می‌شود و خازن‌های متصل به شین‌های ۰۷، ۰۸، ۱۲ و ۰۳ (طبق الگوریتم ارائه‌شده) به ترتیب از ثانیه ۲۰ تا ۶۰ وارد شبکه می‌شوند تا شرایط پایداری ولتاژ را بهبود دهند. با ورود این خازن‌ها به شبکه، همان‌طور که در شکل (۱۳) نشان داده شده است، مقدار شاخص RPRI برای ژنراتور G02 به بیش از صفر می‌رسد. ذکر این نکته ضروری است که در ثانیه ۳۴ از این سناریو، با عملکرد نامناسب تپ‌چنجرهای برخی ترانسفورماتورهای شبکه در VCA2، ولتاژ چند شین کاهش می‌یابد. بر این اساس، الگوریتم طبق گام ۲ دستور توقف عملکرد این ترانسفورماتورها را اجرا می‌کند.



شکل ۱۱. وضعیت ولتاژ شین‌ها بدون SPS پیشنهادی در سناریو۲.



شکل ۱۲. وضعیت ولتاژها با در نظر گرفتن SPS پیشنهادی در سناریو۲.



شکل ۱۳. مقدار شاخص RPRI برای ژنراتورهای سنکرون G02.

علی‌رغم انجام اقدامات فوق، ولتاژ شین‌های ۰۷ و ۰۸ همچنان کمتر از مقدار آستانه TH_V باقی می‌ماند که در شکل (۱۲) نشان داده‌شده است. ازاین‌رو، طبق گام ۴ از الگوریتم پیشنهادی، با انتخاب نزدیک‌ترین بارها به این شین‌ها و اعمال ۴ مرتبه حذف بار به مقدار ۲٪ (۳ مرتبه بر روی بار متصل به شین ۰۸ و ۱ مرتبه بر روی بار متصل به شین ۰۷) دامنه ولتاژ شین‌های ۰۷ و ۰۸ به بیش از مقدار آستانه TH_V می‌رسد و پس از آن، شبکه در یک نقطه تعادل جدید به عملکرد خود ادامه می‌دهد.

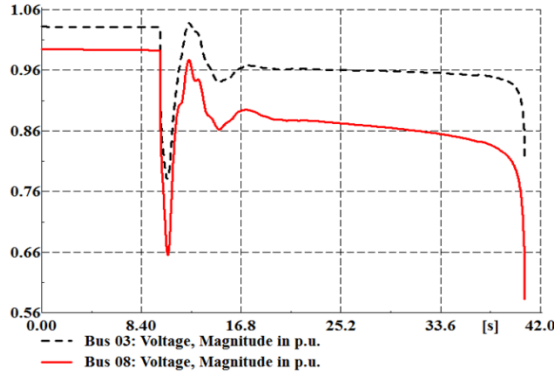
۴-۱-۳. سناریو ۳: خروج خطوط انتقال ۵-۸، ۴-۵ و ۴-۱۴ از VCA 2

در این سناریو، در ثانیه ۱۰ از شبیه‌سازی حوزه زمان خطای اتصال کوتاه سه فاز بر روی خطوط ۵-۸، ۴-۵ و ۴-۱۴ اتفاق می‌افتد. خطاهای اتصال کوتاه سه فاز رخ داده‌شده در ناحیه ۱ (zone1) از رله‌های دیستانس خطوط ۵-۸، ۴-۵ و ۴-۱۴ قرار گرفته و رله‌ها دستور قطع خطوط را حدود ۰/۱ ثانیه پس از وقوع اتصال کوتاه صادر می‌کنند.

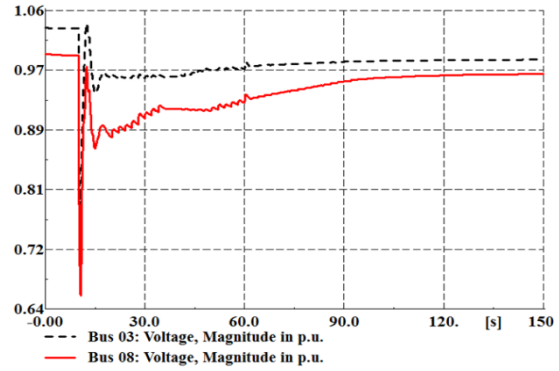
در این سناریو، سامانه قدرت دچار ناپایداری ولتاژ میان مدت می‌شود (شکل ۱۴). این اغتشاش سبب فعال شدن محدودکننده سامانه تحریک ژنراتور G02 می‌گردد. همچنین افت ولتاژ در شین‌ها باعث فعال شدن برخی از OLTCها می‌شود تا به‌طورخودکار موقعیت تپ خود را برای بهبود پروفیل ولتاژ تغییر دهند. با این حال، این تغییرات افت ولتاژ را بیشتر می‌کند و سرانجام سقوط ولتاژ در ثانیه ۴۰ اتفاق می‌افتد.

با این وجود، طبق شکل (۱۵)، SPS پیشنهادی می‌تواند باعث رسیدن نقطه کار شبکه به یک نقطه تعادل شده و از ناپایداری ولتاژ جلوگیری کند. بر اساس شکل (۱۵) با وقوع این اغتشاش‌ها، تنها ولتاژ برخی از شین‌ها در VCA 2 به مقدار کمتر از TH_V رسیده است.

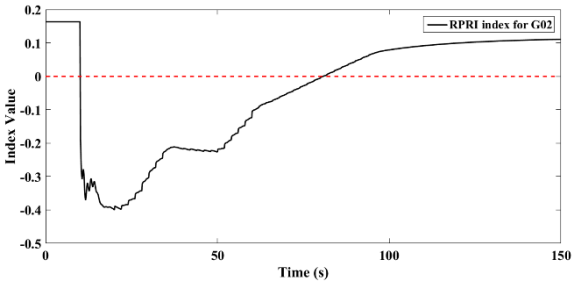
همچنین، بر اساس شکل (۱۶)، از بین تمام ژنراتورهای شبکه، فقط مقدار RPRI برای G02 به مقداری کمتر از صفر می‌رسد.



شکل ۱۴. وضعیت ولتاژ شین‌ها بدون SPS پیشنهادی در سناریو ۳.



شکل ۱۵. وضعیت ولتاژها با در نظر گرفتن SPS پیشنهادی در سناریو ۳.



شکل ۱۶. مقدار شاخص RPRI برای ژنراتورهای سنکرون G02.

بعد از وقوع اغتشاش، دامنه ولتاژ در شین ۸ در VCA 2 (در ثانیه ۲۰ از شبیه‌سازی) کمترین مقدار بوده و به همین دلیل این شین به‌عنوان بحرانی‌ترین شین در VCA2 انتخاب می‌گردد. بر این اساس، در ثانیه ۲۰ از شبیه‌سازی، SPS وارد گام ۳ می‌شود. در این گام، نزدیک‌ترین خازن به شین ۸ (که در شین ۸ نصب شده است) توان راکتیو خود را طی ۱۰ ثانیه و ۵ پله افزایش می‌دهد. با این حال در ثانیه ۳۰ از شبیه‌سازی، همچنان دامنه ولتاژ شین ۸ کمتر از مقدار آستانه TH_V خواهد بود. همچنین طبق شکل (۱۶)، مقدار شاخص RPRI برای ژنراتور G02 (در VCA2) کمتر از صفر است. بنابراین در ثانیه ۳۰، خازن متصل به شین ۷ (در VCA2) به‌عنوان نزدیک‌ترین خازن به شین ۸ توان راکتیو خود را افزایش می‌دهد (در مدت ۱۰ ثانیه و در پنج پله). اگرچه این اقدامات سبب بهبود وضعیت پایداری می‌شود، در ثانیه ۳۶، عملکرد نامناسب OLTCها سبب کاهش ولتاژ شین ۳ می‌شود که براثر آن، الگوریتم پیشنهادی (طبق گام ۲) توقف عملکرد آن‌ها را اجرا می‌کند.

در ادامه این‌روند، در ثانیه ۴۰، خازن متصل به شین ۳ (در VCA 2) به‌عنوان خازن نزدیک به شین ۸ توان راکتیو خود را افزایش می‌دهد (در مدت ۱۰ ثانیه و در پنج پله). با این حال، مقدار دامنه ولتاژ شین ۸ (در VCA2) همچنان کمتر از TH_V و مقدار RPRI برای G02 (در VCA2) کمتر از صفر است.

در ثانیه ۵۰، همچنان مقدار دامنه ولتاژ شین ۸ از مقدار آستانه TH_V کمتر است و مقدار RPRI برای G02 نیز کمتر از صفر خواهد بود که سبب می‌شود خازن متصل به شین 12 (در VCA2)، توان راکتیو خود را افزایش دهد. پس از سپری شدن ΔT_2 ثانیه از به مدار آمدن آخرین پله خازن مذکور، همچنان مقدار دامنه ولتاژ شین ۸ از مقدار آستانه TH_V کمتر است و مقدار RPRI برای G02 نیز کمتر از صفر خواهد بود و به همین دلیل، SPS وارد گام ۴ می‌شود. در این گام با اعمال ۱۰ مرتبه حذف بار (به مقدار ۲٪) بر روی نزدیک‌ترین بار به ژنراتور G02 در VCA2 (بار متصل به شین ۳۱) مقدار شاخص RPRI در ثانیه ۸۲ از شبیه سناریو ۳ به مقداری بیش از صفر می‌رسد. ولی همچنان مقدار دامنه ولتاژ شین ۸ از مقدار آستانه TH_V کمتر است از این‌رو SPS وارد گام ۴-۷ می‌شود. در این گام با اعمال ۷ مرتبه حذف بار (به مقدار ۲٪) بر روی نزدیک‌ترین بار به شین ۸ در VCA2 (بار متصل به شین ۸) مقدار دامنه ولتاژ شین ۸ در ثانیه ۹۶ از شبیه سناریو ۳ به مقداری بیش از مقدار آستانه TH_V می‌رسد و از این زمان به بعد، شبکه در یک نقطه تعادل جدید به عملکرد خود ادامه می‌دهد.

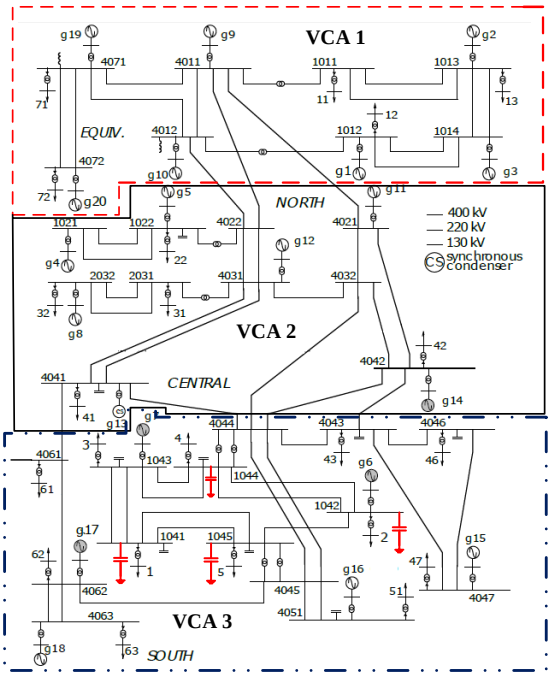
۴-۲. بررسی عملکرد SPS ارائه‌شده در شبکه Nordic32

در این قسمت، از شبکه Nordic32 برای ارزیابی عملکرد SPS ارائه‌شده استفاده می‌شود. بر اساس مطالب ارائه‌شده در بخش ۲-۲ و طبق شکل (۱۷)، با استفاده از معیار "SVSI> 0.8" شین‌های ضعیف موجود در نواحی کنترل ولتاژ مختلف جهت نصب بانک‌های خازنی (هریک از این خازن‌ها دارای ۵ پله هستند که قابلیت کلید زنی دارند) در این شبکه تعیین شده‌اند (VCA1 و VCA2 دارای شین ضعیفی نیستند). در این بخش، برای ارزیابی عملکرد SPS پیشنهادی، سناریوی وقوع اتصال کوتاه بر روی خط ۴۰۳۲-۴۰۴۴ و عملکرد رله‌های حفاظتی برای خروج این خط در نظر گرفته شده است.

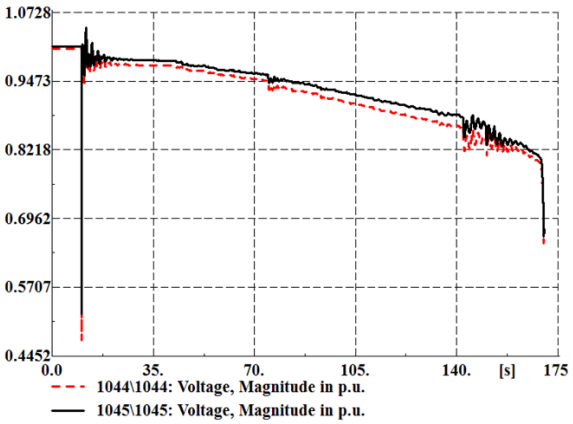
در این سناریو، در ثانیه ۱۰ از شبیه‌سازی حوزه زمان خطای اتصال کوتاه سه فاز بر روی خط ۴۰۳۲-۴۰۴۴ اتفاق می‌افتد. این خطای اتصال کوتاه سه فاز موجب عملکرد رله‌های دیستانس خط ۴۰۳۲-۴۰۴۴ می‌گردد و حدود ۰/۱۱ ثانیه پس از وقوع اتصال‌کوتاه دستور قطع خط از شبکه به کلیدهای قدرت ارسال می‌شود.

این اغتشاش شدید منجر به وقوع ناپایداری ولتاژ بلند مدت می‌شود که در شکل (۱۸) نشان داده شده است. با این حال، طبق شکل (۱۹)، SPS پیشنهادی می‌تواند باعث رسیدن نقطه کار شبکه به یک نقطه تعادل شده و از ناپایداری ولتاژ جلوگیری کند. طبق این شکل، الگوریتم در ثانیه ۳۵ وارد گام ۳ شده و خازن‌های متصل به شین‌های ۱۰۴۴، ۱۰۴۲، ۱۰۴۱ و ۱۰۴۵ را به ترتیب تا ثانیه ۷۵ وارد شبکه می‌کند. با این وجود، در ثانیه ۷۵ همچنان ولتاژ شین ۱۰۴۴ از مقدار آستانه TH_V کمتر است و به همین دلیل الگوریتم وارد گام (۴) شده و با اعمال ۸ مرتبه حذف بار به مقدار ۲٪ بر روی بار متصل به شین ۱۰۴۴، دامنه ولتاژ شین ۱۰۴۴ به مقداری بیش از TH_V می‌رسد (شکل ۱۸). همچنین طبق شکل (۲۰)، SPS ارائه‌شده باعث دور شدن

شاخص RPRI از مقدار بحرانی برای ژنراتور g06 می‌گردد.



شکل ۱۷. آزمایش سامانه Nordic32، تقسیم‌شده به سه VCA.

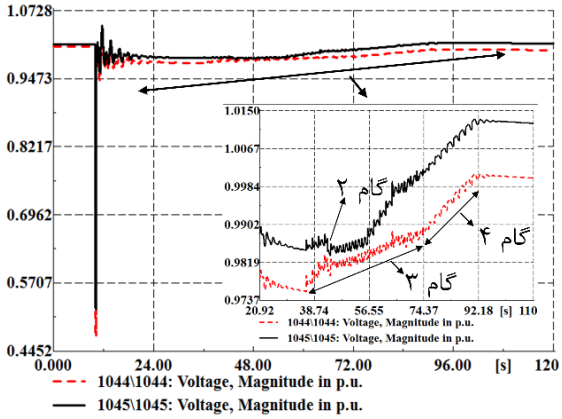


شکل ۱۸. وضعیت ولتاژ شین‌ها بدون در نظر گرفتن SPS پیشنهادی در شبکه Nordic32.

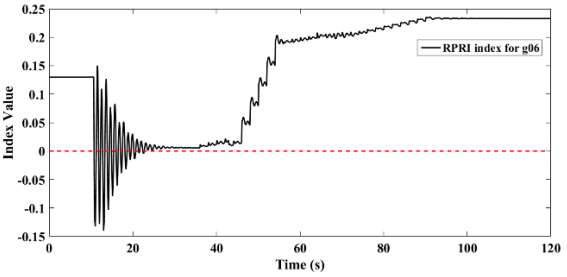
۴-۳. مقایسه روش پیشنهادی با سایر روش‌ها

در این بخش، عملکرد SPS پیشنهادی در سناریوهای ارائه‌شده در بخش ۴-۱و ۴-۲ با عملکرد SPSهای ارائه‌شده در مراجع [۷] و [۲۶] مقایسه می‌شود.

جدول (۳)، نتایج حاصل از این مقایسه را نشان می‌دهد که طبق آن، روش ارائه‌شده قادر به حفظ پایداری سامانه با حذف بار کمتر در مقایسه با سایر روش‌ها است. طبق این جدول، با توجه به اینکه در روش ارائه‌شده در این مقاله از ابزارهای مناسب‌تری برای تشخیص و بهبود وضعیت پایداری استفاده‌شده است، این الگوریتم می‌تواند عملکرد مناسب‌تری از خود نشان دهد و با استفاده از حذف بار بسیار کمتر نسبت به مراجع [۷] و [۲۶]، پایداری ولتاژ سامانه را کنترل کند.



شکل ۱۹. وضعیت ولتاژ شین‌ها با در نظر گرفتن SPS پیشنهادی در شبکه Nordic32.



شکل ۲۰. مقدار شاخص RPRI برای ژنراتورهای سنکرون g06.

جدول ۳. مقایسه عملکرد SPS ارائه‌شده با سایر روش‌ها.

سناریو	میزان حذف بار در روش‌های مختلف (مگاوات)		
	روش ارائه‌شده در این مقاله	[۷]	[۲۶]
خروج خط ۲۱-۲۲ (IEEE 39-bus)	۶۵	-	۲۶۰
خروج خط ۴۰۳۲-۴۰۴۴ (Nordic32)	۱۳۵	۳۱۰	-

۵. نتیجه‌گیری

در این مقاله، یک سامانه حفاظت ویژه کارآمد برای پیشگیری از ناپایداری ولتاژ بلندمدت در هنگام بروز حملات بمب گرافیتی پیشنهاد شده است. روش پیشنهادی شامل ۳ اقدام اصلاحی از نوع افزایش توان راکتیو در شبکه از طریق تزریق خازن‌های موازی سوییچ شونده، حذف بار و کنترل عملکرد تپ‌چنجر ترانسفورماتورهای OLTC می‌باشد. در این‌روش، در ابتدا از مفهوم فاصله الکتریکی برای ناحیه بندی سامانه قدرت به چندین VCA استفاده می‌شود تا اقدامات اصلاحی، با بیشترین تأثیر بر وضعیت

پایداری انتخاب شوند. سپس، در جهت تأمین توان راکتیو در شبکه، الگوریتم پیشنهادی از خازن‌های موازی سوییچ شونده استفاده می‌کند، که قادر است به سرعت میزان تولید توان خود را تغییر داده و به‌طور مؤثر وضعیت پایداری ولتاژ را بهبود ببخشد. در صورتی که اقدامات فوق مؤثر واقع نشود، در گام بعدی، از حذف بار استفاده می‌شود تا مانع از وقوع ناپایداری ولتاژ شود. نتایج شبیه‌سازی دینامیکی انجام‌شده در شبکه‌های IEEE 39-Bus و Nordic32، اثربخشی این‌روش را در اجرای به‌موقع اقدامات اصلاحی مناسب و حفظ پایداری ولتاژ سامانه قدرت نشان می‌دهد. همچنین مقایسه نتایج ارائه‌شده با روش‌های پیشین، تأییدکننده کارایی این‌روش و اجرای حذف بار کمتر جهت جلوگیری از خروج نقطه‌کار از ناحیه جذب شبکه است.

۶. مرجع‌ها

[1] Khoshkhoo, H.; Shahrtash, S. "On-line dynamic voltage instability prediction based on decision tree supported by a wide-area measurement system"; IET Gen Transm Distrib. 2012, 6, 1143-1152.

[2] Yari, S.; Khoshkhoo, H. "A comprehensive assessment to propose an improved line stability index"; Int Trans Electr Energy Syst. 2019, 29, e2809.

[3] Aghdam, P.; Khoshkhoo, H. "Voltage stability assessment algorithm to predict power system loadability margin"; IET Gen Transm Distrib. 2020, DOI: 10.1049/iet-gtd.2019.0230.

[4] Izadi, R "Graphite bombs and EMP and HPM"; J. Military Sci. & Tactics. 2008, 4, 57-73 (In Persian).

[5] Gaffarpour, R.; Ranjbar, A. "Presentation of Special Protection Scheme in Power System to Reduce Graphite Bomb Attacks Damages"; J. Advanced Defence Sci. & Tech. 2017, 4, 33-34 (In Persian).

[6] Nassaj, A.; Shahrtash, S. M. "An Accelerated Preventive Agent Based Scheme for Postdisturbance Voltage Control and Loss Reduction"; IEEE Trans. Power Syst. 2018, 33, 4508-4518.

[7] Islam, S. R.; Sutanto, D.; Muttaqi, K. M. "Coordinated decentralized emergency voltage and reactive power control to prevent long-term voltage instability in a power system"; IEEE Trans. Power Syst. 2015, 30, 2591-2603.

[8] North American electric reliability corporation (NERC). "Special protection systems (SPS) and remedial action schemes (RAS): assessment of definition, regional practices, and application of related standards"; 2013.

[9] Arabzadeh, M.; Seifi, H.; Sheikh-El-Eslami, M. K. "A new mechanism for remedial action schemes design in a multi-area power system considering competitive participation of multiple electricity market players"; Int J Electr Power Energy Syst. 2018, 103, 31-42.

[10] Aman, M.M.; Arshad, M.; Zuberi, H.K.; Laghari, J.A. "A hybrid scheme of load shedding using globalized frequency and localized voltage (GFLV) controller"; Int J Electr Power Energy Syst. 2019, 113, 674-685.

[11] Xie, Jing.; Chen, Liu.; Marino, Sforna.; Yin, Xu. "Consensus weighting of a multi-agent system for load shedding"; Int J Electr Power Energy Syst. 2020, 117, DOI.10.1016/j.ijepes.2019.105615.

[12] Atighechi, H.; Po, H.; Ebrahimi, S.; Jun, L.; Guihua, W.; Liwei, W. "An effective load shedding remedial action scheme considering wind farms generation"; Int J Electr Power Energy Syst. 2018, 95, 353-363.

[13] Van Cutsem, T.; Mevludin, G.; William, R.; Claudio, C.; Michael, K.; Leonardo, L.; Milano, F.; Papangelis, L.; Ramos, RA.; Dos Santos, JA.; Tamimi, B. "Test Systems for Voltage Stability Studies: IEEE Task Force on Test Systems for Voltage Stability Analysis and Security Assessment"; IEEE Trans. Power Syst. 2020, DOI: 10.1109/TPWRS.2020.2976834

[14] Nassaj, A.; Shahrtash, S. "Wide-Area Agent-Based Scheme for Volt/Var Control with a Cooperative Framework Based on Game Theory"; IET Gen Transm Distrib. 2020, DOI: 10.1049/iet-gtd.2019.0285

[15] Nassaj, A.; Shahrtash, S. "A predictive agent-based scheme for post-disturbance voltage control"; IET Gen Transm Distrib. 2018, 98, 189-198.

[16] Huang, H.; Kazerooni, M.; Hossain-McKenzie, S.; Etigowni, S.; Zonouz, S.; Davis, K. "Fast Generation Redispatch Techniques for Automated Remedial Action Schemes"; 20th International Conference on Intelligent System Application to Power Systems (ISAP). 2019, 1-8, IEEE.

[17] Ghahremani, E.; Heniche, A.; Perron, M.; Racine, M.; Landry, S.; Akremi, H. "A detailed presentation of an innovative local and wide-area special protection scheme to avoid voltage collapse: From proof of concept to grid implementation"; IEEE Trans. Smart Grid. 2019, 10, 5196 - 5211.

[18] Choi, D. H.; Lee, S. H.; Kang, Y. C.; Park, J.W. "Analysis on special protection scheme of Korea electric power system by fully utilizing statcom in a generation side"; IEEE Trans. Power Syst. 2017, 32, 1882-1890.

[19] Derafshian, M.; Amjady, N.; Dehghan, S. "Special protection scheme against voltage collapse"; IET Gen Transm Distrib. 2016, 10, 341-351.

[20] Karbalaei, F.; Shahbazi, H. "Determining an appropriate partitioning method to reduce the power system dimensions for real time voltage control"; Int J Electr Power Energy Syst. 2018, 100, 58-68.

[21] Shahidehpour, M.; Wang, Y. "Communication and control in electric power systems: applications of parallel and distributed processing"; John Wiley & Sons, 2004.

[22] Zhong, J.; Nobile, E.; Bose, A.; Bhattacharya, K. "Localized reactive power markets using the concept of voltage control areas"; IEEE Trans. Power Syst. 2004, 19, 1555-1561.

[23] Pérez-Londoño, S.; Rodríguez, L.; Olivar, G. "A simplified voltage stability index (SVSI)"; Int J Electr Power Energy Syst. 2014, 63, 806-813.

[24] Wang, L.; Liu, Y.; Luan, Z. "Power transmission paths based voltage stability assessment"; *T*ransm and Distrib Conf and Exhib: Asia and Pacific. 2005, 1-5.

[25] S. Pérez-Londoño, S.; Olivar-Tost, G.; Mora-Florez, J.; "Online determination of voltage stability weak areas for situational awareness improvement"; Electric Power Systems Research vol. 2017, 145, 112-121.

[26] Yari, S.; Khoshkhoo, H. "An Effective Corrective Remedial Action Algorithm to Prevent Voltage Instability"; Conf. Knowledge Based Eng and Innovation (KBEI). 2019, 460-466.

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۴۲۷-۴۱۵

«علمی- پژوهش»

تبیین نقش بازدارنده ذخیره‌سازهای الکتریکی و برنامه‌ریزی واحدهای تولیدی UC با و بدون حضور ذخیره‌سازها از منظر پدافند غیرعامل

سعید عسکری[۱]، حبیب‌الله سهامی[۲*]، عباس علی‌آبادی[۳]

۱- کارشناس ارشد، ۲- استادیار، دانشگاه صنعتی مالک اشتر ۳- دانشیار دانشگاه صنعتی خواجه نصیرالدین طوسی

(دریافت: ۹۸/۱۲/۱۵، پذیرش: ۹۹/۰۵/۲۹)

چکیده

فناوری‌های ذخیره‌ساز الکتریکی سطوح متفاوتی از مراحل اولیه تحقیق و توسعه را دارا می‌باشد و امروزه در سامانه‌های قدرت به‌ویژه شبکه قدرت در ایران بسیار مورد توجه برنامه ریزان و بهره‌برداران قرار دارد. به‌دلیل خصوصیت‌های ذاتی شبکه‌های برق و وجود آسیب‌پذیری‌های فراوان و در راستای حفاظت و مصون‌سازی مراکز حیاتی کشور و حفظ اقتصاد و پایداری شبکه‌های برق به‌خصوص در شرایط پیک بار، لزوم استفاده از سامانه‌های ذخیره‌ساز در شبکه‌های برق اجتناب‌ناپذیر است. تحقیق حاضر با هدف توسعه استفاده از ذخیره‌سازهای الکتریکی در شبکه توزیع از منظر پدافند غیرعامل انجام شد که جهت تجزیه و تحلیل داده‌ها روش تحلیل محتوا (کیفی) و آمار توصیفی (کمی) انتخاب و نرم‌افزار GAMS به‌عنوان ابزار پردازش اطلاعات و شبیه‌سازی استفاده شده است. بررسی پیک مصرفی کشور نشان می‌دهد سامانه‌های ذخیره‌ساز نسبت به نیروگاه‌ها در جهت پیک‌سایی کاربری بهتر و بهینه‌تری دارند. پس از بررسی ۷ نوع از بهترین باتری‌های کاربردی بر اساس شاخص‌های توان نامی، بازدهی، چگالی، انرژی، تخلیه خودی روزانه و طول عمر، باتری‌های لیتیوم یونی به‌عنوان مناسب‌ترین باتری جهت استفاده در سامانه‌های ذخیره‌سازی معرفی شده‌اند.

کلیدواژه‌ها: شبکه توزیع برق، پدافند غیرعامل، ذخیره‌سازهای انرژی الکتریکی، باتری، GAMS.

Elaborating Deterrent Role and Developing Electric Storage Devices In Distribution Network, Based on Passive Defense Perspective

S. Askari, H. Sahami*, A. Aliabadi
Malek Ashtar University of Technology, Tehran
(Received: 05/03/2020; Accepted: 10/08/2020)

Abstract

Electric storage technologies have different levels of early stages of R&D, and today power systems, especially power grid in Iran, are highly regarded by planners and operators. Because of inherent characteristics of power networks and the presence of many vulnerabillities, using storage systems in power networks is inevitable in order to protect the critical infrastructures and maintain the economy and sustainability of electricity networks. The present study aims to develop the use of electrical storage devices in the distribution network from the passive defense perspective based on (qualitative) and descriptive statistics (quantitative) analysis with help of GAMS software. The country's peak courier survey shows that storage systems have more efficiency compared to power plants. In this investigation, seven types of best-performing batteries are analyzed, based on nominal power indices, efficiency, density, energy, daily insolubility and life span, and Lithium lion batteries are considered to be the most suitable for use in storage systems are introduced as most affordable.

Keywords: Electrical Distribution Network, Passive Defense, Electric Storage Devices, Battery, GAMS

*Corresponding Author E-mail:Hsahami15@gmail.com

۱. مقدمه

انرژی برق اصلی‌ترین و ضروری‌ترین عامل زیربنایی در ایجاد راهبرد و توسعه صنایع در یک کشور می‌باشد. اهمیت برق در زندگی ما به‌قدری زیاد است که گفته می‌شود، برق، قطار تمدن را به‌پیش می‌راند. صنعت برق یکی از صنایع راهبردی و بسیار پویاست که نقش اساسی و محوری در تحقق برنامه‌های توسعه ملی هر کشور ایفاء می‌کند، از این‌رو حکومت‌ها به‌طور سنتی به صنعت برق به‌عنوان یک صنعت پیشرو نگریسته‌اند، از سوی دیگر به‌دلیل اثرات اجتماعی، محیطی و نیاز به حجم بالای سرمایه‌گذاری در این صنعت دولت‌ها سعی نموده‌اند تا آن را به‌صورت متمرکز کنترل نمایند.

اهمیت برق در تولید و اقتصاد کشور از آنجا ناشی می‌شود که صنعت برق در اقتصاد ملی و تأمین رفاه اقتصادی و اجتماعی کشورها ارزش زیادی دارد و جزء چند صنعت مهم زیربنایی است به‌ویژه در صنایع، برق دارای ارزش و منزلت خاصی است زیرا در بیشتر موارد نیروی برق، ماشین‌آلات کارخانه‌ها را به حرکت وا می‌دارد و تمام عملیات و فعالیت‌های تولیدی را امکان‌پذیر می‌کند و به همین دلیل برخی صاحب‌نظران صنعت برق را مادر صنایع دانسته‌اند، بدیهی است تأمین امنیت انرژی و حفاظت از زیرساخت‌های انرژی از وظایف دولت‌ها بشمار می‌رود و ستون فقرات امنیت ملی و دفاع از حاکمیت ملی را تشکیل می‌دهد.

آمار وزارت نیرو نشان از افزایش روز افزون مصرف برق در کشور (سالیانه حدود ۳۰۰۰ مگاوات) دارد که البته بخش قابل توجهی (حدود ۵۰۰ تا ۱۵۰۰ مگاوات) از این افزایش مصرف صرفاً در زمان پیک ایجاد می‌شود که هر ساله موجب خاموشی‌های مکرر در اکثریت نقاط کشورمان شده است. ایجاد خاموشی‌های طولانی‌تر در کشور علاوه بر خسارت‌های اقتصادی می‌تواند زمینه‌ساز اعتراضات و حتی اغتشاش‌هایی در سطح کشور به‌منظور جلوگیری از صادرات برق در فصل تابستان شود. اقدامات پدافند غیرعامل باید قبل از چنین رخدادهایی اندیشیده و اجرا شوند تا موجب ایجاد شرایط بحرانی در کشور نشود.

با مرور سوابق رخدادهای انسان‌ساخت، نظیر حمله جنگنده‌های عراقی به نیروگاه نکا (۱۹۸۷)، حمله هکرهای کره شمالی به نیروگاه هسته‌ای کره جنوبی (۲۰۱۳)، نفوذ هکرها به نیروگاه‌های انگلیس و اوکراین (۲۰۱۷)، حمله هکرهای ناشناس به نیروگاه هسته‌ای آمریکا (۲۰۱۷)، هشت سال دفاع مقدس، جنگ ۴۲ روزه متحدین علیه عراق، جنگ یازده‌هفته‌ای ناتو علیه یوگسلاوی، جنگ دوم خلیج‌فارس، جنگ ۱۱ روزه اسرائیل علیه لبنان، جنگ ۲۲ روزه غزه و ...مؤید این نظر است که کشور مهاجم جهت در هم شکستن اراده ملّت و توان اقتصادی و نظامی کشور موردتهاجم، ثقل توجه خود را صرف بمباران و انهدام مراکز حیاتی و حساس نموده و لذا مراکزی که در آن اقدامات دفاع غیرعامل منظور نشده باشد خسارت کلان و قابل‌توجهی را متحمل خواهند شد که این امر تأثیرات اجتناب‌ناپذیری در تزلزل امنیت ملّی و ایجاد بحران‌های شدید سیاسی، اقتصادی و اجتماعی خواهد داشت [۱].

به‌کارگیری پدافند غیرعامل در جهت مقابله با تهدیدات به‌منظور تقلیل خسارت ناشی از حملات هوایی و زمینی کشور مهاجم، موضوعی بنیادی و اساسی است که وسعت و گستره آن تقریباً تمامی مراکز حیاتی و آسیب‌پذیر اقتصادی، سیاسی، نظامی، ارتباطی، علمی، فرهنگی، نیروگاه‌ها، قرارگاه‌های فرماندهی، پل‌های راهبردی و راه‌های تدارکاتی، فرودگاه‌ها، بندرها، پالایشگاه‌ها و مجتمع‌های بزرگ صنعتی کشور و ... را در برگرفته و حفظ امنیت ملی، استقلال سیاسی، اقتصادی و دفاعی به نحو چشمگیری وابسته به برنامه‌ریزی همه‌جانبه در موضوع یادشده می‌باشد. امروزه کشورهایی که طعم خرابی و خسارات ناشی از جنگ را چشیده‌اند، برای حفظ سرمایه‌های ملی و منابع حیاتی خود، توجه ویژه‌ای به دفاع غیرعامل نموده و در استراتژی دفاعی خود جایگاه والایی برای آن قائل شده‌اند. نمونه بارز آن کشور کره شمالی است که با اتخاذ سیاست و استراتژی تمرکززدایی، اقدامات بنیادی و اساسی جالب‌توجهی اتخاذ نمود [۲].

در دهه اخیر سامانه‌های ذخیره‌ساز انرژی با انگیزه‌های متفاوتی به‌منظور بهبود عملکرد سامانه قدرت، مورد توجه قرارگرفته‌اند این ذخیره‌سازها یا برق شبکه سراسری را به‌وسیله باتری‌ها یا ابرخازن‌ها ذخیره می‌کنند و در زمان لازم آن را به شبکه باز می‌گردانند یا ذخیره‌سازهای الکتریکی می‌توانند به‌صورت مستقل از شبکه برق سراسری کار کنند و توسط مولدهای طبیعی (خورشید، باد، امواج، سوخت فسیلی و ...) انرژی الکتریکی را ذخیره نماید تا در هر زمان به‌صورت مستقل از شبکه برق کشور قابلیت به‌کارگیری را داشته باشند [۳].

ویلهلم کونیگ از نخستین کسانی بود که در مورد باتری‌ها تحقیقاتی انجام داد، طبق تحقیقات ایشان، اولین باتری ۲۲۰۰ سال پیش توسط امپراتوری اشکانیان ساخته و جهت کاربری‌های مختلفی ازجمله تشخیص طلا، نقره و ... استفاده می‌شد.

با اینکه در دهه هفتاد مفهوم ذخیره‌سازی انرژی الکتریکی به شکل مغناطیسی موردتوجه قرار گرفت، اما اولین برنامه ذخیره‌سازی در سال ۱۹۷۸ با عنوان "باتری برای کاربردهای خاص خورشیدی" نام‌گذاری شد. این برنامه مبتنی بر انرژی تجدیدپذیر شامل توسعه و آزمایش فناوری باتری پیشرفته، تجزیه

و تحلیل سامانه‌ها و تحقیقات در مورد ادغام باتری با سامانه‌های انرژی فتوولتائیک و باد بود.

در اوایل دهه هشتاد در مقالات و پژوهش‌ها استفاده از انرژی‌های نو با آلایندگی بسیار اندک و همچنین تجدیدپذیری بالا به‌عنوان یک راه‌حل اساسی در زمینه اقتصاد زیستی مطرح گردید، یکی از این انرژی‌ها، انرژی خورشیدی بود، که با توجه به ناپایداری و موقتی بودن آن، ضرورت ذخیره‌سازی را با خود به همراه داشت.

در سال ۱۹۹۱ سازمان انرژی آمریکا شروع به یک برنامه تحقیق جامع و یکپارچه در مورد سامانه ذخیره‌سازی باتری کرد، در آن تحقیقات، مدیران پروژه سازمان انرژی آمریکا پروژه‌های ذخیره‌سازی بسیار موفق را به نمایش گذاشتند که منجر به تولید محصولات تجاری متعددی شد که تعدادی از آنها بیش از ۱۰۰ جایزه تحقیق و توسعه را کسب کردند [۴].

در سال ۱۹۹۶، سازمان انرژی آمریکا تحقیقات باتری‌ها را به تحقیقات ذخیره‌سازی فعلی که مسئولیت توسعه طیف گسترده‌ای از تحقیقات فناوری‌های ذخیره‌سازی نوین مانند فلاش و ذخیره انرژی هوای فشرده (CAES) را به عهده دارد، گسترش داد.

از اوایل قرن ۲۱ در گزارش پروژه‌های ESS، مزایای ذخیره‌سازی انرژی انتشار و توسط کارشناسان ذخیره‌سازی در سراسر جهان به‌طور مرتب مطرح شد، به همین دلیل توجه و تمرکز شرکت‌ها و افراد بیشتری به این موضوع جلب شد.

برنامه کارآفرینی ESS در مشارکت‌های نزدیک با صنعت، دانشگاه‌ها و دولت‌ها، مسائل مربوط به انرژی را از طریق ذخیره‌سازی انرژی در سطح جهانی هدایت می‌کند [۴].

در بسیاری از مراجع که اکثریت از ۲۰۱۰ به بعد انجام‌شده‌اند از باتری‌ها برای مهار اثرات سوء ناشی از منابع تجدیدپذیر بادی و خورشیدی استفاده می‌شود. نتایج این مطالعات نشان می‌دهد که می‌توان از باتری‌ها به‌طور موفقیت‌آمیزی برای حل مشکلات شبکه استفاده نمود و منابع غیرقابل دیسپچ را برنامه‌ریزی کرد [۵-۷].

در سال ۲۰۱۲ در مقالات زیادی به کاربرد باتری‌ها در بحث ذخیره‌سازی توجه شده است، ذخیره‌سازهای انرژی با اهداف مختلفی از جمله جلوگیری از نوسانات شبکه، افزایش کیفیت توان، تنظیم ولتاژ، تعقیب بار، پیک‌سایی، رزرو چرخشی، کاهش بار شبکه انتقال و پشتیبانی از منابع تجدیدپذیر کاربردی شناخته شد [۸].

در سال ۲۰۱۳ در کتاب‌ها و مقالات فراوانی، بررسی باتری‌ها جهت استفاده در شبکه توزیع بیشتر به چشم می‌خورد،در برخی مطالعات تأثیر توسعه دینامیکی شبکه توزیع بر برنامه‌ریزی باتری‌ها نشان داده‌شده و از یک الگوریتم اجتماع ذرات بهبودیافته برای بهینه‌سازی سود برده شد [۹]. در میان انواع مختلف ذخیره‌سازها، باتری‌ها به خاطر ویژگی‌های خاص خود، به‌صورت گسترده‌تری در سطح شبکه توزیع موردتوجه قرارگرفته‌اند.

از سال ۲۰۱۴ تا به‌حال در کشور ما فنّاوری ذخیره‌سازی به خصوص جهت برق‌رسانی به روستاها در اولویت صنعت برق کشور قرار دارد ، با توجه به رشد فنّاوری ذخیره‌سازها در دیگر کشورها، لزوم توجه و پیگیری ذخیره‌سازها در کشور ما به‌خصوص توسط وزارت نیرو ضروری است [۱۰].

همان‌طور که روند تحقیقات نشان داده، توجه به علم ذخیره‌سازی در تمام دنیا و همین‌طور در کشور ما روزبه‌روز بیشتر می‌شود، با توجه به تهدیدات نوینی (سایبری) که صنعت برق را هدف قرار داده و مسائل مختلفی که باعث شده کشور ما همواره در معرض تهدید دشمنان قرار داشته باشد، توسعه و پیشرفت در زمینه ذخیره‌سازی انرژی به‌خصوص توسط دانشگاه‌ها امری ضروری است که متأسفانه ضرورت نیاز به این موضوع از دید پدافند غیرعامل تاکنون مورد غفلت واقع شده است.

۲. روش تحقیق

رخدادهای طبیعی و تهدیدات متفاوت و متنوع از یک طرف، آسیب‌پذیری‌های موجود در صنعت برق، از طرف دیگر باعث می‌شوند که قطع شدن برق سراسری را در شرایط بحران و جنگ، امری اجتناب‌ناپذیر بدانیم، بنابراین، سؤال اصلی این است که جهت تداوم خدمت‌رسانی به مردم و حفظ عملکرد زیرساخت‌های کشور در زمان بحران راه حل چیست؟ چه کاری می‌توان انجام داد که خاموشی‌ها در تابستان‌ها و پیک بالای برق کمتر شود؟

با توجه به ماهیت بین‌رشته‌ای بودن طرح‌های پدافند غیرعامل، به‌منظور تعیین روش تحقیق در این پروژه از سه منبع متفاوت از سه‌طبقه دانش عمومی، هنر و علوم انسانی مورد استفاده شد و در نهایت از روش ترکیبی- توصیفی (تحلیل محتوا) استفاده‌شده است. جهت گردآوری اطلاعات موردنیاز علاوه بر استفاده از منابع کتابخانه‌ای از نرم‌افزار گمز[1] جهت انجام شبیه‌سازی لازم در شبکه استفاده شده است.

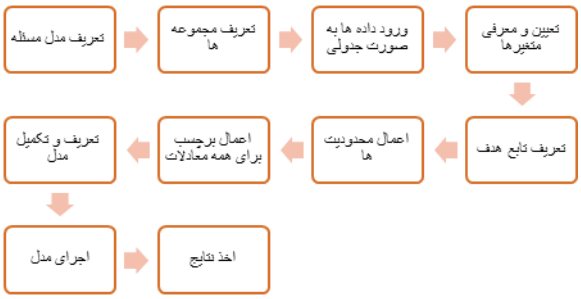
از آنجاکه نرم‌افزار گمز به‌طور خاص برای مدل‌سازی و حل مسائل ریاضی خطی، غیرخطی، مختلط و انواع دیگری از مسائل

[1] GAMS

بهینه‌سازی طراحی‌شده است.، کاربرد ویژه این نرم‌افزار در حل مدل‌های پیچیده و به‌ویژه در مقیاس‌های بزرگ می‌باشد، با وجود اینکه مدل‌هایی که توسط این نرم‌افزار حل می‌شود، دارای حجم

ریاضی استفاده کرده که گمز از ابزارهای بسیار کارآمد حل این نوع مدل‌ها است به همین دلیل جهت شبیه‌سازی‌های مورد نیاز در این پروژه انتخاب شده است.

روش کار نرم‌افزار:



شکل ۱. روش کار نرم‌افزار GAMS

بررسی اقتصادی استفاده از سامانه‌های ذخیره‌ساز در شبکه برق با استفاده از این نرم‌افزار مورد تجزیه قرار گرفته و در نهایت نتایج شبیه‌سازی استخراج‌شده تا مورد تحلیل قرار گیرد.

۳. مبانی نظری و علمی تحقیق

۳-۱. بررسی مناسب‌ترین منابع پشتیبان برق

منابع پشتیبان برق جهت کاربردهای فراوان و متفاوتی موردتوجه هستند ازجمله برخی منابع ذخیره انرژی مانند تلمبه ذخیره یا هوای فشرده در حجم زیاد، کار ذخیره‌سازی را انجام می‌دهند و قابلیت پاسخ‌گویی در حجم‌های بالا را دارند. این نوع سامانه‌ها در زمان کمبود منابع می‌توانند از ذخیره خود به‌عنوان نیروی محرکه‌ای جهت تولید انرژی الکتریکی استفاده کنند و مناسب‌ترین محل استفاده از این نوع سامانه‌های ذخیره انرژی در بخش تولید (در نقش نیروگاه) است. برای هر بخش از شبکه تولید، انتقال و توزیع نوع خاصی از منابع پشتیبان برق کاربرد دارد و ازجمله خصوصیات و ویژگی‌هایی که بنا به محل استفاده از سامانه‌های ذخیره‌سازی انتظار می‌رود یک یا چندتای آن‌ها را داشته باشند مواردی را در زیر ارائه داده‌ایم:

- پیک‌سایی و جابه‌جایی زمانی مصرف
- بار خارج از شبکه
- یکپارچه‌سازی منابع عرضه متغیر
- تولید هم‌زمان برق و حرارت
- تنظیم فرکانس

داده بالایی می‌باشند، اما زمانی که صرف پردازش آن‌ها می‌گردد بسیار ناچیز است، به‌علاوه هرجا نیاز به تصمیم‌گیری بهینه با محدودیت زمان، هزینه و منابع داشته باشیم باید از مدل‌سازی

- ذخیره‌سازی فصلی
- تجارت انرژی
- پخش بار
- ولتاژ پشتیبانی
- راه‌اندازی مجدد
- تعویق سرمایه‌گذاری در زیرساخت انتقال و توزیع
- چرخان غیر ذخیره

ذخیره‌سازی انرژی می‌تواند در سراسر بخش‌های سامانه انرژی شامل عرضه، انتقال و توزیع و تقاضای مصرف‌کننده نهایی استفاده شوند. بهترین محل برای استقرار فنّاوری ذخیره‌سازی بستگی به قابلیتی که از آن در فرایند سامانه انرژی از عرضه تا مصرف انتظار می‌رود، دارد. علاوه بر این، تحولات شبکه‌های هوشمند و دیگر فنّاوری‌های جدید در تعیین مکان بهینه این ذخیره‌سازها تأثیرگذار خواهد بود. ذخیره‌سازی انرژی در سه بخش مورد بررسی قرار گرفته است که در هر بخش مقدار و نوع خاصی از سامانه‌های ذخیره‌ساز قابلیت به‌کارگیری دارند که به‌صورت مختصر توضیح می‌دهیم:

➢ بخش تولید

عمدتاً ذخیره‌سازهای تلمبه ذخیره‌ای و هوای فشرده برای این منظور مناسب می‌باشند. هدف از ذخیره‌سازی در این بخش کفایت تولید، تبعیض قیمت و یکپارچه‌سازی انرژی‌های تجدیدپذیر، ذخیره‌سازی متمرکز حجم بالایی از انرژی برای خدمات جانبی و مدیریت انرژی است که می‌توان گفت ذخیره‌سازی در این بخش در ابعاد بزرگ قابل انجام است که مناسب‌ترین سامانه‌های ذخیره برای این بخش عبارت‌اند از تلمبه ذخیره‌ای، مخازن ذخیره‌سازی حرارتی، هوای فشرده و نمک مذاب.

➢ بخش انتقال

هدف از ذخیره‌سازی در این بخش را می‌توان خدمات فرهی و کنترل ولتاژ و فرکانس دانست که در این بخش ذخیره‌ساز نقشی واسط بین تولید و توزیع دارد از طرفی در بخش انتقال نیرو عموماً به‌منظور الحاق انرژی‌های تجدیدپذیر به شبکه از ذخیره‌سازهای هوای فشرده و باتری‌ها با هدف ذخیره‌سازی متمرکز و غیرمتمرکز بزرگ برای جابه‌جایی زمانی تولید برق از نیروگاه‌های تجدیدپذیر و به‌طورکلی بهترین نوع سامانه ذخیره‌ساز قابل‌استفاده در این بخش عبارت است از: باتری‌ها، هوای فشرده و

چرخ طیار می‌باشند که نوع باتری مناسب را بر اساس شرایط انتخاب می‌کنند.

- **بخش توزیع**

هدف از ذخیره‌سازی در این بخش مدیریت بار، کنترل ولتاژ، قابلیت اطمینان، جابه‌جایی زمانی (مصرف)، کیفیت انرژی و تأخیر انداختن در سرمایه‌گذاری در ایجاد نیروگاه‌های جدید است که بنا به میزان افزایش سالانه مصرف و مصرف پیک کشور می‌توان مقیاس ذخیره‌سازی در این بخش را متغیر دانست به این صورت که اگر در بخش مصرف مشترکین استفاده کنیم، علاوه بر باتری‌ها، فنّاوری‌های ذخیره‌سازی انرژی حرارتی زیرزمینی می‌تواند مورد استفاده قرار گیرد. در صورت استفاده از باتری‌ها، در مقیاس کوچک (حدود ۲ تا ۳ کیلووات ساعت) استفاده می‌شود. درصورتی‌که تصمیم به استفاده از ذخیره‌سازی در مجاورت پست‌ها باشد صرفاً از باتری‌ها و در مقیاس‌های بزرگ استفاده می‌کنیم، در بخش توزیع مناسب‌ترین سامانه ذخیره‌ساز انرژی الکتریکی باتری‌ها هستند که بعد از بررسی‌های فنی – اقتصادی باتری لیتیوم یون به‌عنوان مناسب‌ترین نوع تعیین شده است.

۳-۲. ضروری‌ترین بخش‌ها جهت وجود ذخیره‌سازهای الکتریکی

۳-۲-۱. مراکز حیاتی و حساس

قطع برق حتی به مدت کوتاه در مراکز حیاتی به‌خصوص در زمان بحران غیرقابل‌تحمل می‌باشد و خود می‌تواند باعث افزایش فشار به مردم و عدم خدمت‌رسانی نهادهای مختلف شود، به همین دلیل پیش‌بینی منبع پشتیبان بدون وقفه، برای مراکز حیاتی و حساس، امری ضروری است تا در صورت قطعی برق بتوانند مدت‌زمانی را خدمات‌دهی کنند تا مشکل رفع شود، در صورت قطعی چندثانیه‌ای یک مرکز حساس مانند صداوسیما، مراکز کنترل و فرماندهی، پایگاه نظامی، بیمارستان و ... ممکن است آسیب‌های جبران‌ناپذیری به ساختار کشور وارد شود.

۳-۲-۲. مراکز راهبردی در عمق زمین

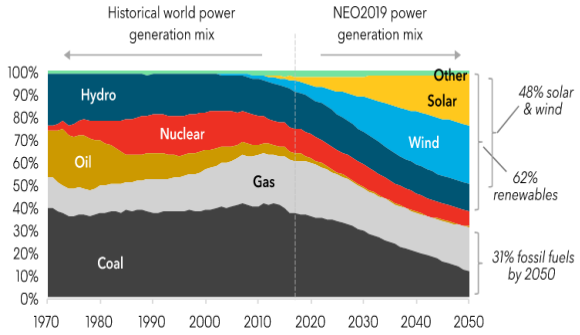
برخی از مراکز دارای اهمیت ویژه‌ای در جهت حفظ امنیت ملی کشور به‌خصوص در زمان جنگ و بحران هستند که آن‌ها را به زیر سطح زمین برده‌اند تا حفاظت از آن‌ها در برابر عوامل دشمن بهتر انجام شود. ایجاد فضای مناسب در عمق زمین برای برخی مراکز، محافظت آن‌ها را در برابر شناسایی دشمن، زلزله، حملات تروریستی و ... کامل‌تر کرده و عملکرد آن‌ها را در شرایط بحرانی ممکن می‌سازد. با این وجود یکی از تهدیدات اصلی برای شبکه برق بمب‌های EMP هستند که مقابله با آن در سطح کل شبکه توزیع (به‌دلیل وسیع و گسترده بودن) غیرممکن است و حتی تأسیسات برقی سازه‌های زیرزمینی در برابر این نوع بمب‌ها کاملاً بدون دفاع هستند. بمب‌های الکترومغناطیس بهترین گزینه برای حمله به مراکز زیرزمینی هستند زیرا چنین سنگرهایی به‌وسیله موشک‌ها و بمب‌های معمولی، قابل‌انهدام نیستند. یک پالس الکترومغناطیسی رهاشده از بمب الکترومغناطیسی می‌تواند از لایه‌های زمین عبور کرده و موجب قطع برق مراکز زیرزمینی شود حال تنها راه محافظت مراکز زیرزمینی در برابر بمب‌های EMP عایق کردن کامل تأسیسات، تجهیزات و کابل‌ها در مراکز زیرزمینی در برابر الکترومغناطیس با استفاده از روش‌های شناخته‌شده تابه‌حال مانند، قفس فارادی است؛ که در این روش‌ها عبور سیم‌های برق و اتصال تأسیسات داخلی به شبکه‌های سراسری بزرگ‌ترین نقطه‌ضعف آن‌هاست زیرا که پالس‌های الکترومغناطیس در کمتر از یک میکرون ثانیه تمامی سیم‌ها و تأسیسات متصل را از کار انداخته و سبب عدم کارکرد آن‌ها می‌شود. حال در صورت استفاده از ذخیره‌سازهای الکتریکی در مراکز زیرزمینی، در شرایط جنگی بعد از شارژ شدن باتری‌ها می‌توانیم آن‌ها را نسبت به برق سراسری مجزا کرده و در آن شرایط بدون اتصال به شبکه سراسری از عملکرد آن استفاده ببریم. به‌این‌ترتیب که بخش حیاتی مرکز (مثل مراکز داده‌ها) به همراه سامانه ذخیره‌ساز را با روش قفس فارادی در برابر پالس‌های الکترومغناطیس محافظت نمود، کلیه کابل‌ها و سیم‌کشی‌ها را با عایق‌های ساخته‌شده پوشش داده تا در صورت هرگونه اتفاق، مرکز زیرزمینی کاملاً سالم مانده و عملکردش به‌طور کامل محافظت شود. از آنجا که مراکز حیاتی زیرزمینی اکثراً سامانه‌های کم‌مصرف در زمینه برق هستند این امکان را می‌سازد که با یک ذخیره‌ساز باتری برای چندین ساعت کارکرد مناسب داشته باشند، بنابراین، در شرایط عادی این سامانه به‌طور کامل شارژ شده و در زمان ایجاد خطر از شبکه سراسری جداشده و مرکز مورد نظر به آن وصل خواهد شد و از الکتریسیته آن استفاده می‌کند.

۳-۲-۳. همراه با مولدهای انرژی تجدیدپذیر (نو)

با توجه به کاهش روزافزون هزینه‌های تولید برق تجدیدپذیر، باید به دنبال روشی برای دائمی و پایدار بودن آن باشیم، حدود ۶۸ ٪ انرژی الکتریکی تولیدی در دنیا با استفاده از سوخت‌های فسیلی می‌باشد که از این مقدار، سهم هر یک از سوخت‌ها به ترتیب زغال‌سنگ ۴۲ ٪ ، گاز طبیعی ۲۱ ٪ ، نفت ۵ ٪ و ۳۲ ٪ باقیمانده مربوط به هسته‌ای ۲۱ ٪ ، هیدرو ۱۵ ٪ و ۳ ٪ باقیمانده از انرژی‌های تجدیدپذیر می‌باشد [۱۱]. این در حالی

است که از ۲۸۰ تراوات ساعت برق تولیدی در کشور حدود ۹۰ ٪ از طریق انرژی حرارتی می‌باشد. درصورتی‌که متوسط دی‌اکسید کربن تولیدی به ازای هر کیلووات ساعت برق ۷۰۰ گرم می‌باشد، می‌توان گفت که انتشار ۱۷۶ میلیون تن دی‌اکسید کربن از طریق تولید انرژی و در نیروگاه‌های کشور می‌باشد [۱۲].

انتظار می‌رود تا سال ۲۰۵۰ و با پیشرفت روزافزون انرژی‌های تجدیدپذیر به مرور زمان پروژه‌های خورشیدی و بادی در برخی کشورها مانند هند و آمریکا، برقی به ارزانی برق تولیدی ارزان‌ترین نیروگاه‌های زغال‌سنگی تولید کنند.(شکل ۲)



شکل ۲. مقایسه بهای استفاده از انواع انرژی

روشی که شرکت تسلا در شهر آدلاید استرالیا امتحان کرده، به نتایج خوبی رسیده است. با نصب یک شبکه از باتری‌های لیتیوم-یونی در این شهر، در زمان ارزان بودن برق، آن‌ها را شارژ کرده و در زمان اوج مصرف، برق موجود را به شبکه برمی‌گرداند.

سامانه ذخیره‌ساز انرژی الکتریکی با توان مشخص قادر است انرژی الکتریکی را به مدت تعیین‌شده ذخیره نماید و این سامانه‌ها می‌توانند با مولدهای انرژی متنوعی همچون توربین‌های بادی، پانل‌های فتوولتائیک و ... به‌صورت هیبرید یا مجزا کار کنند.

۳-۲-۴. مراکز صنعتی

تعداد مشترکین صنعتی حدود ۲۳۶ هزار و مقدار مصرف آن‌ها حدود ۸۴ میلیون مگاوات ساعت است که با تقسیم مصرف بر تعداد مشترک به‌طور میانگین مصرف هر یک واحد صنعتی حدود ۳۵۶ مگاوات ساعت به‌دست می‌آید، بااینکه برخی صنایع میزان مصرف بالاتر از این عدد دارند (مانند مجتمع فولاد اصفهان میانگین ۶۰۰ مگاوات ساعت مصرف برق دارد) ولی عدد میانگین مصرف صنایع ۳۵۶ مگاوات‌ساعت می‌باشد با این وجود، این عدد برای صنعت برق کشور عدد بزرگی است و باید در زمان پیک این مصرف تا حد ممکن کاهش یابد، این عدد نشان‌دهنده تأثیر مصرف برق صنایع بر کل مصرف برق کشور و تنظیم پیک بار می‌باشد. درحالی‌که کمتر از یک درصد از مشترکین صنعت برق را صنایع تشکیل می‌دهند، برق صنعتی مصرفی در کشور ما، بین ۳۱ تا ۳۵ درصد کل مصرف برق می‌باشد بنابراین، رعایت مصرف بهینه توسط صنایع می‌تواند کمک شایانی به پایین آمدن پیک بار به‌خصوص در فصل تابستان داشته باشد. همان‌طور که منابع مختلف نشان می‌دهند از سال ۷۶ تا ۹۷ هر چه جلوتر می‌آییم تعداد کارخانه‌ها و صنایع بیشتری وارد چرخه تولید و کار شده‌اند و به‌تبع آن، حداکثر مصرف پیک را افزایش می‌دهند که جهت آمادگی برای رفع نیاز برق در اوج پیک نیاز است که مولدها و نیروگاه‌های بیشتر و با توان بالاتری همیشه آماده تولید باشند که تنها در زمان‌های پیک بار با راندمان مناسب کار می‌کنند و در باقی زمان یا غیرفعال می‌شوند یا با راندمان پایین کار می‌کنند، در این شرایط نیروگاه‌ها بازدهی کمی دارند و فشار اقتصادی زیادی به کشور وارد می‌کنند، درصورتی‌که این کارخانه‌ها و صنایع در زمان کم باری فعالیت کمتری دارند و در طول روز که پیک بار بالایی داریم فعالیت و کارکرد بالاتری دارند؛ بنابراین، اگر برق مصرفی این کارخانه‌ها و صنایع در زمانی که کم باری (پیک پایین) داریم ذخیره شوند و در روزها و زمان‌های پیک بار استفاده شوند این فشار پیک کاهش می‌یابد و حداکثر بار مصرفی در روز حداکثر نیاز مصرف کاهش خواهد یافت، این کار ازیک‌طرف باعث می‌شود، کارخانه‌دار بابت برق مصرفی در زمان پیک بار هزینه کمتری بپردازند چون از برق ذخیره‌شده در زمان ارزانی، استفاده می‌کند، دوم اینکه تعادل بیشتری در پیک و غیر پیک ایجاد می‌شود و نوسان حداکثر پیک نسبت به زمان‌های دیگر کاهش می‌یابد که این امر باعث می‌شود که نیروگاه‌ها و مولدهای تولید انرژی کمتری در حالت آماده‌باش قرار داشته باشند.

۳-۲-۵. بخش مصارف خانگی

میزان مصرف برق یک خانواده در یک منطقه با شرایط آب‌وهوایی میانگین متوسط، در یک شبانه‌روز، در فصل نوسانات، محاسبه‌شده است؛ که بر اساس بررسی‌های انجام‌شده در شرایط عادی خانواده‌ها به‌طور میانگین حدود ۵۲ کیلووات در روز انرژی مصرف دارند که بخش زیادی از این مصرف در پیک مصرفی قرار دارد و برای مردم هزینه بالایی را رقم میزند. بر اساس آخرین مصوبه وزارت نیرو در سال ۱۳۹۵ میزان بهای برق را در حوزه مصرف عمومی در جدول (۱) آورده‌ایم.

جدول ۱. بهای برق مصارف عمومی [۱۳]

تعرفه	قدرت بیش از ۳۰کیلووات			قدرت ۳۰ کیلووات و کمتر		
	بهای انرژی(ریال /kwh)			بهای انرژی(ریال /kwh)		
	کم‌باری	میان‌باری	اوج‌بار	کم‌باری	میان‌باری	اوج‌بار
مسکونی	۲۷,۵	۵۵۷	۱۱۱۴	۴۹۰	۷۲۱	۱۴۴۲

در جدول بالا به‌خوبی تفاوت بین بهای برق در ساعات کم باری، میان‌باری و اوج بار مشخص است. در ابتدا با عدم استفاده از وسایل پرمصرف در زمان پیک که تا حدودی قابل‌اجراست مثلاً می‌توان از ماشین لباس‌شویی یا اتو در زمان غیر پیک استفاده کرد اما نیاز مداوم به برخی وسایل، این امکان را به ما نمی‌دهد و درهرصورت لازم است که در زمان پیک برق که مصرف در کل کشور در آن زمان بالاست و برق، قیمت بالایی هم دارد به کار گرفته شوند مثل کولرگازی که یک وسیله با مصرف برق بالا است که نمی‌توان زمان پیک بار آن را خاموش کرد، بنابراین، برای این‌گونه دستگاه‌ها و کمک به مصرف بهینه و اقتصاد خانواده‌ها و کشور بهترین راه ذخیره‌سازی برق در زمان غیر پیک و استفاده از آن در زمان پیک بار است.

۳-۲-۶. در مجاورت پست برق

در زمان و شرایط عادی بهترین محل برای قرار دادن سامانه‌های ذخیره‌ساز در مجاورت پست برق است زیرا که استفاده از سامانه‌های ذخیره انرژی در شبکه توزیع در بخش مصرف‌کننده‌ها زمانی صرفه اقتصادی خواهد داشت که شبکه هوشمند باشد و سامانه بتواند با شبکه سراسری به‌راحتی مبادله انرژی و خریدوفروش انرژی را داشته باشد.

بنابراین، یکی از مناطقی که لازم است از ذخیره‌سازهای الکتریکی استفاده شود در محدوده پست‌های حیاتی کشور می‌باشد. درصورتی‌که شبکه به ذخیره‌ساز الکتریکی مجهز باشد به‌محض بالا رفتن پیک بار (در حدی که پیک از محدوده مجازی که تعریف می‌شود عبور کند) و یا ازکارافتادن پست و یا ژنراتور، ذخیره‌ساز که در زمان عادی و پیک پایین انرژی لازم را ذخیره کرده، بدون وقفه وارد مدار می‌شود و برق شبکه را برای مدت‌زمان لازم تأمین می‌کند.

مقدار بهینه سامانه ذخیره انرژی الکتریکی (BESS) در شبکه، از ۵۰۰ تا ۱۵۰۰ مگاوات تعیین شده است، از منظر پدافند غیرعامل یکی از راهکارهای محافظت از زیرساخت‌ها پراکنده‌سازی آنها است از طرفی جهت پوشش دادن تعداد مناطق بیشتر در شرایط بحرانی این ظرفیت را در تعدادی از مهم‌ترین و حیاتی‌ترین پست‌های برق کشور تقسیم می‌کنیم.

۳-۳. نحوه قرارگیری ذخیره‌سازها در شبکه برق

با توجه به مطالب ارائه‌شده در بخش‌های قبل، جهت قرارگیری سامانه‌های BESS در شبکه، بخش توزیع نسبت به بخش تولید و انتقال دارای اولویت و بازدهی بالاتری می‌باشد. BESS در شبکه توزیع جهت عملکردهای مختلفی به‌کار گرفته می‌شود ازجمله:

۱- مراکز حیاتی و حساس کشور
۲- مراکز راهبردی و زیرزمینی
۳- در مناطقی که انرژی تجدیدپذیر استفاده می‌کنند.
۴- صنعت
۵- مصارف خانگی
۶- ایستگاه‌های برق

همان‌طور که بیان شده، موارد ۱ تا ۵ ازجمله مناطقی هستند که وجود سامانه‌های BESS در حدی که قطع برق باعث بروز بحران در آنها نشود، ضرورت دارد.

به‌طورکلی، ایستگاه‌های برق به‌عنوان مناسب‌ترین بخش جهت قرارگیری سامانه‌های BESS تعیین‌شده‌اند، با محاسبات انجام‌شده، مقدار ذخیره‌ساز موردنیاز در شبکه توزیع جهت پیک‌سایی، حدود ۵۰۰ تا۱۵۰۰ مگاوات است.

ایستگاه‌های برق کشور با توجه به اهمیت، نقش و عملکردی که در شبکه دارند از اولویت بالاتری جهت قرارگیری سامانه‌های ذخیره‌ساز برخوردارند از این‌رو ظرفیت BESS مورد نیاز شبکه را بین حیاتی‌ترین ایستگاه‌های برق به ترتیب اولویت و اهمیت تقسیم می‌کنیم (به‌دلیل طبقه‌بندی داشتن اطلاعات مربوط به اولویت‌بندی ایستگاه‌های برق نام ایستگاه‌ها قابل‌ارائه نیست).

با لحاظ نمودن شاخص‌هایی ازجمله وضعیت تأمین بودجه، توانایی شرکت‌های تولیدکننده در ساخت و تحویل، منابع در اختیار، ضرورت و میزان نیاز به سامانه‌های ذخیره‌ساز و ...، درصدی از ظرفیت که در توان کشور ما باشد را هر سال به شبکه تزریق کرده که با مطالعات انجام‌شده حداکثر ۲۰ درصد از مصرف پیک بار شبکه، قابل تأمین می‌باشد که به این صورت بعد از چند سال کل ظرفیت موردنیاز جهت پیک‌سایی را در شبکه تأمین کرده‌ایم.

پراکنده‌سازی ازجمله الزامات پدافند غیرعامل جهت مراقبت و مصون‌سازی زیرساخت‌ها و مراکز می‌باشد از این‌رو ظرفیت BESS موردنیاز در شبکه را به ترتیب اولویت بین ایستگاه‌های برق حیاتی کشور تقسیم کرده و متناسب با ارزش و اهمیت هر یک از ایستگاه‌ها بخشی از ظرفیت را در مجاورت آن قرار خواهیم داد.

۳-۳-۱. بهترین نوع باتری قابل‌استفاده

با توجه به موارد مربوط به فنّاوری باتری‌ها که در فصل دوم به‌طور کامل شرح داده‌شده است، مشخصات اصلی ۷ نوع از باتری‌ها به شکل بسیار مختصر استخراج‌شده و در جدول زیر

آورده‌ایم که متناسب با کارکرد مورد نیاز از باتری‌ها، نوع مناسب باتری‌ها را انتخاب می‌کنیم.

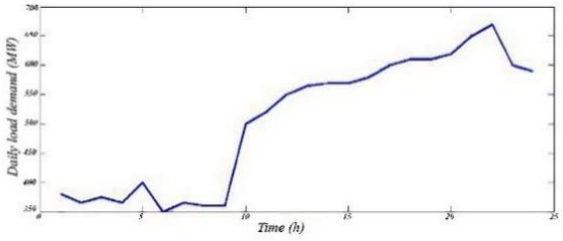
جدول ۲. مشخصات فنی باتری‌ها [۱۵،۱۴]

نوع باتری	توان نامی (MW)	بازدهی(%)	چگالی انرژی (Wh/kg)	تخلیه خودی روزانه (%)	طول عمر (سال)	قیمت ($/kwh)
Na-S	۰٫۰۰۵-۸	۷۵-۹۰	۱۵۰-۲۵۰	۲۰	۱۰-۱۵	۳۰۰-۵۰۰
Ni-Cd	≤۴۰	۶۰-۷۳	۱۵-۳۰۰	۰٫۲-۰٫۶	۱۰-۲۰	۸۰۰-۱۵۰۰
Li-ion	۱-۱۰۰	۸۵-۹۵	۱۵۰-۳۵۰	۰٫۱-۰٫۳	۵-۱۵	۶۰۰
VRFB	۰٫۰۳-۳	۶۵-۸۵	۱۰-۳۵	ناچیز	۵-۱۰	۶۰۰
Zn-Br	۰٫۵-۲	۶۰-۷۰	۳۰-۸۵	ناچیز	۵-۱۰	۵۰۰
ZEBRA	۵۰	۸۶-۸۸	۱۰۰-۱۴۰	۱۵	۱۵	۱۵۰۰
Lead-acid	≤۲۰	۷۰-۹۰	۳۰-۵۰	۰٫۱-۰٫۲	۵-۱۵	۳۳۰

با توجه به ویژگی‌ها و قابلیت‌های دارای اهمیت برای باتری‌ها که در بخش‌های قبل آورده‌ایم و مشخصات انواع باتری‌ها که در جدول (۲) مشخص‌شده، باتری لیتیوم یون با بازدهی ۹۵-۸۵ درصد و چگالی انرژی ۳۵۰-۱۵۰ وات‌ساعت بر کیلوگرم، (به کمک نرم‌افزار گمز) بهینه‌ترین نوع باتری جهت ذخیره‌سازی برق انتخاب شد.

۴. تجزیه و تحلیل و ارائه مدل

جهت نشان دادن کارایی ذخیره‌سازهای انرژی در این پروژه، علاوه بر آنالیز قابلیت اطمینان (میزان قطعی بار)، کارایی ذخیره‌سازهای انرژی در پیک‌سایی و کاهش هزینه‌های شبکه (بررسی اقتصادی) مورد بررسی قرار گرفت، با توجه به نمودار بار روزانه تغییرات تقاضای مصرف در طول یک شبانه‌روز از حدود ۳۵۰ تا ۷۰۰ مگاوات در شبکه انتخاب شده، متغیر است و پیک بار نسبت به میانگین تقاضا فاصله زیادی دارد (شکل ۳).



شکل ۳. نمودار بار روزانه (مگاوات/ ساعت)

۶ ژنراتور حرارتی به همراه یک مولد بادی برای تأمین بار مورد نیاز شبکه استفاده می‌شود، حال در چنین شبکه‌ای بررسی فنی، اقتصادی حضور و عدم حضور ذخیره‌سازهای الکتریکی مورد ارزیابی قرار گرفت.

مشخصات واحدهای حرارتی شبکه در جدول زیر مشاهده می‌شود، در ادامه تعریف مختصری از پارامترهای موجود در جدول آورده‌ایم.

جدول ۳. اطلاعات ۶ واحد حرارتی [۱۶]

واحد	A	B	C	Pmin	Pmax	SU	SD	MUT	MDT
۱	۰٫۰۶۹	۲۶٫۲۴	۳۱٫۶۷	۵	۳۰	۴۰	۰	۱	۱
۲	۰٫۰۶۹	۲۶٫۲۴	۳۱٫۶۷	۵	۳۰	۴۰	۰	۱	۱
۳	۰٫۰۶۹	۲۶٫۲۴	۳۱٫۶۷	۵	۳۰	۴۰	۰	۱	۱
۴	۰٫۰۱۹	۱۲٫۸۸	۶٫۷۸	۱۵۰	۳۰۰	۴۴۰	۰	۱۰	۱۰
۵	۰٫۰۱۹	۱۲٫۸۸	۶٫۷۸	۱۵۰	۳۰۰	۱۱۰	۰	۱۰	۱۰
۶	۰٫۰۶۹	۲۶٫۲۴	۳۱٫۶۷	۱۰	۳۰	۱۵	۰	۱	۱

a_i ،b_i ،c_i: ضرایب هزینه واحدهای حرارتی / SU: هزینه روشن ماندن واحد حرارتی / SD: هزینه خاموش ماندن واحد حرارتی / MUT: حداقل زمان روشن ماندن واحد / MDT: حداقل زمان خاموش ماندن واحد. قابل‌ذکر است که در این تحقیق عدم قطعیت توان تولیدی واحد بادی لحاظ نشده است و تنها با اتکا بر داده‌های تاریخی بر اساس مرجع [۱۶] توان خروجی واحد بادی لحاظ می‌گردد که در جدول (۴) قابل مشاهده است.

جدول ۴. توان تولیدی واحد بادی (مگاوات)

ساعت	توان	ساعت	توان
۱	۵۱/۳۹۵	۱۳	۱۰۲/۵
۲	۴۰/۸۸۴	۱۴	۱۰۲/۵
۳	۵۴/۱۳۷	۱۵	۱۰۲/۵
۴	۵۷/۸۴۷	۱۶	۱۰۲/۵
۵	۸۰/۳۹۶	۱۷	۱۰۲/۵
۶	۲۲/۶۰۴	۱۸	۱۰۲/۵
۷	۴۲/۷۶۴	۱۹	۱۰۲/۵
۸	۳۰/۱۸۱	۲۰	۸۳/۳۳۶
۹	۱۰۲/۵	۲۱	۴۹/۰۰۶
۱۰	۱۰۲/۵	۲۲	۷/۲۶۷
۱۱	۱۰۲/۵	۲۳	۸/۳۴
۱۲	۱۰۲/۵	۲۴	۹/۵۱۴

۴-۱. بررسی اقتصادی حضور و عدم حضور ذخیره‌سازهای الکتریکی در شبکه توزیع برق

گام اول: تعریف تابع هدف

تابع هدف که با کمی تغییر بر اساس مرجع [۱۶] در نظر گرفته‌شده، جهت حداقل کردن هزینه بهره‌برداری و هزینه روشن و خاموش ماندن واحدهای حرارتی است:

$$\text{Min} = \sum_t \left(\sum_i \left[c_i + b_i P_i(t) + a_i P_i^2(t) + SU_i + SD_i\right] + \sum_{j=1} P_{c,j}(t)\lambda(t)\right) \quad (۱)$$

- در رابطه بالا $P_i(t)$ توان تولیدی واحد i ام در زمان t ام است.
- ضرایب c_i، b_i و a_i، ضرایب هزینه واحد حرارتی i ام هستند.
- جملات دوم و سوم در تابع هدف، هزینه روشن و خاموش ماندن واحد حرارتی را نشان می‌دهند.
- جمله آخر تابع هدف مربوط به هزینه انرژی خریداری‌شده توسط ذخیره‌ساز است.
- $P_{c,j}$ میزان توان خریداری‌شده جهت شارژ است.
- $\lambda(t)$ قیمت خرید و فروش برق در لحظه t ام.
- هزینه بهره‌برداری از توربین بادی برابر صفر در نظر گرفته شده است.

گام دوم: معرفی قیود مسئله

- قید تعادل: در هرلحظه از شبانه‌روز باید توان تولیدی از واحدهای موجود با توان مورد تقاضای مشترکین برابر باشد.

$$\sum_i P_i(t) + P_{wind}(t) \pm P_{storage}(t) = \sum_l P_{Load_l}(t) \qquad \forall\, t=1,....24 \quad (۲)$$

در رابطه بالا $P_{wind}(t)$ توان توربین بادی، $P_{storage}(t)$ توان ذخیره‌ساز که در حالت دشارژ با علامت مثبت و در حالت شارژ با علامت منفی است و P_{Load_l} بار مصرفی است.

- قیود بهره‌برداری از واحدهای حرارتی شامل حداقل و حداکثر توان تولیدی، حداقل زمان روشن و خاموش ماندن: (واحدهای حرارتی را نمی‌توان سریع از مدار خارج کرد و همچنین نمی‌توان آن‌ها را روشن کرد. فرضاً وقتی حداقل زمان خاموش ماندن یک واحد ۲ ساعت است، یعنی برای روشن کردن مجدد آن باید از آخرین زمانی که خاموش شده است ۲ ساعت گذشته باشد).

$$P_i^{\min}(t) \le P_i(t) \le P_i^{\max}(t) \quad (۳)$$

$$MUT_i \;\; (u_i(t) - u_i(t-1)) \le T_i^{on} \quad (۴)$$

$$MDT_i \;\; (u_i(t-1) - u_i(t)) \le T_i^{off} \quad (۵)$$

در رابطه‌های "۴ و ۵"، $u_i(t)$ و $u_i(t-1)$ متغیر باینری در زمان t و t-۱ هستند که در صورت یک بودن به معنی روشن بودن واحد حرارتی و در صورت صفر بودن به معنای خاموش بودن آن است. T_i^{on} و T_i^{off} مدت‌زمان روشن و خاموش ماندن واحد i ام است

- قیود مربوط به ذخیره‌ساز انرژی: شامل حداقل و حداکثر توان شارژ و دشارژ شده، حالت شارژ (SoC) و تفکیک کردن حالت‌های شارژ و دشارژ از همدیگر (ذخیره‌ساز نمی‌تواند هم‌زمان هم شارژ کند و هم دشارژ شود لذا باید این دو حالت کاری از همدیگر تفکیک شوند که به کمک دو پارامتر باینری این دو حالت کاری از همدیگر تفکیک شده است).

$$SOC^{\min} \le SOC(t) \le SOC^{\max} \quad (۶)$$

$$P_{\text{dis.storage}}^{\min} x_d \le P_{storage} \le P_{\text{dis.storage}}^{\max} x_d \quad (۷)$$

$$P_{\text{char.storage}}^{\min} x_c \le -P_{storage} \le P_{\text{charstoraget}}^{\max} x_c \quad (۸)$$

$$x_d + x_c = 1 \quad (۹)$$

در رابطه (۷-۹)، x_d و x_c همان پارامترهای باینری هستند که برای جداسازی حالت شارژ و دشارژ به کار می‌روند. هرکدام که یک باشند متناسب با آن قید مربوطه حداکثر و حداقل توان شارژ و دشارژ رعایت می‌شود. به‌طور مثال اگر در حالت شارژ باشیم ($x_c = 1$) قید (۸) فعال‌شده و قید (۷) در نظر گرفته نمی‌شود.

- به‌منظور جلوگیری از تأثیر برنامه‌ریزی یک روز بر روی روزهای دیگر، لازم است که SOC باتری در ابتدا و انتهای دوره برنامه‌ریزی برابر باشد که این قید نیز به‌صورت رابطه (۷) مدل‌سازی می‌شود.

$$SOC(end) = SOC_0 \quad (۱۰)$$

گام سوم: بررسی نتایج

برای بررسی نتایج دو حالت را در نظر می‌گیریم که در زیر آمده است. در حالت اول فرض بر این است که ذخیره‌ساز انرژی حضور ندارد و برنامه‌ریزی را برای این حالت انجام می‌دهیم

- در حالت دوم برنامه‌ریزی در حضور ذخیره‌سازهای الکتریکی انجام‌شده و برآورد هزینه و سود حاصل محاسبه شد.

بعد از قرار دادن ذخیره‌ساز در شبکه برق، در ساعاتی تأمین برق شبکه علاوه بر مولد بادی و مولدهای حرارتی توسط ذخیره‌ساز نیز انجام می‌شود از این‌رو، توان‌های تولیدی مولدهای حرارتی نسبت به حالت قبل تغییر خواهند کرد.

۵. نتایج و بحث

برای حالت اول که ذخیره‌ساز انرژی موجود نیست، توان تولیدی واحدهای حرارتی جهت پاسخ‌گوی بار شبکه با رعایت تمامی قیود اعمال شده، مطابق جدول (۵) به‌دست آمد.

جدول ۵. توان تولید ۶ واحد حرارتی بدون در نظر گرفتن ذخیره‌ساز

	واحد ۱	واحد ۲	واحد ۳	واحد ۴	واحد ۵	واحد ۶
۱	۱۱/۱۱۵	۰	۱۱/۱۱۵	۱۵۰	۱۵۰	۱۱/۱۱۵
۲	۵	۰	۵	۱۵۹/۱۱۳	۱۵۹/۱۱۳	۱۰
۳	۰	۰	۰	۱۶۲/۷۱	۱۶۲/۷۱	۰
۴	۰	۰	۰	۱۶۳/۳۳	۱۶۳/۳۳	۰
۵	۰	۰	۰	۱۵۷/۳۹	۱۵۷/۳۹	۰
۶	۰	۰	۰	۱۷۴/۶۱۳	۱۷۴/۶۱۳	۰
۷	۰	۰	۰	۱۵۶/۴۸	۱۵۶/۴۸	۰
۸	۰	۰	۰	۱۶۸/۸۶۵	۱۶۸/۸۶۵	۰
۹	۰	۰	۰	۱۹۸/۳۴	۱۹۸/۳۴	۰
۱۰	۰	۰	۰	۲۰۲/۰۰۵	۲۰۲/۰۰۵	۰
۱۱	۰	۰	۰	۲۱۰/۰۳۵	۲۱۰/۰۳۵	۰
۱۲	۰	۰	۰	۲۱۶/۶	۲۱۶/۶	۰
۱۳	۰	۰	۰	۲۲۲/۵۷	۲۲۲/۵۷	۰
۱۴	۰	۰	۰	۱۷۵/۰۹۲	۱۷۵/۰۹۲	۰
۱۵	۰	۰	۰	۲۲۳/۹۴	۲۲۳/۹۴	۰
۱۶	۰	۰	۰	۲۲۹/۳۸۵	۲۲۹/۳۸۵	۰
۱۷	۰	۰	۰	۲۳۶/۲۱۵	۲۳۶/۲۱۵	۰
۱۸	۰	۰	۰	۲۴۱/۹۷۵	۲۴۱/۹۷۵	۰
۱۹	۰	۰	۰	۲۵۶/۶۷۵	۲۵۶/۶۷۵	۰
۲۰	۰	۰	۰	۲۸۳/۲۸۲	۲۸۳/۲۸۲	۰
۲۱	۰	۸/۳۹۳	۰	۲۹۹/۲۰۶	۲۹۹/۲۰۶	۱۰
۲۲	۰	۲۳/۳۹۳	۱۵	۳۰۰	۳۰۰	۲۵
۲۳	۰	۱۰/۳۲۷	۱۰/۳۲۷	۳۰۰	۳۰۰	۱۰،۳۲۷
۲۴	۰	۰	۵	۲۹۷/۹۲۸	۲۹۷/۹۲۸	۰

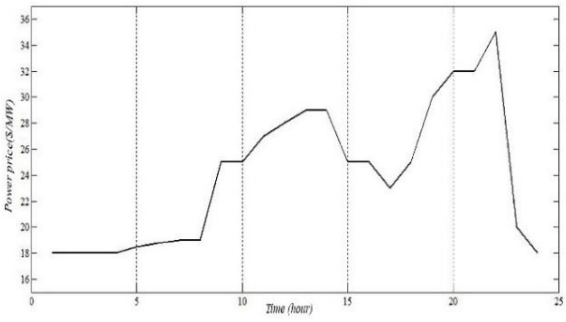
از جدول (۲) (پارامترهای هزینه واحدهای حرارتی)، می‌توان دریافت که ژنراتورهای ۱،۲،۳ و ۶ ژنراتورهای گران‌قیمتی هستند. لذا در صورت روشن ماندن هزینه زیادی را به شبکه تحمیل خواهند کرد. در این حالت که سامانه فاقد ذخیره‌ساز الکتریکی است، هزینه کل شبکه بر اساس تابع تعریف‌شده و با رعایت تمامی قیود (قید تعادل، قیود بهره‌برداری از واحدهای حرارتی شامل حداقل و حداکثر توان تولیدی و حداقل زمان روشن و خاموش ماندن) برابر ۱۶۵۹۷۹،۵ دلار محاسبه شده است.

در حالت دوم برنامه‌ریزی در حضور ذخیره‌ساز انرژی صورت می‌گیرد. در جدول (۶) مشخصات ذخیره‌سازی که در شبکه به کار گرفته شد، مشاهده می‌شود.

جدول ۶. ویژگی‌های ذخیره‌ساز موردنظر

راندمان λ(٪)	SOC^{min}/SOC^{max} (%)	ظرفیت (MW)	حداقل و حداکثر توان شارژ یا دشارژ (MW)	حداقل زمان شارژ و دشارژ (hr)
۹۰	۹۰-۲۰	۱۰۰	۵۰	۲

همان‌طور که بیان شد، هدف اصلی ذخیره‌ساز، ذخیره کردن انرژی در ساعت‌های کم باری و تحویل آن در ساعت پیک بار است. قیمت برق متناسب با تغییرات بار مصرفی کم و زیاد می‌شود، در شکل (۴) این موضوع به‌خوبی قابل مشاهده است.



شکل ۴. منحنی قیمت روزانه خرید و فروش برق (مگاوات/ دلار)

جهت پاسخگویی به رشد بار بعد از قرارگیری ذخیره‌ساز با رعایت تمامی قیود و لحاظ نمودن قیمت خرید و فروش برق در شبکه مطابق نمودار ۴-۲، نتایج به‌دست‌آمده برای توان تولیدی واحدهای حرارتی و میزان توان شارژ و دشارژ شده ذخیره‌ساز به شکل جدول (۷) تغییر کرد.

- هزینه بهره‌برداری از واحدهای حرارتی شبکه در این حالت برابر ۱۶۲۴۸۳٫۶ دلار است. هزینه خرید برق توسط ذخیره‌ساز نیز برابر ۱۹۹۱٫۳۹ دلار است. لذا هزینه کلی در حالت حضور ذخیره‌ساز برابر ۱۶۴۴۷۵ دلار است؛ یعنی بیش از ۱۵۰۰ دلار هزینه کمتر در طول یک شبانه‌روز (۵۵۰ هزار دلار در هر سال) انجام‌شده که این فقط بخشی از سود حاصل از پیک‌سایی توسط ذخیره‌سازها است.

علاوه بر صرفه اقتصادی ناشی از پیک سایی، در صورت استفاده از ذخیره‌ساز در شبکه نیازی به وجود نیروگاه‌های ۳۰ مگاواتی شماره ۲ و ۳ و ۶ که نیروگاه‌های پرهزینه‌ای نیز بوده‌اند، نداریم.

جدول ۷. توان تولید واحدها در حضور ذخیره‌ساز انرژی

شارژ	دشارژ	واحد ۶	واحد ۵	واحد ۴	واحد ۳	واحد ۲	واحد ۱	
۰	۳۳/۳۴۶	۰	۱۵۰	۱۵۰	۰	۰	۰	۱
۰	۵	۰	۱۶۹/۱۱۳	۱۶۹/۱۱۳	۰	۰	۰	۲
۳۲/۹۳۵	۰	۰	۱۶۲/۷۱۱	۱۶۲/۷۱۱	۰	۰	۰	۳
۳۱/۰۹۲	۰	۰	۱۶۳/۱۳	۱۶۳/۱۳	۰	۰	۰	۴
۰	۰	۰	۱۵۷/۳۹	۱۵۷/۳۹	۰	۰	۰	۵
۰	۰	۰	۱۷۴/۶۱۳	۱۷۴/۶۱۳	۰	۰	۰	۶
۰	۰	۰	۱۶۵/۴۸	۱۶۵/۴۸	۰	۰	۰	۷
۰	۰	۰	۱۶۸/۸۶۵	۱۶۸/۸۶۵	۰	۰	۰	۸
۰	۰	۰	۱۹۸/۳۴	۱۹۸/۳۴	۰	۰	۰	۹
۰	۰	۰	۲۰۲/۰۰۵	۲۰۲/۰۰۵	۰	۰	۰	۱۰
۰	۰	۰	۲۱۰/۰۳۵	۲۱۰/۰۳۵	۰	۰	۰	۱۱
۰	۰	۰	۲۱۶/۶	۲۱۶/۶	۰	۰	۰	۱۲
۰	۰	۰	۲۲۲/۵۷	۲۲۲/۵۷	۰	۰	۰	۱۳
۰	۰	۰	۱۷۵/۰۹۲	۱۷۵/۰۹۲	۰	۰	۰	۱۴
۰	۰	۰	۲۲۳/۹۴	۲۲۳/۹۴	۰	۰	۰	۱۵
۰	۰	۰	۲۲۹/۳۸۵	۲۲۹/۳۸۵	۰	۰	۰	۱۶
۰	۰	۰	۲۳۶/۲۱۵	۲۳۶/۲۱۵	۰	۰	۰	۱۷
۰	۰	۰	۲۴۱/۹۷۵	۲۴۱/۹۷۵	۰	۰	۰	۱۸
۰	۰	۰	۲۵۶/۶۷۵	۲۵۶/۶۷۵	۰	۰	۰	۱۹
۰	۰	۰	۲۸۳/۲۸۲	۲۸۳/۲۸۲	۰	۰	۰	۲۰
۰	۵	۰	۳۰۰	۳۰۰	۰	۰	۱۱/۸۰۴	۲۱
۰	۴۷	۰	۳۰۰	۳۰۰	۰	۰	۱۶/۴۳۶	۲۲
۰	۱۴/۵	۰	۳۰۰	۳۰۰	۰	۰	۱۶/۴۳۶	۲۳
۴۶/۶۰۶	۰	۰	۲۷۹/۹۲۸	۲۷۹/۹۲۸	۰	۰	۵	۲۴

۵-۱. محاسبه هزینه تمام‌شده (LCOE[1]) برای ذخیره‌ساز (BESS) به‌کار رفته در شبکه

یکی از مطالعات مهم در حوزه اقتصاد انرژی، محاسبه قیمت تمام‌شده برای هر یک از حامل‌های اولیه و یا ثانویه انرژی (به‌طور خاص، انرژی الکتریکی) است. وجود یک روش و الگوی جامع که بتواند قیمت واقعی انرژی را همراه با جزئیات آن محاسبه و تحلیل نماید، این‌روش از مهم‌ترین ابزارهای تحلیلی در اقتصاد انرژی است که به‌ویژه در صنعت برق یکی از مهم‌ترین چالش‌ها و نیازهای این صنعت می‌باشد، در این بخش هزینه هم‌تراز یا LCOE برای ذخیره‌ساز به‌کاررفته مورد بررسی قرار گرفت. رابطه (۱۱) بر اساس مرجع [۱۶] به‌عنوان معادله اصلی جهت محاسبه هزینه هم‌تراز شده در نظر گرفته شد.

$$LCOE = \frac{ALCC}{yearly\ operating\ hours} = \frac{C_{LCC,a}}{n \times h}(€/kWh) \qquad (۱۱)$$

LCOE: هزینه یکنواخت یا هم‌تراز شده برحسب سنت بر کیلووات ساعت

ALCC[2]: هزینه چرخه کارکرد

[1] Levelized cost of electricity
[2] Annualized life cycle costs

CLCC,a: هزینه سرمایه‌گذاری کلی

n: عمر ذخیره‌ساز برحسب سال

h: ساعت

در گام اول مشخصات باتری مورد استفاده در جدول (۸) ارائه‌شده است.

جدول ۸. مشخصات باتری استفاده‌شده

پارامتر	مقدار
طول عمر	۷ سال
هزینه سرمایه اولیه	۷۰۰ $/kWh
هزینه تعمیر و نگهداری	۲ درصد هزینه سرمایه‌گذاری برای هر سال
نرخ بهره	۲۰ درصد
راندمان باتری	۹۰ درصد

روابط مربوط به محاسبه LCOE برای ذخیره‌سازها در مطالعاتی که به بررسی تطبیقی هزینه چرخه عمر سامانه‌های ذخیره ساز انرژی الکتریکی پرداخته اند به‌طور کامل ارائه‌شده است[۱۷]. بر اساس توضیحات ارائه‌شده در این منابع، ابتدا لازم است هزینه کلی سرمایه‌گذاری با در نظر گرفتن نرخ بهره به‌صورت سالیانه محاسبه شود برای این کار ابتدا ضریب بازگشت سرمایه (CRF) به‌صورت زیر محاسبه می‌شود:

$$CRF = \frac{i(1+i)^T}{(1+i)^T - 1} \quad (۱۲)$$

در این رابطه i نرخ بهره بوده و T طول عمر ذخیره‌ساز می‌باشد. با در نظر گرفتن نرخ بهره ۲۰ درصد و طول عمر ۷ سال برای باتری، مقدار CRF به‌صورت زیر به‌دست می‌آید:

$$CRF = \frac{0.2(1+0.2)^7}{(1+0.2)^7 - 1} = 0.2774$$

هزینه سرمایه‌گذاری بر اساس داده‌های جدول (۷) می‌باشد.

$$TCC = 700 \times 1000 = 700{,}000 \ \$/MWh$$

با استفاده از CRF، سرمایه‌گذاری سالیانه به‌صورت زیر محاسبه می‌شود:

$$C_{cap,a} = TCC \times CRF\left(\frac{€}{kW} - yr\right) \quad (۱۳)$$

$$C_{cap,a} = 700 \times 10^3 \times 0.2774 = 194200 \ \$$$

نتایج بالا نشان می‌دهد که سرمایه‌گذاری اولیه (TCC) به مبلغ ۷۰۰ هزار دلار، معادل ۱۹۴۲۰۰ دلار بر مگاوات ساعت سرمایه‌گذاری سالیانه می‌باشد.

همان‌طور که اشاره شد، هزینه تعمیرات دو درصد هزینه سرمایه‌گذاری اولیه در نظر گرفته‌شده است. با در نظر گرفتن هزینه سالیانه تعمیر و نگهداری سامانه ($C_{o\&M,a}$)، هزینه سرمایه‌گذاری کلی ($C_{LCC,a}$) به‌صورت زیر به‌دست می‌آید:

$$C_{LCC,a} = C_{cap,a} + C_{O\&M,a}\left(\frac{€}{kW} - yr\right) \quad (۱۴)$$

$$C_{LCC,a} = 194200 + 0.02 \times 700{,}000 = 208200 \ (\$/MWh)$$

درنهایت LCOE برای ذخیره‌ساز با در نظر گرفتن اینکه ذخیره‌ساز در هر شبانه‌روز ۸ ساعت مورد بهره‌برداری قرار گرفت، به‌صورت رابطه زیر محاسبه می‌شود:

$$LCOE = \frac{208200}{365 \times 8} = 71.3014 \quad (\$/MWh)$$

بر اساس این توضیحات و داده‌های ارائه‌شده در جدول۸، مشخص است که مقدار LOCE برای ذخیره‌ساز استفاده‌شده در این کار برابر ۷۱/۳۰۱۴ دلار بر مگاوات ساعت، معادل ۷/۱۳ سنت بر کیلووات ساعت به‌دست می‌آید.

در این بخش با کم کردن هزینه انرژی جهت ذخیره‌سازی در باتری (شارژ باتری) از LCOE در نهایت LCOS حاصل می‌شود.

$$\text{LCOS} = \text{LCOE} - \frac{\text{Price of charging power}}{\text{overall efficiency}} \ (€/\text{kwh}) \quad (۱۵)$$

از آنجا که برق در کم باری (قیمت پایین) مورد ذخیره‌سازی قرار می‌گیرد، بنابراین، مطابق نمودار قیمت بار و زمان‌های شارژ باتری در شبکه مدل شده، دو قیمت برای انرژی موجود است، ۱۸ دلار و ۲۲ دلار به ازای هر مگاوات

قیمت شارژ به ازای هر مگاوات: (به‌طور متوسط) ۲۰ دلار و قیمت شارژ به ازای هر مگاوات ساعت: ۰/۵۵ دلار

راندمان باتری استفاده شده: ۹۰ درصد

LCOE : ۷۱/۳۰۱۴ دلار بر مگاوات ساعت

$$\text{LCOS} = 71.3014 - \frac{0.55}{0.9} = ۷۰.۶۹ \ (\$/\text{MWh}) = 7.069 \ (\text{ct/kwh})$$

این‌روش علاوه بر الگوریتم محاسبات دقیق، قابلیت مقایسه نتایج حاصل را برای فناوری‌های مختلف در اختیار قرار می‌دهد. ازاین‌رو نتیجه حاصل‌شده برای ذخیره‌ساز با نتایج حاصل برای سایر فناوری‌ها از مطالعات مختلف که به بررسی تطبیقی هزینه چرخه عمر سامانه‌های ذخیره ساز انرژی الکتریکی پرداخته اند،

مقایسه شده است.

هزینه تمام‌شده انرژی (هم‌تراز) در فناوری سیکل ترکیبی (۷٫۳ ct/kWh)، فنّاوری زغال‌سنگ (۶/۸ ct/kWh تا ۸/۷)، فنّاوری هسته‌ای (۸/۳ ct/kWh تا ۱۰/۵)، فنّاوری بادی (۸/۳۸ ct/kWh تا ۱۲/۱۵) تعیین شده [۱۷] و بر اساس محاسبات انجام‌شده در این پروژه، هزینه هم‌تراز فنّاوری باتری در شبکه به‌کار رفته ct/kWh ۷/۰۶ به‌دست‌آمده است، لذا به‌وضوح مشخص است که هزینه هم‌تراز برای باتری‌ها نسبت به سایر فناوری‌ها جهت کاربرد مورد نظر مقرون به‌صرفه‌تر و پایین‌تر است.

۶. نتیجه‌گیری

به‌دلیل خصوصیت‌های ذاتی شبکه‌های برق و وجود آسیب‌پذیری‌های فراوان در آنها، انواع رویدادهای انسان‌ساخت و طبیعی همواره آن را تهدید می‌کنند، به همین دلیل در جهت مصون‌سازی مراکز حیاتی، حساس و راهبردی و مراکز نظامی و زیرزمینی کشور برای شرایط بحرانی و جهت حفظ اقتصاد و پایداری شبکه‌های برق در تمامی زمان‌ها به‌خصوص در شرایط پیک بار، استفاده از سامانه‌های ذخیره‌ساز انرژی الکتریکی در شبکه‌های برق ضروری است.

از ابتدایی‌ترین الزامات پدافند غیرعامل رعایت اصل پراکنده‌سازی است، بنابراین، بخشی از ظرفیت تعیین‌شده برای ذخیره‌سازها در کنار مولدهای خورشیدی و باقی ظرفیت در کنار پست‌های با اهمیت بالای کشور به‌صورت پراکنده قرار می‌گیرد.

۷. مرجع‌ها

[1] Mashhadi, H. “Providing Model for Infrastructure Vulnerability Assessment in the Country”; M.Sc. Thesis, Malek Ashtar University of Technology, 2012 (In Persian).

[2] Senjyu, T.; Shimabukuro, K.; Uezato, K; Funabashi, T. “A Technique for Thermal and Energy Storage System Unit Commitment”; IEEE Power & Energy Society General Meeting 2005, 1, 601-606.

[3] Deptt. Of Energy.“ Energy Storage Systems ”; sandia.gov, 2017 [Online]. Available: https://www.sandia.gov/ess-ssl/energy-storage-systems-history/.

[4] Marra, F.; Yang, G.; Traeholt, C.; Ostergaard, J.; Larsen, E. “A Decentralized Storage Strategy for Residential Feeders with Photovoltaics”; IEEE Trans. Smart Grid 2014, 5(2), 974-981.

[5] Tant, J. “Multi objective Battery Storage to Improve PV Integration in Residential Distribution Grids”; IEEE Power & Energy Society General Meeting 2013, 4, 182–191.

[6] Ahmadian, A.; Golkar, M.; Sedghi, M. “Optimal Storage Planning in Active Distribution Network Considering Uncertainty of Wind Power Distributed Generation”; IEEE Trans. Power System. 2016, 31, 304–316.

[7] Diaz-Gonzalez, F. “A Review of Energy Storage Technologies for Wind Power Applications”; Renew. Sust. Energ. Rev. 2012, 16, 21-54.

[8] Golkar, M.; Sedghi, M. “Distribution Network Expansion Considering Distributed Generation and Storage Units Using Modified PSO Algorithm”; Int. J. Elec. Power 2013, 52, 221–230.

[9] Ministry of Energy. “New Approaches to the Ministry of Energy”; Ministry of Energy Public Relations and Information Center 2016 (In Persian).

[10] Ministry of Energy. “Detailed Statistics of the Iranian Power Industry for Strategic Management”; Tavanir Motherhood Corporation 2018 (In Persian).

[11] Jun, L; Yang, A. “Electrochemical Energy Storage for Green Grid”; Chem. Rev. 2011, 111(5), 3577–3613.

[12] David, G.; Reuben, C.; Martin, G. “Solar Energy Conversion Toward 1 Terawatt”; Harnessing Materials for Energy MRS Bulletin 2008, 33(4) 355-364.

[13] Ministry of Energy. “General Terms and Conditions for General Purposes”; Approved by the Ministry of Energy 2017 (In Persian).

[14] Dooner, M.; Clarke, J.; Xing, L. “Overview of Current Development in Electrical Energy Storage Technologies and the Application Potential in Power System Operation”; Appl. Energy 2015, 137, 511-536.

[15] Anindita, R.; Shireesh, B. K.; Santanu B. “Optimum Sizing of Wind-Battery Systems Incorporating Resource Uncertainty”, Appl. Energy 2010, 87(8), 2712-2727.

[16] Abbaspour, M.; Satkin, M.; Mohammadi-Ivatloo, F.; Hoseinzadeh L.; Noorollahi, Y. “Optimal Operation Scheduling of Wind Power Integrated with Compressed Air”; Renew. Energ. 2013, 51, 53-59

[17] Zakeri, B.; Syri, S. “Electrical Energy Storage Systems a Comparative Life Cycle Cost Analysis”; Renew. Sust. Energ. Rev. 2015, 42, 569-596.

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۴۳۷-۴۲۹

«علمی- پژوهش»

کاهش هشدارهای سامانه‌های تشخیص نفوذ به کمک تعمیم ویژگی‌های حملات در حوزه داده‌کاوی چندبعدی

مهدی ملکی[۱*]، محمد لطفی[۲]

۱- استادیار، ۲- مربی، دانشگاه آیت ا... بروجردی

(دریافت: ۹۸/۱۲/۱۵، پذیرش: ۹۹/۰۵/۲۹)

چکیده

امروزه حجم حملات پیشرفته سایبری در حال افزایش است، لذا استفاده از سامانه‌های تشخیص نفوذ در شبکه‌ها امری اجتناب‌ناپذیر است. یکی از مشکلات عمده در استفاده این سامانه‌ها حجم زیاد هشدارهای تولیدشده سطح پایین است. در این مقاله یکی از روش‌های حوزه داده‌کاوی به نام استنتاج ویژگی محور، استفاده شده است. اساس این روش تعمیم داده‌های سطح پایین به مفاهیم سطح بالاست. با توسعه این راهبرد در حوزه حملات سایبری، حجم هشدارهای حسگرهای تشخیص نفوذ کاهش داده شده است. این کاهش نه‌تنها باعث اختلال در شناسایی حملات نمی‌شود بلکه با تمرکز بیشتر در ویژگی‌های مشترک حملات باعث افزایش دقت در تشخیص حملات خواهد شد. همچنین یکی از پایه‌های اساسی این روش، سلسله‌مراتب تعمیم است که برای ویژگی‌های مؤثر در حملات طراحی شده است. از نکات بارز دیگر این مقاله، ارائه یک روش شهودی مناسب در انتخاب ویژگی‌ها برای تعمیم است. برای ارزیابی روش پیشنهادی از مجموعه داده جدید CICIDS2017 استفاده شده است که کاستی‌های مجموعه داده‌های قبل خود را مرتفع نموده است. نتایج بیانگر کاهش هشدارها با نرخ ۹۹ درصد در پایین‌ترین سطح تعمیم و میانگین ۲۵ ٪ در سطوح دیگر تعمیم است. در کنار ترافیک نرمال ۱۴ نوع حمله مختلف شناسایی شده است که حمله Dos Hulk با فراوانی ۸,۱۶٪ بیشترین فراوانی و حمله Heartbleed با فراوانی ۰/۰۰۰۴٪ کمترین فراوانی را دارا بوده‌اند. از دیگر قابلیت‌های ارائه‌شده در روش پیشنهادی، امکان عملیات پردازش تحلیلی برخط و داده‌کاوی چندبعدی در فضای حملات سایبری به کمک حرکت در سطوح مختلف تعمیم است.

کلیدواژه‌ها: سامانه تشخیص نفوذ، تعمیم ویژگی‌ها، داده‌کاوی چندبعدی، پردازش تحلیلی برخط، حملات چندمرحله‌ای

The Reduction of Intrusion Detection Systems Alerts by Generalizing Attack Features in Multidimensional Data Mining Domain

M. Maleki*, M. Lotfi
Ayatollah Boroujerdi University
(Received: 05/03/2020; Accepted: 10/08/2020)

Abstract

The volume of advanced cyber attacks is increasing today; hence the use of intrusion detection systems in networks is inevitable. One of the major problems by using these systems are considered as the high volume of low-level alarms produced. In the present paper, one of the data mining techniques called Attribute-Oriented Induction is utilized. The basis of this approach is to generalize low-level data to high-level concepts. By the development of this strategy in the field of cyber attacks, the volume of intrusion detection alarms has been decreased. This reduction not only disrupts the detection of attacks but by more focusing on the common features of the attacks, it will increase the accuracy of detection. Moreover, one of the basic foundations of this method is a generalized hierarchy designed for effective attack features. Another highlight of this investigation is to provide an intuitive approach to selecting features for generalization. The new CICIDS2017 data set was employed to evaluate the proposed method, which overcame the shortcomings of its previous data set. In conclusion, the results show a 99% decrease in alarms at the lowest generalization level and an average of 25% at the other generalization levels. In addition to the normal traffic, 14 different attack types were identified, with the Dos Hulk attack being the most frequent with 8.16% and the Heartbleed attack having the lowest frequency 0.0004%. Other capabilities were offered in the proposed method include the possibility of online analytical processing and multidimensional data mining in cyber attack space by moving at different levels of generalization..

Keywords: Intrusion Detection System, Feature Generalization, Multidimensional Data Mining, OLAP, Multistage Attacks

*Corresponding Author E-mail: mahdi.maleki@abru.ac.ir

۱. مقدمه

امروزه به‌دلیل وابستگی شدید به سامانه‌های ارتباطی و کامپیوتری اثرات حملات سایبری بسیار زیاد است. به همین دلیل استفاده از سامانه‌های دفاعی چون ضد بدافزارها، دیواره‌های آتش و سامانه‌های تشخیص نفوذ[1] غیرقابل‌انکار است. حجم فزاینده ترافیک شبکه‌های کامپیوتری استفاده از چندین مؤلفه دفاعی را در قطعات مختلف شبکه ایجاب نموده است [۱]. افزایش سامانه‌های تشخیص نفوذ مسائل جدیدی را به دنبال دارند که از مهم‌ترین آن‌ها عبارت‌اند از : "مدیریت حجم هشدارهای تولیدشده و کاهش آن به صورتی‌که باعث مخفی شدن حملات نشوند و دوم کشف ارتباط و همبستگی بین هشدارها[2] به‌منظور کشف سناریوی حملات به‌ویژه در نوع حملات پیشرفته چندمرحله‌ای و حملات مخفیانه"[3]. سامانه‌های تشخیص نفوذ همکار[4] برای حل این مسائل ارائه‌شده‌اند [۲ و ۳]. در این سامانه‌ها مؤلفه‌های دفاعی در حوزه‌های اجرایی متفاوت با مشارکت هم هشدارهای لازم را تولید کرده و پس از پردازش و کشف ارتباطات بین هشدارها حملات هماهنگ سایبری مشخص می‌شوند. در کشف وابستگی‌ها این روش‌ها به دودسته تک‌بعدی [۴ و ۵] و چندبعدی [۶ و ۷] تقسیم می‌شوند در روش تک‌بعدی کشف وابستگی‌ها با محور قرار دادن یک ویژگی انجام می‌شود (مانند کشف همه هشدارهایی که از یک آدرس مبدأ تشکیل‌شده‌اند) این روش‌ها ساده می‌باشند اما قدرت تشخیص مناسبی را ارائه نمی‌دهند در مقابل روش‌های چندبعدی با تمرکز بر روی چندین ویژگی از قدرت تشخیص مناسبی برخوردارند ولی در عوض حجم محاسبات بخصوص در ترافیک‌های بالای شبکه بسیار سنگین است. برای مقابله با محاسبات سنگین روش‌های مختلف سعی در تبدیل هشدارهای خام به قالبی دارند که در عین سادگی حالت کلی حملات را حفظ کنند و هشدارهای کاذب را تقلیل دهند. در یک روش از گراف‌هایی با محوریت شبکه‌های نقشینه[5] برای کاهش هشدارها استفاده‌شده است [۸]. در روش دیگر از بین تمام ویژگی‌ها چندین ویژگی(شامل آدرس مبدأ، درگاهی مبدأ، درگاهی مقصد و پروتکل) بنا بر تحلیل و نقش آن‌ها در شناسایی حملات مختلف انتخاب‌شده و گراف(گراف مشبکه[6]) بر اساس ریشه آدرس مبدأ شکل‌گرفته و تعداد الگوهای مختلف در گره-های گراف محاسبه می‌شود سپس با توجه به مقادیر آستانه بخشی از هشدارها حذف می‌گردند [۹]. در رویکردی دیگر از الگوریتم کشف الگوهای تکراری[7] برای پیدا کردن هشدارها با تعداد تکرار مشخص در ویژگی‌ها استفاده شده است. مشکل عمده روش‌های فوق درکاهش هشدارها عدم توجه به ارتباطات منطقی و مفهومی بین ویژگی‌ها است که باعث عدم شفافیت لازم در خروجی این سامانه‌ها و قدرت تصمیم‌گیری کم در تشخیص حملات خواهد شد. یکی از روش‌های تعمیم داده‌ها[8] در داده‌کاوی عبارت‌اند از: "تبدیل داده‌های سطح پایین به مفاهیم سطح بالاتر و حذف ویژگی‌های نامرتبط" . این عمل که به آن شرح مفهوم[9] هم گفته می‌شود، قدرت توصیف و تمایز[10] کلاس‌های مختلف داده را فراهم می‌آورد. این روش مهم در حوزه تعمیم داده‌ها روش استنتاج ویژگی محور[11] است [۱۰-۱۳]. اساس این روش، تعمیم ویژگی‌های با کمک سلسله‌مراتب موجود در بین آن‌ها است. پایگاه‌های داده رابطه‌ای با کمک پرس‌وجوها (توسط زبان‌هایی مانند SQL) داده‌های لازم برای داده‌کاوی را در روش استنتاج ویژگی محور فراهم می‌آورند [۱۴ و ۱۵]. پرس‌وجوهایی با ساختار SQL با هدف داده‌کاوی بر مبنای استنتاج ویژگی محور[12] ایجاد شده است [۱۶]. از استنتاج ویژگی محور در استخراج قوانین [۱۷]، رده‌بندی [۱۸]، خوشه‌بندی [۱۹] و در کشف الگوهای تکراری [۲۰] استفاده شده است. در این مقاله هدف کاهش هشدارهای سطح پایین با استفاده از سلسله‌مراتب موجود در بین ویژگی‌های حملات بوده است. حرکت در سطوح مختلف تعمیم در فضای حملات سایبری دستاورد ویژه این مقاله در کسب دانش در این حوزه هست.

سازمان‌دهی مقاله در ادامه به شرح زیر است:

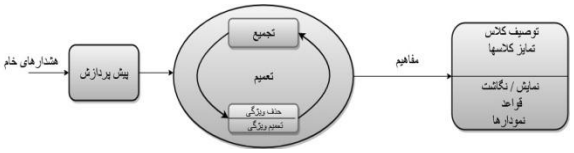
در بخش دو الگوریتم استنتاج ویژگی محور توضیح داده شده است. در ادامه روش پیشنهادی مبتنی بر الگوریتم فوق در حوزه حملات سایبری توسعه داده شده و متناسب با شبکه استفاده‌شده در مجموعه داده پیاده‌سازی شده است. در بخش نتایج، خروجی روش روی مجموعه داده ارائه‌شده نمایش یافته است. همچنین نتایج و قوانین تولیدشده مورد ارزیابی قرارگرفته است.

۲. روش تحقیق

روابط مفهومی بین سلسله‌مراتب موجود بین ویژگی‌ها این امکان را می‌دهد که با استخراج مناسب آن‌ها توصیف بهتر و درنتیجه درک کامل‌تری از هشدارها صورت پذیرد و به‌تبع آن تهدیدهای رخداده کشف شود. لذا از الگوریتم‌هایی در داده‌کاوی استفاده شده است که بتوانند با در نظر گرفتن روابط بین ویژگی‌ها هشدارها را تعمیم داده و حجم هشدارها را با حفظ روابط بین آن‌ها کاهش دهند. در این روش ابتدا داده‌های مرتبط با حوزه خاص توسط پرس‌وجوی مجموعه داده جمع‌آوری می‌شود سپس رکوردهای ناقص در مرحله پیش‌پردازش اصلاح می‌گردند. مرحله

[1] Intrusion Detection Systems (IDS)
[2] Alert Correlation
[3] Stealthy Attack
[4] Collaborative Intrusion Detection Systems (CIDS)
[5] Network Motif
[6] Lattice Graph
[7] Frequent Itemset Mining
[8] Data Generalization
[9] Concept Description
[10] Characterization & Discrimination
[11] Attribute-Oriented Induction
[12] Data Mining Query Language (DMQL)

تعمیم شامل حذف ویژگی[1] یا تعمیم ویژگی[2] است. سپس عمل تجمیع بر روی رکوردهای تکراری انجام شده و خروجی مفاهیم تولید می‌شود (شکل ۱). مفاهیم تولیدشده با نمایش‌ها و نگاشت‌های مختلفی چون نمودارها، قواعد و غیره قابل‌ارائه می‌باشند. در قسمت بعدی الگوریتم اصلی روش ارائه‌شده، توضیح داده‌شده است. همچنین روش پیشنهادی و پیاده‌سازی مؤلفه‌های اساسی آن بیان شده است.



شکل ۱. فرایند کلی روش ارائه‌شده بر مبنای استنتاج ویژگی محور

۲-۱. استنتاج ویژگی محور

این روش که یکی از روش‌های داده‌کاوی محسوب می‌شود مبتنی بر تعمیم داده‌ها با نظر گرفتن سلسله‌مراتب موجود بین ویژگی‌ها است. تعمیم داده از دو قسمت اصلی حذف ویژگی‌ها و تعمیم ویژگی‌ها تشکیل شده است:

حذف ویژگی‌ها: ستون‌هایی که در آن‌ها تعداد حالت‌های مختلف ویژگی‌ها از مقدار آستانه‌ای بیشتر می‌باشند در صورت وقوع یکی از شرایط زیر حذف می‌شوند:

۱. سلسله‌مراتب مفهومی[3] برای آن ستون موجود نباشد
۲. سلسله‌مراتب مفهومی برای این ستون در ستون‌های دیگر موجود باشد.

تعمیم ویژگی‌ها: اگر تعداد حالت‌های مختلف ویژگی‌ها یک ستون از یک مقدار آستانه بیشتر باشد در صورت وجود سلسله‌مراتب مفهومی برای آن ستون، ویژگی‌ها آن ستون تعمیم پیدا می‌کنند.

انتخاب مقادیر آستانه به ویژگی‌ها و حوزه کاربرد وابسته است. این مقادیر توسط فرد خبره و یا کاربر بسته به اینکه کدام ویژگی‌ها بیشتر و کدام کمتر نیاز به تعمیم دارند انتخاب می‌شود. این انتخاب، کنترل تعمیم ویژگی[4] نام دارد. این مقدار طوری تعیین می‌شود که ویژگی‌ها نه بیشتر از حد لازم تعمیم یابند[5] و نه ویژگی‌ها در سطوح پایین قرار بگیرند[6] در هر دو حالت قوانین تولید شده اطلاعات لازم و مفید را تولید نخواهند کرد. روش‌های مختلفی برای تعیین مقادیر آستانه وجود دارد که دو روش مهم عبارت‌اند از:

۱) کنترل آستانه تعمیم ویژگی[7]
۲) کنترل آستانه روابط تعمیم‌یافته[8]

در اولی مقادیر آستانه برای همه ویژگی‌ها و یا تک‌تک ویژگی‌ها تعریف می‌شوند، که در داده‌کاوی این مقادیر معمولاً بین ۲ تا ۸ هستند و مقدار خاص آن توسط خبره یا کاربر انتخاب می‌شود. در روش دوم مقدار آستانه برای تعداد قوانین (خروجی‌های تعمیم‌یافته) انتخاب می‌شود و معمولاً در سامانه‌های داده‌کاوی عددی بین ۱۰ تا ۳۰ هست. به‌عنوان‌مثال اگر بعد از تعمیم تعداد روابط خروجی از مقدار آستانه بیشتر بود تعمیم دوباره روی ویژگی‌ها انجام می‌شود. در الگوریتم ارائه‌شده روش اول استفاده شده است و با توجه به تعداد سطوح سلسله‌مراتب موجود در ویژگی‌ها این مقدار برای ویژگی‌ها آدرس (IP Source, IP Dest) در محدوده ۸ تا ۳ تغییر کرده تا خروجی‌های مختلف تعمیم حاصل شود. برای ویژگی‌ها دیگر به علت سطوح کمتر عدد ۲ انتخاب شده است.

در شکل (۲) سلسله‌مراتب مفهوم برای ویژگی موقعیت به تصویر درآمده است همین‌طور که از شکل مشخص است در تعمیم ویژگی موقعیت، جهت حرکت به‌صورت زیر است:

خیابان › شهر › استان › کشور › همه

شکل ۲. سلسله‌مراتب مفهومی برای ویژگی موقعیت مکانی

الگوریتم استنتاج ویژگی محور از قدم‌های زیر تشکیل شده است:

۱. ویژگی‌ها مرتبط به حوزه کاری از پایگاه داده استخراج می‌شود
۱-۱. در این مرحله مقادیر داده‌های معیوب اصلاح می‌شوند (پیش‌پردازش)
۲. مرحله مقدماتی تعمیم انجام می‌شود:
۲-۱. تعداد حالت‌های مختلف هر ویژگی در ستون‌ها محاسبه می‌شود
۲-۲. عمل حذف یا تعمیم ویژگی انجام می‌گردد و در صورت تعمیم مقدار هر ویژگی با مقدار تعمیم‌یافته جایگزین می‌گردد

[1] Attribute Removal
[2] Attribute Generalization
[3] Concept Hierarchy
[4] Attribute Generalization Control
[5] Overgeneralization
[6] Undergeneralization
[7] Attribute Generalization Threshold Control
[8] Generalized Relation Threshold Control

۳. عمل تعمیم در کل جدول پایگاه داده انجام می‌شود

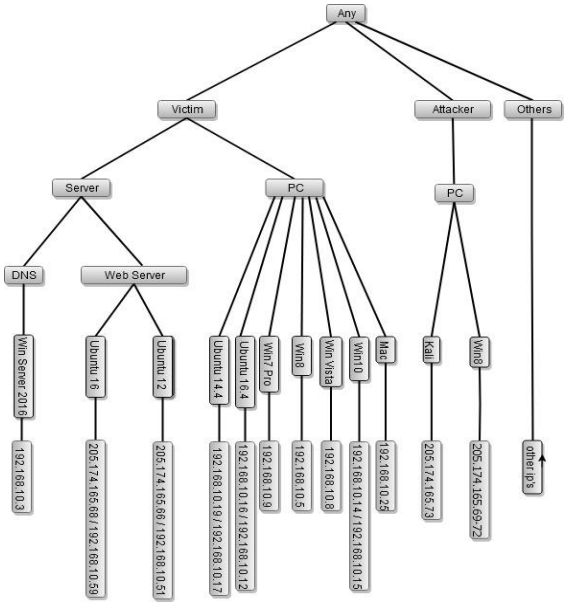
۳-۱. این کار با ادغام رکوردهای تکراری و محاسبه تعداد رکوردهای تکراری انجام می‌شود.

۴. اگر تعداد رکوردهای جدول به میزان موردنظر نرسیده(اطلاعات به میزان موردنظر تعمیم نیافته باشد) مراحل ۲ به بعد تکرار می‌گردند.

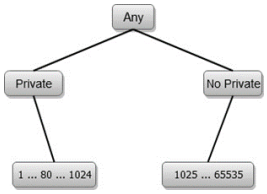
در قسمت بعدی الگوریتم اصلی مطابق با شبکه ارائه‌شده برای تشخیص حمله سایبری توسعه داده شده و همچنین سلسله‌مراتب مفهومی برای ویژگی‌ها موردنظر طراحی خواهد شد همچنین یک روش شهودی برای انتخاب ویژگی‌ها به‌منظور تعمیم تهیه شده است.

۲ -۲. روش پیشنهادی

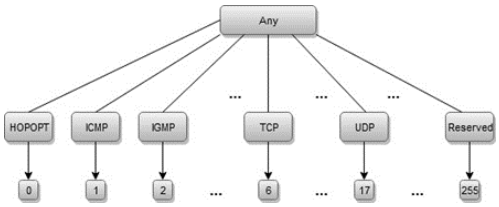
در این قسمت الگوریتم استنتاج ویژگی محور مطابق ضروریات تشخیص حملات سایبری تغییر داده شده است. مطابق مقاله‌ها و گزارش‌های اعلام‌شده در سایت‌های اعلام هشدار آسیب‌پذیری ویژگی‌ها ضروری برای تشخیص حملات عبارت‌اند از: "آدرس IP مبدأ، آدرس IP مقصد، درگاهی مبدأ، درگاهی مقصد و پروتکل" [۲۸-۲۱]. علاوه بر این ویژگی‌ها، ویژگی شمارش[1] و برچسب[2] نیز به داده‌ها اضافه شده است. ویژگی شمارش که با مقدار اولیه ۱ برای هر هشدار ایجاد می‌شود در فرآیند تعمیم افزایش یافته و به‌عنوان معیاری برای اندازه‌گیری اهمیت هشدار برای تصمیم‌گیرنده قابل‌استفاده است. ضمناً با کمک فیلد برچسب خروجی هشدارهای تعمیم‌یافته برحسب ترافیک عادی و ترافیک حملات(انواع حملات) قابل دسته‌بندی خواهند بود. بعد از استخراج اولیه داده‌ها برحسب ویژگی‌های بیان‌شده پیش‌پردازش اولیه‌ای روی‌داده‌ها انجام می‌شود، مثلاً رکوردهای ناقص حذف می‌شوند و یا بعضی از ویژگی‌ها (ویژگی شمارش) مقدار می‌گیرند. یکی از پایه‌های اصلی الگوریتم ارائه‌شده تولید ساختارهای لازم برای سلسله‌مراتب مفهوم برای ویژگی‌هایی است که چنین روابطی را دارا می‌باشند. طراحی چنین ساختارهایی که توسط خبرگان ایجاد می‌شوند بسیار به شبکه هدف مرتبط می‌باشند. این ساختارها به‌عنوان دانش پیش‌زمینه[3]، الگوریتم را در فرآیند تعمیم هدایت می‌کنند. در شکل‌های (۵-۳) ساختارهای درختی برای سلسله‌مراتب مفهوم برای آدرس‌های IP ، شماره درگاهی و پروتکل نمایش داده‌شده‌اند. این ساختارها مطابق شبکه هدف شکل (۶) طراحی شده‌اند که از شبکه هدف مجموعه داده CICIDS2017 اقتباس شده است [۲۹].



شکل ۳. سلسله‌مراتب مفهومی برای آدرس‌های IP



شکل ۴. سلسله‌مراتب مفهومی برای درگاهی



شکل ۵. سلسله‌مراتب مفهومی برای پروتکل

در ادامه الگوریتم پیشنهادی برای تعمیم هشدارهای سایبری که مبتنی بر روش استنتاج ویژگی محور است بیان شده است:

ورودی‌ها: مجموعه داده حملات D(r)، مقادیر آستانه (α) ، و سلسله‌مراتب مفهوم برای هر ستون G(c)

خروجی‌ها: GR(r)(Generalized Relation) روابط تعمیم‌یافته

الگوریتم:

۱) پیش‌پردازش D(r) برای حذف یا اصلاح ستون‌ها و فیلدهای لازم: W ← Preproccessing(D(r))

ستون‌های (IP+PORT+PROTOCOL) برای مرحله بعد انتخاب می‌گردند.

[1] Count
[2] Label
[3] Background Knowledge

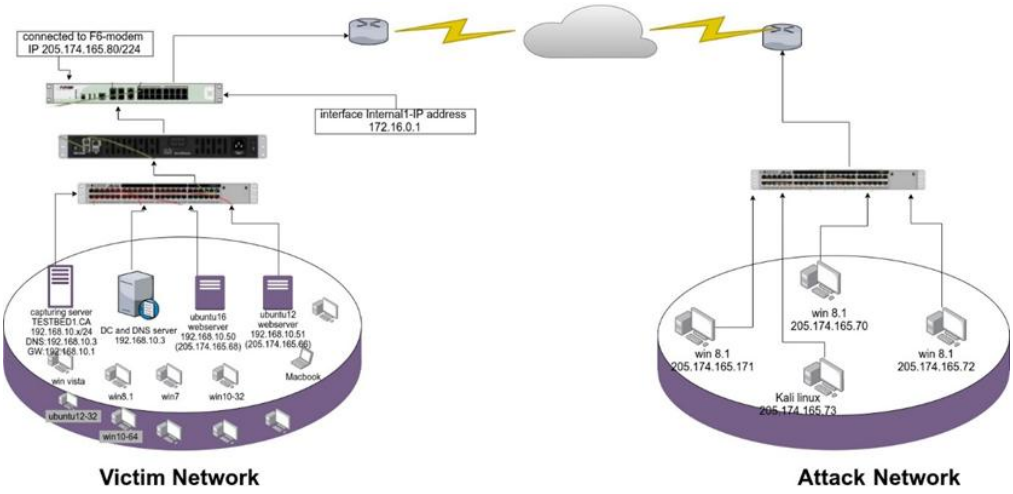
۲) اگر ویژگی قبلاً تعمیم نیافته باشد، برای تعمیم انتخاب می‌شود وگرنه انتخاب یک ویژگی برای تعمیم بر اساس بیشترین مقدار تابع شهودی H(c) است.

۳) تعمیم ویژگی‌ها ستون انتخاب‌شده در مرحله ۲: $W \leftarrow Genralization(W(c))$

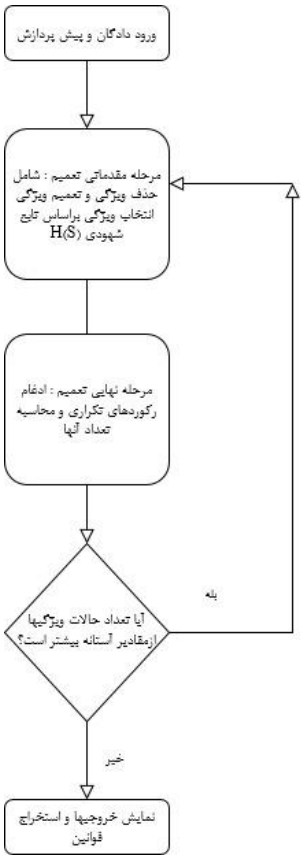
۴) تجمیع رکوردهای تکراری و مقداردهی در مجموعه داده جدید W : $W \leftarrow Aggregation(W)$

۵) اگر تعداد حالت‌های مختلف ویژگی‌ها و یا روابط تعمیم‌یافته از مقادیر آستانه α بیشتر است مراحل ۲ تا ۵ تکرار گردد در غیر این صورت $W \leftarrow GR(r)$

در روابط فوق r ردیف‌ها و c ستون‌ها است شکل (۷).



شکل ۶. ساختار شبکه مورد آزمایش، ویرایش شده از منبع [۲۹]



شکل ۷. فلوچارت پیشنهادی برای تعمیم هشدارهای سایبری مبتنی بر روش استنتاج ویژگی محور

۲-۲-۱. تابع شهودی H(c)

با بررسی و تحلیل هشدارهای سایبری و همچنین استخراج روابط موجود بین ویژگی‌ها اصلی هشدارها مانند آنچه در درخت‌های سلسله‌مراتب مفهومی نمایان شد متوجه می‌شویم سطوح سلسله‌مراتب در تمام ویژگی‌ها به‌طور یکسان تنظیم نشده است، مثلاً سلسله‌مراتب برای ستون آدرس‌های IP دارای بیشترین سلسله‌مراتب (سطح ۶) درحالی‌که سلسله‌مراتب برای ستون‌های درگاهی و پروتکل کمترین(سطح ۳) مقدار رادارند. لذا برای آنکه مقادیر تعمیم‌یافته شفافیت لازم را داشته باشند باید تعمیم را از ستون‌های IP شروع کنیم در غیر این صورت ستون‌هایی با سطح کمتر سریعاً به مقدار همه[1] تعمیم می‌یابند در حالی‌که ستون‌های با سطح بیشتر در مقادیر میانی قرار می‌گیرند و این در تابع شهودی حل شده است:

$$H(c)=MAX(Depth(H(c_i))) \quad (۱)$$

تابع Depth عمق درخت H(c) را می‌دهد و منظور از متغیر c_i ستون i ام یا ویژگی i ام است.

[1] Any

۳. نتایج و بحث

برای ارزیابی روش ارائه‌شده از مجموعه داده جدید CICIDS2017 استفاده شده است. مزایای این مجموعه داده رایگان نسبت به مجموعه داده‌های متداول DARPA، KDD'99، DEFCON، CAIDA و CDX حل مشکلاتی است که عبارت‌اند از[۳۰ تا ۳۴]: "عدم تناسب لازم بین کمیت حملات و کمیت ترافیک نرمال، دارا بودن بسته‌هایی با ویژگی‌های عمداً مخفی‌شده و نامشخص[1] که تحلیل حملات را با مشکل مواجه می‌کنند، محدودیت در انواع حملات بخصوص حملات جدید و عدم وجود مجموعه کاملی از ویژگی‌ها و ابر داده‌ها[2]. شبکه استفاده‌شده در این آزمایش مطابق شکل (۶) است که از دو قسمت اصلی شبکه قربانی و شبکه حمله تشکیل شده است. برای پیاده‌سازی طرح از زبان برنامه‌نویسی پایتون و کتابخانه pandas استفاده شده است[۳۵]. همچنین برای پیاده‌سازی درخت‌های سلسله‌مراتب از کتابخانه anytree بهره برده شده است [۳۶]. در شکل (۸) ساختار درختی پیاده‌سازی شده با ماژول anytree در پایتون نمایش داده شده است. این شکل درواقع پیاده‌سازی شکل (۳) به کمک ماژول فوق است. در جدول (۱) هشدارهای خروجی برنامه در سطوح مختلف تعمیم برای ۵ رکورد اول با بیشترین تکرار نمایش داده شده است. سطوح مختلف تعمیم[3] از GL0 بدون تعمیم تا GL5 بیشترین تعمیم انجام‌شده است. تعمیم بیشتر از این سطح اطلاعات جدیدی تولید نخواهد کرد. در خروجی GL0 اطلاعات با جزئیات زیاد موجود است حجم زیاد هشدارها (حدود ۲۸۳۰۰۰۰) و مقادیر عددی با تنوع زیاد تصمیم‌گیری سریع و مناسب را حتی برای متخصصین با مشکل مواجه می‌نماید درحالی‌که با تعمیم در سطوح بالاتر هم حجم هشدارها کمتر شده و هم تصویر مناسب‌تری از حملات با تعمیم مقادیر عددی به مقادیر حروفی بامعنی به‌دست آمده است. در جدول (۲) میزان کاهش هشدارها در سطوح مختلف نمایش داده شده است، همان‌طور که ملاحظه می‌شود GL1 بیشترین کاهش (۹۹٪) را داشته زیرا که هشدارهای تعمیم نیافته و سطح پائین که تعداد زیادی دارند(با اکثریت ترافیک نرمال) تعمیم‌یافته است در صورتی‌که در سطوح دیگر تعمیم، به‌دلیل آنکه عملیات روی هشدارهای تعمیم‌یافته با تعداد کمتر انجام شده است، نرخ کاهش کمتر است(۲۵٪). در جدول (۳) حملات کشف‌شده و نسبت ترافیک آن‌ها نمایش داده شده است.

[1] Anonymized Packet
[2] Metadata
[3] Generalization Level (GLx)

```
Node('/Any')
├── Node('/Any/Victim')
│   ├── Node('/Any/Victim/Server')
│   │   ├── Node('/Any/Victim/Server/DNS Server')
│   │   │   └── Node('/Any/Victim/Server/DNS Server/Win Server 2016')
│   │   │       └── Node('/Any/Victim/Server/DNS Server/Win Server 2016/192.168.10
│   │   └── Node('/Any/Victim/Server/Web Server')
│   │       ├── Node('/Any/Victim/Server/Web Server/Ubunto 16')
│   │       │   ├── Node('/Any/Victim/Server/Web Server/Ubunto 16/192.168.10.50')
│   │       │   └── Node('/Any/Victim/Server/Web Server/Ubunto 16/205.174.165.68')
│   │       └── Node('/Any/Victim/Server/Web Server/Ubunto 12')
│   │           ├── Node('/Any/Victim/Server/Web Server/Ubunto 12/192.168.10.51')
│   │           └── Node('/Any/Victim/Server/Web Server/Ubunto 12/205.174.165.66')
│   └── Node('/Any/Victim/PC_V')
│       ├── Node('/Any/Victim/PC_V/MAC')
│       │   └── Node('/Any/Victim/PC_V/MAC/192.168.10.25')
│       ├── Node('/Any/Victim/PC_V/Win 10')
│       │   ├── Node('/Any/Victim/PC_V/Win 10/192.168.10.14')
│       │   └── Node('/Any/Victim/PC_V/Win 10/192.168.10.15')
│       ├── Node('/Any/Victim/PC_V/Win Vista')
│       │   └── Node('/Any/Victim/PC_V/Win Vista/192.168.10.8')
│       ├── Node('/Any/Victim/PC_V/Win 8_V')
│       │   └── Node('/Any/Victim/PC_V/Win 8_V/192.168.10.5')
│       ├── Node('/Any/Victim/PC_V/Win 7pro')
│       │   └── Node('/Any/Victim/PC_V/Win 7pro/192.168.10.9')
│       ├── Node('/Any/Victim/PC_V/Ubunto 16.4')
│       │   ├── Node('/Any/Victim/PC_V/Ubunto 16.4/192.168.10.16')
│       │   └── Node('/Any/Victim/PC_V/Ubunto 16.4/192.168.10.12')
│       └── Node('/Any/Victim/PC_V/Ubunto 14.4')
│           ├── Node('/Any/Victim/PC_V/Ubunto 14.4/192.168.10.19')
│           └── Node('/Any/Victim/PC_V/Ubunto 14.4/192.168.10.17')
└── Node('/Any/Attacker')
    └── Node('/Any/Attacker/PC_A')
        ├── Node('/Any/Attacker/PC_A/Kali')
        │   └── Node('/Any/Attacker/PC_A/Kali/205.174.165.73')
        └── Node('/Any/Attacker/PC_A/Win 8_A')
            ├── Node('/Any/Attacker/PC_A/Win 8_A/205.174.165.69')
            ├── Node('/Any/Attacker/PC_A/Win 8_A/205.174.165.70')
            └── Node('/Any/Attacker/PC_A/Win 8_A/205.174.165.71')
```

شکل ۸. ساختار درختی سلسله‌مراتب آدرس پیاده‌سازی شده با ماژول anytree

جدول ۱. پنج رکورد اول در سطوح مختلف تعمیم از GL0 تاGL5

GL0: Generalization Level #0						
Source IP	Source Port	Destination IP	Destination Port	Protocol	Label	count
192.168.10.17	123	198.206.133.14	123	17	BENIGN	1
192.168.10.51	59108	162.213.33.50	443	6	BENIGN	1
192.168.10.51	59108	162.213.33.50	443	6	BENIGN	1
192.168.10.15	54012	205.174.165.73	8080	6	Bot	1
192.168.10.25	123	17.253.14.125	123	17	BENIGN	1
GL1: Generalization Level #1 (IP+PORT+PROTOCOL)						
Source IP	Source Port	Destination IP	Destination Port	Protocol	Label	count
Win Server 2016	No Private	Others	Private	UDP	BENIGN	295361
Others	No Private	Ubunto 16	Private	TCP	DoS Hulk	231073
Win 10	No Private	Win Server 2016	Private	UDP	BENIGN	144503
Win 10	No Private	Others	Private	TCP	BENIGN	135772
Ubunto 16.4	No Private	Others	Private	TCP	BENIGN	134845
GL2: Generalization Level #2 (IP)						
Source IP	Source Port	Destination IP	Destination Port	Protocol	Label	count
PC_V	No Private	Any	Private	TCP	BENIGN	692429
PC_V	No Private	DNS Server	Private	UDP	BENIGN	633037
Any	Private	PC_V	No Private	TCP	BENIGN	343405
DNS Server	No Private	Any	Private	UDP	BENIGN	295361
Any	No Private	Web Server	Private	TCP	DoS Hulk	231073
GL3: Generalization Level #3 (IP)						
Source IP	Source Port	Destination IP	Destination Port	Protocol	Label	count
Victim	No Private	Any	Private	TCP	BENIGN	692429
Victim	No Private	Server	Private	UDP	BENIGN	650963
Server	No Private	Any	Private	TCP	BENIGN	346649
Any	Private	Victim	No Private	UDP	BENIGN	343405
Any	No Private	Server	Private	TCP	DoS Hulk	231073
GL4: Generalization Level #4 (IP)						
Source IP	Source Port	Destination IP	Destination Port	Protocol	Label	count
Any	No Private	Any	Private	TCP	BENIGN	702616
Any	No Private	Victim	Private	UDP	BENIGN	651252
Victim	No Private	Any	Private	TCP	BENIGN	346800
Any	Private	Any	No Private	UDP	BENIGN	344348
Any	No Private	Victim	Private	TCP	DoS Hulk	231073
GL5: Generalization Level #5 (IP)						
Source IP	Source Port	Destination IP	Destination Port	Protocol	Label	count
Any	No Private	Any	Private	UDP	BENIGN	1746444
Any	Private	Any	No Private	TCP	BENIGN	417942
Any	No Private	Any	Private	TCP	DoS Hulk	231073
Any	No Private	Any	No Private	TCP	PortScan	133891
Any	No Private	Any	Private	TCP	DDoS	128024

جدول ۲. نرخ کاهش هشدارها در سطوح مختلف تعمیم

سطح عملیات تعمیم	تعداد هشدارها	نرخ کاهش هشدارها
GL0 (IP+PORT+PROTOCOL)	۲۸۳۰۳۶۵	۰,۰%
GL 1 (IP)	۲۲۸	۹۹/۹۹%
GL 2 (IP)	۶۸	۷۰/۱۸%
GL 3 (IP)	۵۱	۲۵/۰۰%
GL 4 (IP)	۳۲	۳۷/۲۵%
GL 5 (IP)	۲۰	۳۷/۵۰%

جدول ۳. نسبت تعداد هشدارها در ترافیک نرمال و حملات

حملات	تعداد هشدارها	درصد
BENIGN	۲۲۷۳۰۹۷	۸۰/۳۰%
DoS Hulk	۲۳۱۰۷۳	۸/۱۶%
PortScan	۱۵۸۹۳۰	۵/۶۱%
DDoS	۱۲۸۰۲۷	۴/۵۲%
DoS GoldenEye	۱۰۲۹۳	۰/۳۶%
FTP-Patator	۷۹۳۸	۰/۲۸%
SSH-Patator	۵۸۹۷	۰/۲۱%
DoS slowloris	۵۷۹۶	۰/۲۰%
DoS Slowhttptest	۵۴۹۹	۰/۱۹%
Bot	۱۹۶۶	۰/۰۷%
Web Attack – Brute Force	۱۵۰۷	۰/۰۵%
Web Attack – XSS	۶۵۲	۰/۰۲%
Infiltration	۳۶	۰/۰۰%
Web Attack – Sql Injection	۲۱	۰/۰۰%
Heartbleed	۱۱	۰/۰۰%
مجموع	۲۸۳۰۳۶۵	

کمیت‌های محاسبه‌شده از روابط (۲ و ۳) به‌دست‌آمده‌اند:

$$f_i = \frac{f}{n} \times 100 \qquad (۲)$$

در رابطه فوق f_i درصد فراوانی هشدارهای حملات نوع i و f تعداد هشدارهای حملات نوع i و n تعداد کل هشدارها است.

$$R_i = \frac{A_{i-1} - A_i}{A_{i-1}} \times 100 \qquad (۳)$$

در رابطه فوق A_{i-1} تعداد هشدارها در سطح i-1 تعمیم و A_i تعداد هشدارها در سطح i و R_i درصد کاهش هشدارها در تعمیم از GL_{i-1} به GL_i

چند استنتاج از خروجی‌های برنامه به‌صورت زیر است:

۱) در کنار هشدارهای نرمال[1] ۱۴ نوع حمله مختلف انجام شده است که با توجه به جدول (۳) حمله Dos Hulk با فراوانی ۸,۱۶ ٪ بیشترین فراوانی و حمله Heartbleed با فراوانی ۰/۰۰۰۴ ٪ کمترین فراوانی را در بین حملات دارا می‌باشند.

۲) از خروجی‌های GL0 مشخص است که حمله‌ای از نوع Bot از آدرس ۱۹۲,۱۶۸,۱۰,۱۵ از شماره درگاهی ۵۴۰۱۲ به آدرس ۲۰۵,۱۷۴,۱۶۵,۷۳ به شماره درگاهی ۸۰۸۰ با پروتکل شماره ۶ و تعداد یک انجام شده است. همان‌طور که مشاهده می‌شود داده‌های سطح پایین با تکرار کم امکان تصمیم‌گیری مناسب در مورد میزان اهمیت حملات را مهیا نمی‌سازند.

۳) با انجام سازوکار تعمیم و مراجعه به سطح بعدی سلسله مراتب GL1 مشخص می‌شود که حدود ۲۳۱۰۰۰ هشدار از نوع حمله DOS Hulk به مقصدی با سیستم‌عامل Ubunto16 با درگاهی مقصد خصوصی انجام پذیرفته است. تعداد زیاد هشدارها در این مورد و تعمیم هشدارهای سطح پایین در این مرحله مدیر شبکه را در تصمیم‌گیری درباره اهمیت این هشدارها و اقدامات لازم برای مقابله توانا خواهد ساخت.

۴) با مراجعه به سطوح بالاتر تعمیم (GL2-GL5) دید بالاتری از هشدارها و کشف روند موجود بین هشدارها به‌دست خواهد به‌عنوان‌مثال در آخرین مرحله تعمیم انجام‌شده سه نوع حمله DOS Hulk، Port Scan و DDos از فراوانی بیشتری در بین حملات برخوردار بوده‌اند با حرکت رو به عقب در تعمیم می‌توان اطلاعات با جزئیات بیشتری را کسب کرد مثلاً بیشتر حملات DDos به Web Server حمله کرده‌اند.

حرکت در سطوح مختلف تعمیم، امکان حرکت روبه‌جلو و عقب[2] در هشدارها را فراهم می‌آورد که از ابزارهای اصلی عملیات پردازش تحلیلی برخط[3] و داده‌کاوی چندبعدی[4] هست.

۴. نتیجه‌گیری

در این مقاله از یک روش مؤثر تعمیم داده‌ها از حوزه داده‌کاوی به نام استنتاج ویژگی محور استفاده‌شده است و اقدام به توسعه و پیاده‌سازی آن به‌منظور کشف حملات سایبری در شبکه هدف مطابق با مجموعه داده CICIDS2017 شده است. برای این منظور در ابتدا سطوح سلسله‌مراتب برای ویژگی‌ها مهم در شناسایی حملات طراحی‌شده‌اند، سپس یک روش شهودی برای انتخاب ویژگی برای عمل تعمیم ارائه شده است. نتایج بیانگر تعمیم مناسب(۹۹ ٪ در سطح ۱ و حداقل ۲۵٪ در سطوح دیگر تعمیم) هشدارهای تولیدشده در سامانه‌های تشخیص نفوذ به‌منظور کشف و تمایز با دقت حملات است. در کنار ترافیک نرمال ۱۴

[1] Benign

[2] Roll-Up & Drill-Down
[3] OLAP
[4] Multidimensional data mining

نوع حمله مختلف شناسایی شد که حملـه Dos Hulk بـا فراوانـی ۸/۱۶٪ بیشـترین و حملـه Heartbleed بـا فراوانـی ۰/۰۰۰۴٪ کمترین را دارا می‌باشند. همچنین با کمک خروجی‌های مختلف تعمیم امکان حرکت روبه‌جلو و عقب در سطوح مختلف هشـدارها کـه لازمـه تحلیـل مناسـب در داده‌کـاوی چندبعـدی در حـوزه تشخیص حملات سایبری است فراهم شده است. در پژوهش‌های آینده می‌تـوان بـا پیـاده‌سـازی معیارهـایی، کیفیـت هشـدارهای ارائـه‌شـده را در سـطوح مختلـف بـرای کـاربر محاسـبه کـرد و هشدارهای کاذب و واقعی را با مقادیر احتمالی محاسبه کرد. ایـن کار نیازمند بررسی دقیق‌تر ویژگـی‌هـای مـؤثر دیگـر در حمـلات سایبری دربسته‌های شبکه است. همچنین طراحی سازوکارهایی برای تشخیص حملات مخفیانه مفید اسـت. حملاتـی کـه باعـث تولید هشدارهای کم ولی اثرات تخریبی زیاد می‌شوند.

۵. مرجع‌ها

[1] Emmanouil, V.; Shankar, K.; Max, M.; Mathias, F. “Taxonomy and Survey of Collaborative Intrusion Detection”; ACM Computing Surveys (CSUR) 4, 2015.

[2] Min, C.; Kai, H.; Yu-Kwong, K.; Shanshan, S.; Yu, C. “Collaborative Internet Worm Containment”; IEEE Security & Privacy 3, 2005.

[3] Carlos, G., C.; Sascha, H.; Max, M.; Mathias, F. “Analyzing Flow-based Anomaly Intrusion Detection using Replicator Neural Networks”; In Annual Conference on Privacy, Security and Trust (PST), 2016.

[4] Onwubiko, C. “Situational Awareness in Computer Network Defense: Principles, Methods and Applications “; IGI Global, 2012.

[5] Estan, C; Savage, S; Varghese, G. “Automatically Iinferring Patterns of Resource Consumption in Network Traffic”; In: Proceedings of the conference on applications, technologies, architectures, and protocols for computer communications (SIGCOMM), 2003.

[6] Locasto, M.; Parekh, J.; Keromytis, A.; Stolfo, S. “Towards Collaborative Security and P2P Intrusion Detection”; In: Proceedings of the IEEE workshop on information assurance and security, 2005.

[7] Najafi, M.; Rafeh, R. “A New Light Weight Intrusion Detection Algorithm for Computer Networks”; Advanced Defence Sci. & Tech. 2016, 8, 191-200 (In Persian).

[8] Steffen, H.; Mathias, F. “GAC: Graph-Based Alert Correlation for the Detection of Distributed Multi-Step Attacks”; In ACM/SIGAPP Symposium On Applied Computing (SAC), 2018.

[9] Chenfeng, V. Z.; Christopher L.; Shanika, K. “Decentralized Multi-dimensional Alert Correlation for Collaborative Iintrusion Detection”, Volume 32, Issue 5, September 2009.

[10] Han, J.; Micheline, K.; Jian, P. “Data Mining Concepts and Techniques”; the Morgan Kaufmann Series in Data Management Systems, 2011.

[11] Beneditto, M. “Using Concept Hierarchies in Knowledge Discovery”. Lecture Notes in Computer Science, 2004.

[12] Han, J.; Fu, Y. “Exploration of the Power of Attribute-Oriented Induction in Data Mining”; in U. Fayyad, G. Piatetsky-Shapiro, P. Smyth and R. Uthurusamy, eds. Advances in Knowledge Discovery and Data Mining, 399-421, 1995.

[13] Han, J.; Cai, Y.; Cercone, N. “Knowledge Discovery in Databases: an Attribute-oriented Approach”; In Proceedings of the 18th International Conference on Very Large Data Bases, 547-559, 1992.

[14] Meo, R.; Psaila, G.; Ceri, S. “An Extension to SQL for Mining Association Rules”; In Proceedings of Data Mining and Knowledge Discovery; 1998, 2,195-224.

[15] Muyeba, M.; Marnadapali, R. “A framework for Post-Rule Mining of Distributed Rules Bases”; In Proceeding of Intelligent Systems and Control; 2005.

[16] Elfeky, M.G.; Saad, A.; Fouad, S.A. “ODMQL: Object Data Mining Query Language”; In Proceedings of the International Symposium on Objects and Databases, 2000, 128-140.

[17] Cheung, D.W.; Hwang, H.; Fu, A.W. “Efficient Rule-Based Attribute-Oriented Induction for Data Mining”; Journal of Intelligent Information Systems, 2000, 15, 175–200.

[18] Cai, Y.; Cercone, N.; Han, J. “An attribute-oriented Approach for Learning Classification Rules from Relational Databases”; InProceedings. Sixth International Conference on Data Engineering IEEE, 1990, 281-288.

[19] WU, X.; XIE, L. “Attribute-oriented Induction and Conceptual Clustering”; Computer Engineering, Beijing, 2003, 92-99.

[20] Warnars, H. “Using Attribute Oriented Induction High level Emerging Pattern (AOI-HEP) to mine frequent patterns”; International Journal of Electrical and Computer Engineering (IJECE). 2016 Dec, 3037-46.

[21] Chenfeng, V. Z.; Christopher, L.; Shanika, K. “a Survey of Coordinated Attacks and Collaborative Intrusion Detection”; Computers & Security, 2010.

[22] Estan, C.; Savage, S.; Varghese, G.”Automatically Inferring Patterns of Resource Consumption in Network Traffic”; In: Proceedings of the conference on applications, technologies, architectures, and protocols for computer communications (SIGCOMM), 2003. 137–48.

[23] Haas, S.; Florian, W.; Mathias, F. "Efficient Attack Correlation and Identification of Attack Scenarios based on Network-Motifs." arXiv preprint arXiv: 1905.06685, 2019.

[24] ICS-CERT Advisories, Information about Current Security issues, Vulnerabilities, and Exploits. Available: https://www.us-cert.gov/ics/advisories, 2019.

[25] The National Institute of Standards and Technology (NIST) ,National Vulnerability Database, Available: https://nvd.nist.gov/vuln, 2019.

[26] Internet Storm Center, DShield.org. Available: http://www.dshield.orgi, 2019.

[27] Hu, Y.; Chiu, D.; Lui, J. “Adaptive Flow Aggregation—a New Solution for Robust Flow Monitoring under Security Attacks”; In: Proceedings of the 10th IEEE/IFIP network operations and management symposium (NOMS); 2006, 424–35.

[28] Taheri, R.; Parsaei, M.; Javidan, R. “Real-Time Intrusion Detection System Using a Combination of Discretization and Feature Selection”; Advanced Defence Sci. & Tech. 2017, 8, 251-263 (In Persian).

[29] Sharafaldin, I.; Habibi, A.; Lashkari; Ghorbani, A. “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on

Information Systems Security and Privacy (ICISSP), Portugal, January 2018.

[30] Thomas, C.; Vishwas, S.; Balakrishnan N. "Usefulness of DARPA Aataset for Intrusion Detection System Evaluation"; Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008. Vol. 6973. International Society for Optics and Photonics, 2008.

[31] Cup, K. D. D. "Intrusion Detection Data Set." The UCI KDD Archive Information and Computer Science University of California, Irvine. DOI= http://kdd. ics. uci.Edu/databases/kddcup99, 1999.

[32] Cowan, C. "Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack"; Proceedings DARPA Information Survivability Conference and Exposition, IEEE, 2003, 1.

[33] CAIDA: Center for Applied Internet Data Analysis, Available: https://www.caida.org, 2019.

[34] CDX 2009 DataSet, Available: https://www.usma.edu/centers-and-research/cyber-research-center/data-sets, 2019.

[35] McKinney, W. "Pandas: a Foundational Python Library for Data Analysis and Statistics. "Python for High Performance and Scientific Computing 14.9, 2011.

[36] Anytree 2.7.3 Documentation, Available: https://anytree.readthedocs.io/en/latest/intro.html, 2019.

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۴۵۰-۴۳۹

«علمی- پژوهش»

بهبود احراز هویت در خانه هوشمند مبتنی بر رمز یکبار مصرف و رمزنگاری منحنی بیضوی

نرگس اسدنجفی[۱]، مهدی ملامطلبی[۲*]

۱- کارشناسی ارشد، ۲-استادیار، گروه کامپیوتر، واحد بوئین زهرا، دانشگاه آزاد اسلامی، بوئین زهرا، ایران

(دریافت: ۹۸/۰۷/۰۴، پذیرش: ۹۸/۱۲/۰۹)

چکیده

در خانه‌های هوشمند، اغلب اشیا با یکدیگر و با افراد خانه، در تعامل هستند. یکی از مزایای خانه هوشمند، امکان کنترل و نظارت بر خانه، از راه دور است. درعین‌حال، خانه هوشمند به‌طور بالقوه در معرض مشکلات امنیتی و نقض حریم خصوصی افراد است. با توجه به این‌که اشیاء درون خانه هوشمند، همواره در حال جمع‌آوری اطلاعات خصوصی از فعالیت‌های افراد هستند، اگر شخصی به اشیاء داخل منزل، به‌طور غیرمجاز دسترسی یابد، اشیا را تحت کنترل خود درآورده و به داده‌های خصوصی افراد دست‌یافته و باعث صدمه زدن به اشیا و یا فاش نمودن اطلاعات می‌نماید. جهت جلوگیری از این امر، افرادی که قصد استفاده از اشیاء داخل منزل را دارند، باید پیش از استفاده، احراز هویت گردند. در این مقاله، روشی برای بهبود احراز هویت افراد، مبتنی بر رمز یکبار مصرف با استفاده از کارت هوشمند و الگوریتم رمزنگاری منحنی بیضوی در سامانه خانه هوشمند، ارائه‌شده است. ارزیابی روش پیشنهادی توسط منطق بن و در محیط نرم‌افزار آویسپا انجام شده است. نتایج ارزیابی‌ها حاکی از بهبود احراز هویت متقابل بین کاربر و گره دروازه جهت مقابله با حملات متداول به خانه هوشمند، در مقایسه با روش‌های موجود است. به‌علاوه، روش پیشنهادی از حملات استراق سمع و حمله سرک‌کشی جلوگیری می‌نماید که اکثر روش‌های موجود، قادر به جلوگیری از آنها نیستند.

کلیدواژه‌ها: احراز هویت، خانه هوشمند، رمز یکبار مصرف، کارت هوشمند، رمزنگاری منحنی بیضوی.

Improving the Authentication in Smart Home Using Cryptography One-Time Password and Elliptic-Curve

N. Asadnajafi, M. Mollamotalebi*
Department of Computer, Buinzahra Branch, Islamic Azad University, Buinzahra, Iran
(Received: 26/09/2019; Accepted: 28/02/2020)

Abstract

In smart homes, most objects interact with each other and with people in the home. One of the advantages of a smart home is the ability to control and monitor the home remotely. At the same time, the smart home is potentially vulnerable to security issues and privacy violance. Given that objects inside the smart home are always collecting private information about people's activities, if someone unauthorizedly accesses objects inside the house, they take control of the objects and give them data. Private property is accessed by individuals and causes damage to objects or disclosure of information. To prevent this, people who intend to use indoor objects must be authenticated before use. In this paper, a method to improve the authentication of individuals, based on one-time password using a smart card and elliptic curve encryption algorithm in the smart home system, is presented. The evaluation of the proposed method is done by Ban Logic and in Avispa environment. The results of the evaluations indicate an improvement in the mutual authentication between the user and the gateway node to deal with common attacks on the smart home, compared to existing methods. In addition, the proposed method prevents eavesdropping attacks and Shoulder surfing attacks that most existing methods are unable to prevent.

Keywords: Authentication, Smart Home, One-Time Password, Smart Card, Elliptic-Curve Cryptography.

*Corresponding Author E-mail: motalebi@qiau.ac.ir

۱. مقدمه

در دنیای مدرن امروز، با پیشرفت علم و فناوری، اشیا هوشمند به‌طور تقریباً نامحسوسی وارد جریان زندگی روزمره افراد شده‌اند. این اشیا می‌توانند پوشیدنی و یا خوردنی بوده و یا از اجزا تشکیل‌دهنده خانه باشند. یک خانه با قطعات هوشمند مرتبط باهم، ممکن است حاوی داده‌های بااهمیتی (نظیر تصاویر و ویدئوهای شخصی که به‌صورت دیجیتالی نگهداری می‌شوند) باشد.

دستگاه‌هایی مانند دوربین‌های باقابلیت اتصال به شبکه که از راه دور کنترل می‌شوند، میکروفون‌های نصب‌شده در منزل که صحبت‌های محرمانه را شنود می‌کنند و بسیاری تجهیزات دیگر، امروزه حریم خصوصی و امنیت افراد را به مخاطره می‌اندازند [۱]. مثلاً، سامانه‌های سخن گوی هوشمند[1] مانند محصول اکو[2] ساخت شرکت آمازون و میکروفون خانگی شرکت گوگل که برنامه‌ریزی‌شده‌اند تا دستور "بیدار شو" را اجرا کنند و بعداز آن دستور، دستوراتی که به‌وسیله صدا به آن‌ها داده می‌شود (کارهایی مثل کم کردن نور یا پخش موسیقی) را می‌شنوند و اجرا می‌کنند [۲]. در بسیاری از موارد، معضلات امنیتی شبکه‌های بی‌سیم یا اقتضایی، به خانه‌های هوشمند نیز تسری می‌یابند [۳].

لذا اشیا هوشمند، اطلاعات گاه ارزشمند و محرمانه‌ای را که مربوط به اعضای خانه (کاربران) است دربردارند که بایستی از دسترسی غیرمجاز، محافظت گردند. ازاین‌رو، موضوع احراز هویت افرادی که مجاز به استفاده از اشیا خانه هوشمند هستند، بحثی حیاتی محسوب می‌شود. صرفاً افراد مجاز می‌توانند قابلیت دسترسی، برنامه‌ریزی و یا فرماندهی به اشیا هوشمند را داشته باشند و دسترسی افراد خرابکار[3] به این اشیاء بایستی مسدود باشد تا از خسارات مالی و گاهی جانی افراد جلوگیری نمود [۴] [۵].

روش‌های مختلفی جهت مقابله با تهدیدهای احراز هویت کاربران خانه هوشمند ارائه‌شده‌اند که هرکدام مزایا و معایبی دارند. با درنظر گرفتن متحرک بودن کاربران و اجازه دسترسی و ورود از مکان‌های مختلف، روش‌های احراز هویت رایج، مانند استفاده از نام کاربری و رمز عبور، به‌تنهایی، ناکارآمد بوده و نیاز به بهبود روش‌های احراز هویت، مشهود است.

در معماری و طراحی‌های فعلی خانه‌های هوشمند، توجه چندانی به مساله امنیت و حریم خصوصی افراد نشده است و درنتیجه، در یک خانه هوشمند با قدرت امنیتی پایین، اطلاعات محرمانه کاربران به راحتی در اختیار افراد ناشناس یا مخرب قرار می‌گیرد [۶]. از طرفی نیز، با توجه به ویژگی ارتباط چند پروتکلی و قابلیت‌های متنوع دستگاه‌ها، راهکارهای امنیتی سنتی برای قطعات خانه هوشمند، کارایی مناسبی ندارند [۲]. روش امنیتی که در خانه‌های هوشمند ارائه می‌شود باید سازگاری بین استانداردهای چندگانه را نیز در نظر داشته باشد.

احراز هویت باید یک روال کلی باشد به این معنی که، کاربر برای دسترسی به سامانه و تک‌تک ابزارهای وابسته به آن، فقط یک‌بار احراز هویت شود، و برای استفاده از هر یک از دستگاه‌های موجود در سامانه، نیازی به احراز هویت مجدد نداشته باشد. علاوه بر آن، این روال باید امنیت سامانه را بالا برده و استفاده از رابط کاربری را به حداقل برساند و همچنین از روش‌های احراز هویت بیومتریک به‌دلیل هزینه‌بر بودن آن‌ها، ترجیحاً استفاده نکند. با توجه به عامل‌ها و نیازهای عنوان‌شده و تحقیقاتی که پیش‌ازاین صورت گرفته است، می‌توان ادعا کرد که استفاده از روش احراز هویت مبتنی بر رمز یکبار مصرف با استفاده از کارت هوشمند و الگوریتم منحنی بیضوی در سامانه خانه هوشمند در تحقیق حاضر، توجیه‌پذیر است.

این مقاله در ادامه، شامل بخش‌های زیر است. بخش دوم به مرور روش‌های مرتبط و نقد و بررسی آن‌ها می‌پردازد. روش پیشنهادی این مقاله در بخش سوم با جزئیات تشریح شده است. در بخش چهارم، نتایج روش پیشنهادی این تحقیق با روش‌های مرتبط اخیر، مقایسه و ارزیابی می‌گردد و بخش پنجم به نتیجه‌گیری این مقاله می‌پردازد.

۲. کارهای مرتبط

اشیا هوشمند موجود در یک خانه هوشمند، با پروتکل‌های مختلفی مانند زیگبی[4]، زِد- ویو[5]، کِی‌اِن‌ایکس[6]، تِرِد[7]، و اِس‌سی‌اس[8] و شیوه‌های ارتباطی گوناگونی نظیر وای‌فای، بلوتوث، آراِف‌آیدی، و اِن‌اف‌سی[9]، با یکدیگر ارتباط برقرار می‌کنند [۷] و گاهی جهت ارتباط، نیازمند استفاده از پل[10]، هاب و دروازه[11] هستند. همچنین ممکن است یک دستگاه از پروتکل اختصاصی به‌منظور ارتباطات محلی (پروتکل بدون استفاده از IP) و از یک

[1] Smart speaker systems
[2] Echo
[3] Intruder

[4] Zig-bee
[5] Z-wave
[6] KNX
[7] Thread
[8] SCS
[9] NFC
[10] Bridge
[11] Gateway

پروتکل استاندارد، برای اتصال به ابر[1]، استفاده کند. این عوامل در کنار محدودیت‌های سخت‌افزاری، باعث شده روش‌های رمزنگاری ضعیفی در خانه‌های هوشمند به کار گرفته شوند [۲]. در ادامه، تحقیقات مرتبط با امنیت و احراز هویت در خانه‌های هوشمند، معرفی می‌شوند.

صالح اصفهانی و همکارانش [۳] یک چارچوب احراز هویت متن- آگاه[2] جهت حفاظت از دستگاه‌های هوشمند در برابر دسترسی‌های غیرمجاز ارائه داده است. در زمان ورود کاربر جدید به سامانه، اطلاعات کاربر، مانند مکان، پروفایل، تقویم برنامه‌ریزی، زمان درخواست و الگوهای رفتاری دسترسی وی، ثبت می‌شود و یک سطح دسترسی معین توسط صاحب‌خانه، برایش ثبت می‌شود. زمانی که کاربر نیاز به دسترسی به خانه هوشمند، از خارج آن داشته باشد، این اطلاعات جهت تصمیم‌گیری در خصوص پذیرش یا رد درخواست کاربر استفاده می‌شوند.

این چارچوب توانایی حفاظت از قطعات خانه هوشمند را در برابر دسترسی غیرمجاز کاربران محلی و راه دور دارد. همچنین بر دسترسی‌ها و فعالیت‌هایی مانند ورود کاربر، درخواست سرویس، و مدت زمان استفاده از خدمت نظارت دارد و این اطلاعات را، در یک پایگاه داده جهت استفاده در آینده، ثبت می‌نماید و می‌تواند جهت مقابله با حمله بروت‌فورس[3] نیز مفید واقع شود. از سوی دیگر، این چارچوب در برابر حمله سرک‌کشی آسیب‌پذیر است به‌طوری‌که اگر شخصی با سرک‌کشیدن، اطلاعات کاربر را به‌دست آورد، به راحتی می‌تواند به‌جای او وارد سامانه شود.

در روش پیشنهادی سانتوس و همکارانش [۴]، احراز هویت کاربران توسط گوشی‌های هوشمند مجهز به صفحه لمسی صورت می‌گیرد. تعداد ۳۰ الگوی رفتاری لمس کردن صفحه گوشی هوشمند توسط کاربر (مثلاً حرکت به راست و چپ یا بالا و پایین) ثبت می‌شود و با بررسی تعاملات کاربر حاضر با صفحه لمسی، نشست کاری وی، حفظ یا حذف می‌گردد. این چارچوب در مقابل حمله سرک‌کشی و جعل هویت کاربر، مقاوم است ولی نمی‌تواند به‌عنوان یک روش مستقل احراز هویت، استفاده شود؛ بلکه باید به‌عنوان بخشی از سامانه احراز هویت چندحالته[4] استفاده شود. همچنین در این چارچوب، همه دستگاه‌های مورد استفاده کاربر، باید مجهز به صفحه لمسی باشند و ممکن است کاربر در استفاده از آن، راحت نباشد و یا متحمل هزینه بیشتر گردد.

جیونگ و همکارانش [۸] روشی جهت احراز هویت با استفاده از رمز یکبار مصرف و کارت هوشمند در شبکه خانه هوشمند، ارائه داده است. این روش به‌دلیل استفاده از تابع چکیده‌سازی یک‌طرفه، بار محاسباتی کمی دارد هرچند که احراز هویت متقابل بین گره دروازه و قطعات هوشمند، کاربر و قطعات هوشمند را ارائه نمی‌دهد. پیام‌ها در آن می‌توانند ردیابی شوند و برای کاربر دور از خانه، مناسب نیست. کاستی دیگر این روش، ناامن بودن در برابر حمله سرک‌کشی و دزدیده شدن کارت هوشمند است. مهاجم می‌تواند بعد از به دست آوردن کارت، به تمام اطلاعات محرمانه کاربر که در آن ذخیره‌شده است، دسترسی یابد. روش ارائه‌شده توسط وایدیا و همکارانش [۹] که در آن، احراز هویت کاربران بر اساس کلمه عبور است نیز، از مشکلات مشابه رنج می‌برد.

سانتوسو و همکارانش [۱۰] روشی مبتنی بر رمزنگاری منحنی بیضوی جهت احراز هویت، ارائه داده است. هویت کاربر توسط دستگاه‌هایی که داخل خانه هوشمند قرار دارند و با یک گره مرکزی دروازه مرتبط هستند، محرز می‌شود. این روش در ناشناس نگاه‌داشتن دستگاه‌ها و به‌تبع آن، کاربر، ناتوان است.

چنگ و همکارانش [۱۱] یک روش احراز هویت دو عاملی برای شبکه‌های حسگر بی سیم با استفاده از کارت هوشمند و رمز عبور ارائه کرده است. در آن، از دو پروتکل استفاده‌شده است؛ پروتکل اول بر اساس تابع چکیده‌سازی و عملگر بیتی یای انحصاری، و پروتکل دوم بر اساس تابع چکیده‌سازی و رمزنگاری منحنی بیضوی و عملگر بیتی یای انحصاری کار می‌کند. این روش، احراز هویت متقابل را تأمین می‌کند ولی در برابر حمله تکرار[5] و حمله فرد میانی[6] مقاوم نیست. پروتکل اول در برابر حمله قفل و کلید در نشست‌ها ناامن است و هر دو پروتکل در برابر حمله حدس رمز عبور، ناامن هستند. جهت از میان بردن محدودیت های این دو پروتکل، روش احراز هویت دیگری توسط داس و همکارانش[۱۲] ارائه‌شده است که از کلید و رمزنگاری منحنی بیضوی استفاده می‌کند هرچند که هیچ تمهیدی برای حمله سرک‌کشی ارائه نمی‌دهد.

وزید و همکارانش [۱۳] یک روش احراز هویت متقابل از راه دور و برقراری ارتباط با کلید ارائه داده است. این روش، احراز هویت متقابل بین کاربر و گره دروازه، اشیا و گره دروازه، و کاربر و

[1] Cloud
[2] Context-aware authentication framework
[3] Brute force
[4] Multi-modal
[5] Replay
[6] Man in the middle

اشیا را اداره می‌کند. نتایج بررسی امنیت این روش با استفاده از ابزار آویسپا و شبیه‌ساز NS2، نشان می‌دهد که در حفظ امنیت خانه هوشمند در برابر حملات متداول، امن است. بااین‌حال، در برابر حمله سرک‌کشی ضعیف است.

کومار و همکارانش [۱۴] روشی بر پایه کلید امن برای خانه هوشمند ارائه داده است. برای ایجاد اعتماد متقابل، واحد کنترل هر دستگاه هوشمند، با استفاده از توکن‌های احراز هویت، یک نشست کلید با گره دروازه برقرار می‌کند. گره دروازه ناشناس نیست و احراز هویت متقابل بین کاربر و قطعات هوشمند، و کاربر و گره دروازه را تأمین نمی‌کند. لی و همکارانش [۱۵] یک روش مبتنی بر رمزنگاری منحنی بیضوی در سامانه مدیریت انرژی خانه هوشمند، معرفی نموده است که ازنظر زمان و حافظه مصرفی، کارایی مناسبی دارد هرچند که برای حمله سرک‌کشی در آن، تدبیری اندیشیده نشده است.

نوی و همکارانش [۱۸] برای جلوگیری از دسترسی غیرقانونی افراد به داده‌های تولید شده توسط اشیا هوشمند، روش کم مصرف[1] احراز هویت بر مبنای پسورد را ارائه نمودند. در این روش امنیت خانه هوشمند بهبود یافته است و میزان مصرف انرژی دستگاه‌های هوشمند کاهش پیدا کرده است اما برای مقابله با حمله سرک کشی راه حلی ارائه نشده است.

منگشیا شوای و همکارانش [۱۹] برای مقابله با دزدیده شدن اطلاعات از کانال‌های ارتباطی اشیا هوشمند روشی ارائه کرده‌اند. این روش برای مقابله با اکثر حملات احتمالی راه حل مناسبی است، اما برای حمله استراق سمع و حمله سرک کشی راه‌حلی ارائه نکرده است.

مهدی اکبری گورابی [۲۰] یک روش مبتنی بر سخت‌افزار با استفاده از کارت هوشمند و احراز هویت دوفاکتوره ارائه کرده است. این روش، رازداری پیش‌رو[2] را ارائه نمی‌دهد، حمله استراق سمع و سرک کشی را نیز بررسی نمی‌کند. اما در برابر حملات تکرار و یا دزدیده شدن کارت، مقاوم است.

با عنایت به موارد فوق، روش‌های موجود در تأمین احراز هویت ازنظر حملات متداول به خانه هوشمند، ضعف دارند. لذا در مقاله حاضر، یک روش مبتنی بر رمز یکبار مصرف و استفاده از کارت هوشمند و الگوریتم منحنی بیضوی، به‌منظور بهبود روش‌های پیشین، و مقابله با حملات متداول، ارائه‌شده است. در این روش، احراز هویت متقابل بین کاربر و گره دروازه و همچنین اشیا خانه هوشمند و گره دروازه، انجام می‌شود.

۳. روش پیشنهادی

روش پیشنهادشده در این مقاله، از دو بخش تشکیل‌شده است. بخش اول مربوط به احراز هویت فرد و سرویس‌دهنده خانه هوشمند است و شامل سه مرحله ثبت کاربر، ورود افراد/احراز هویت، و درخواست خدمت است. در مرحله ثبت کاربر، اطلاعات کاربر در سرویس‌دهنده ثبت می‌گردد. پس از ثبت اطلاعات، به او یک کارت هوشمند تعلق می‌گیرد. در مرحله ورود افراد/احراز هویت، کاربر کارت هوشمند را وارد پایانه می‌کند و باید اثبات شود که او همان شخصی است که قبلاً در سرویس‌دهنده خانه هوشمند ثبت‌شده بود. پس از احراز هویت کاربر توسط سرویس‌دهنده، کاربر درخواست استفاده از هریک از لوازم هوشمند موردنظرموردنظرش را به گره دروازه موجود در خانه هوشمند، ارسال می‌کند.

در بخش دوم، گره دروازه درخواست کاربر را دریافت کرده است و کاربر باید برای استفاده از وسیله هوشمند موردنظرموردنظرش، توسط گره دروازه، احراز هویت گردد. پس از احراز هویت دوطرفه بین کاربر و گره دروازه و مجاز شناخته شدن کاربر، درخواست استفاده از شی هوشمند توسط گره دروازه، برای شی موردنظر ارسال می‌گردد. در این مرحله، یک احراز هویت دوطرفه نیز بین گره دروازه و شی هوشمند انجام می‌گیرد تا گره دروازه از مخرب نبودن شی هوشمند مطمئن شود و شی هوشمند نیز از این‌که درخواست از طرف گره دروازه برای او ارسال‌شده است، اطمینان یابد. برای توضیح و تفسیر مراحل روش پیشنهادی، در این تحقیق از یک سری علائم اختصاری استفاده‌شده که در جدول (۱) نشان داده شده‌اند.

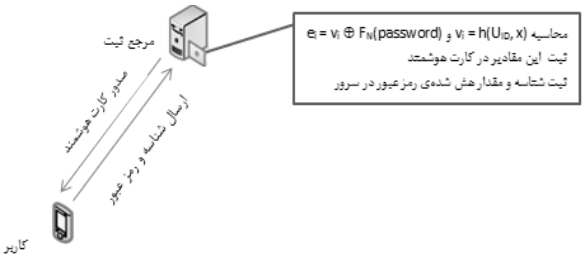
جدول ۱. علائم اختصاری استفاده‌شده در روش پیشنهادی

علامت	توضیح
RA	مرجع ثبت
R_{Ui}	عدد حاصل از چکیده‌سازی رمز کاربر در RA
R_{Si}	عدد تصادفی تولیدشده توسط RA
F(), h()	توابع چکیده‌سازی
N	تعداد دفعات مجاز ورود در مدت زمان معتبر بودن بلیط
S_{key}	کلید مشترک بین دروازه و کاربر
U_{ID}	کاربر دارای شناسه کاربری
RA_{ID}	شناسه RA
$E_{RA-GW}()$	رمزگذاری با استفاده از کلید متقارن بین RAو GW
E_K	رمزگذاری با استفاده از K
E_K	مهرزمانی نشان‌دهنده معتبر بودن کلید نشست

[1] lightweight
[2] Forward secracy

لازم به توضیح است که دو پارامتر N و T برای محدود کردن کاربر استفاده می‌شوند. برای مثال، اگر N=150 و (ماه)T=1 باشد، یعنی یک کاربر مجاز، می‌تواند در طول یک ماه، ۱۵۰مرتبه، بدون ورود/ احراز هویت مجدد، به گره دروازه دسترسی داشته باشد. در ادامه، فازهای مختلف بخش اول روش پیشنهادی تشریح می‌شوند.

در مرحله ثبت کاربر، فرض می‌شود که x یک کلید سری است که در مرجع ثبت، نگهداری می‌شود. تابع h() به‌عنوان یک تابع چکیده‌ساز در نظر گرفته می‌شود. U نیز به‌عنوان کاربر در نظر گرفته می‌شود که درخواست احراز هویت می‌کند. همان‌گونه که در شکل (۱) نشان داده‌شده است، کاربر، شناسه و رمز خودش را جهت ثبت، به سامانه مرجع ثبت ارسال می‌کند. مرجع ثبت، بعد از دریافت شناسه و رمز از کاربر، عملیات زیر را اجرا می‌کند: ۱) عبارت‌های $v_i = h(U_{ID}, x)$ و $e_i = v_i \oplus F_N(password)$ را برای U محاسبه می‌کند و آن‌ها را به‌عنوان اطلاعات سری U در نظر می‌گیرد. ۲) مقدار v_i و e_i را در حافظه کارت هوشمند ثبت می‌کند و کارت را برای U صادر می‌کند و در اختیار او می‌گذارد. $F_N(0)$ مقدار نهایی چکیده‌سازی پذیرفته‌شده برای کاربر است. ۳) درنهایت، سرویس‌دهنده مقدار U_{ID} و رمزی را که توسط تابع F درهم شده است، در خودش نگه می‌دارد. این عملیات در مرحله ثبت هر کاربر جدید، به‌صورت مجزا برای هر کاربر اجرا می‌شود.



شکل ۱. مرحله ثبت کاربر در مرجع ثبت

در مرحله ورود و احراز هویت، وقتی کاربر U_{ID} قصد ورود به سامانه مرجع ثبت را داشته باشد، باید کارت هوشمند را در پایانه وارد کند و شناسه U_{ID} و رمز عبور $F_N(password)$ را وارد کند. سپس کارت هوشمند، عملیات زیر را اجرا می‌کند:

۱) برای i اُمین احراز هویت کاربر، به تعداد i مرتبه، تابع چکیده‌سازی $F^i_N(password)$ را اجرا می‌کند و نتیجه را محاسبه می‌کند.

۲) مقدار $C = h(e_i \oplus F^i_N(password))$ را محاسبه می‌کند.

۳) پیام محتوی (U_{ID}, C) را که درواقع، پیام درخواست احراز هویت است، به مرجع ثبت ارسال می‌کند. بعد از این‌که اطلاعات توسط سرویس‌دهنده مرجع ثبت دریافت شد، برای برقراری احراز هویت بین کاربر و مرجع ثبت، مراحل بعد در مرجع ثبت اجرا می‌شود.

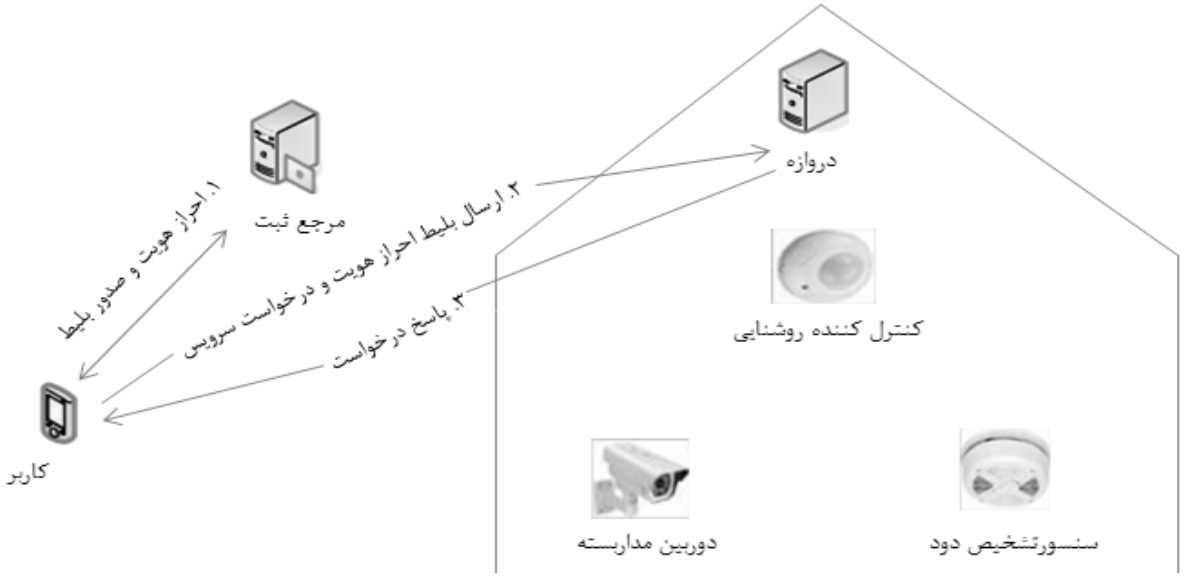
۴) سرویس‌دهنده، U_{ID} را می‌شناسد و تائید می‌کند. سپس یک مقدار $v'_i = h(U_{ID}, x)$ تولید می‌گردد و بررسی می‌شود که آیا $C = h(e'_i \oplus F'^i_N(password))$ است یا خیر. سپس به مقدار چکیده‌سازی کاربر و سرویس‌دهنده، یک واحد اضافه می‌شود، یعنی $F^i_N(password)$ برای کاربر و $F^{i+1}_N(password)$ برای سرویس‌دهنده. اگر این دو مقدار برابر نباشند، درخواست کاربر رد و در غیر این‌صورت، تائید می‌شود. در صورت تائید، سرویس‌دهنده باید اطلاعاتی را برای استفاده او از خانه هوشمند و ارتباط او با دروازه در اختیارش بگذارد.

۵) سرویس‌دهنده مقدار عدد تصادفی یکبار مصرف R_{Si} را تولید می‌کند و مقدار $F^i_N(password)$ را درون R_{Ui} قرار می‌دهد؛ سپس مقدار $S_{key} = h(R_{Si}, R_{Ui})$ را محاسبه می‌کند.

۶) سرویس‌دهنده یک بلیط احراز هویت تولید می‌کند و آن را با کلید متقارن که بین خودش و دروازه، مشترک است، قفل می‌کند. سپس $E_{RA-GW}(U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T)$ را به همراه پیامی که نشان‌دهنده این است که کاربر احراز هویت شده است به‌صورت $E_{RUi}(U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T, h(S_{key}, U_{ID}))$ به کاربر می‌فرستد.

۷) کاربر با دریافت پیام متوجه می‌شود که درخواست احراز هویت او پذیرفته‌شده است. حال باید مطمئن شود که پیام از سمت سرویس‌دهنده است. کاربر با دانستن $R_{Ui} = F^i_N(password)$ پیام را رمزگشایی می‌کند و با دست یافتن به R_{Si} از داخل پیام می‌تواند مقدار $S_{key} = h(R_{Si}, R_{Ui})$ را محاسبه کند و با دانستن S_{key}، مقدار $h(S_{key}, U_{ID})$ را به دست آورده و با تابع $h(S_{key}, U_{ID})$ که از طرف سرویس‌دهنده فرستاده‌شده، مقایسه می‌کند و مطمئن می‌شود که پیام از سمت سرویس‌دهنده است.

قابل‌توجه است که فقط کاربرِ مجاز، مقدار password را می‌داند و به R_{Ui} دسترسی دارد؛ پس فقط کاربر مجاز می‌تواند پیامی که از سمت سرویس‌دهنده آمده است را رمزگشایی کند و R_{Si} را به‌دست آورد. برای ساده‌سازی و درک سازوکار احراز هویت کاربر، به شکل (۲) توجه شود.

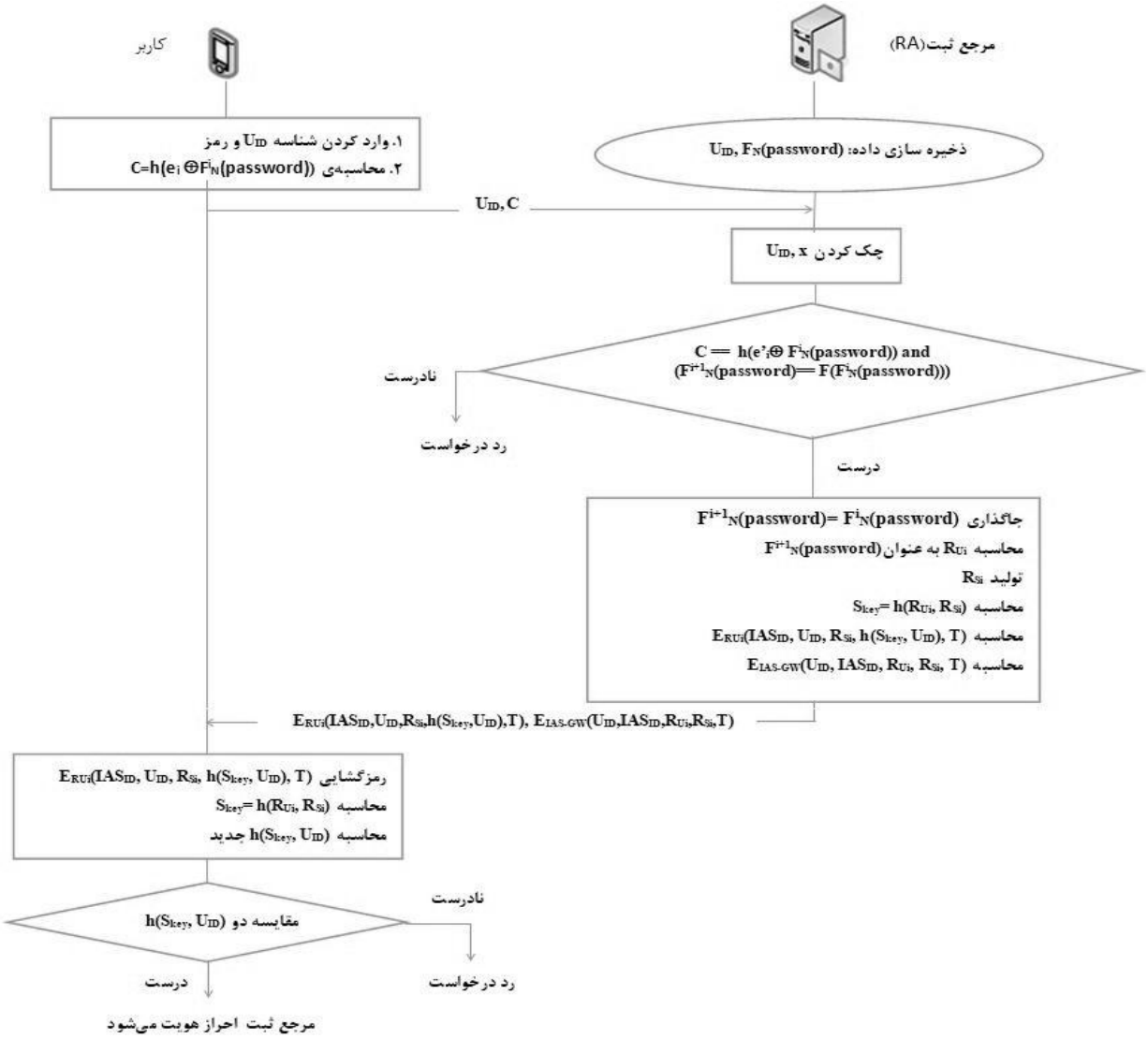


شکل ۲. سازوکار احراز هویت کاربر

با توجه به شکل (۲)، در روش پیشنهادی، یک مرجع ثبت، چند شی هوشمند، یک گره دروازه و کاربرانی که قصد دسترسی به خانه را دارند، در نظر گرفته می‌شوند. قبل از همه، ثبت هر دستگاه هوشمند و گره دروازه در مرجع ثبت (RA)، انجام‌شده است. اگر کاربری بخواهد به دستگاه‌های هوشمند دسترسی داشته باشد و از خدمات خانه هوشمند استفاده نماید، باید از طریق مرجع ثبت، احراز هویت شود و بلیط احراز هویت را دریافت کند. این بلیط برای ارتباط کاربر با گره دروازه، کاربرد دارد. کاربری که احراز هویت شده است، برای استفاده از خدمات خانه هوشمند، به این بلیط نیاز دارد.

در شکل (۳)، مرحله ورود و احراز هویت نشان داده‌شده است. یک درخواست احراز هویت از سوی کاربر به سرویس‌دهنده ارسال می‌شود و بعد از تائید اطلاعات کاربر از سوی سرویس‌دهنده، یک پاسخ از سمت سرویس‌دهنده برای کاربر ارسال می‌شود. کاربر نیاز دارد که پاسخ دریافت شده از سمت سرویس‌دهنده را تائید اعتبار نماید. در مرحله درخواست سرویس، بعد از این‌که کاربر، توسط مرجع ثبت، تائید و احراز هویت گردید، به‌عنوان کاربر مجاز شناخته می‌شود؛ یعنی این کاربر اجازه دارد تا از خدمات خانه هوشمند استفاده کند. برای این کار، کاربر باید درخواست خود را به‌صورت(U_{ID}, Service) که شامل شناسه او و خدمت درخواستی است، به سمت گره دروازه ارسال کند. این درخواست به‌وسیله S_{key} رمزگذاری شده و از سوی کاربر به همراه بلیطی که کاربر در مرحله قبل، از سرویس‌دهنده دریافت کرده، یعنی ($E_{RA-GW}(U_{ID}, RA_{ID}, R_{Ui},$ R_{Si}, T، برای دروازه ارسال می‌شود.

در مرحله درخواست خدمت از سوی کاربر به سمت دروازه، دروازه دو پیام دریافت می‌کند. یک پیام، بلیطی است که سرویس‌دهنده از طریق کاربر برای او فرستاده است و دیگری، درخواست استفاده از خدمات خانه که توسط کاربر برای دروازه ارسال‌شده است. دروازه در ابتدا پیامی را که با کلید مشترک بین خودش و سرویس‌دهنده رمزگذاری شده بود، باز می‌کند. T را چک می‌کند و مطمئن می‌شود پیام معتبر است. با به دست آوردن R_{Ui} و R_{Si} از داخل بلیط دریافت شده، مقدار S_{key} را دست می‌آورد و با آن، پیام کاربر را رمزگشایی می‌کند. U_{ID} که در پیام کاربر است را با U_{ID} ای که توسط بلیط فرستاده شده است، مقایسه می‌کند و اعتبار کاربر را تائید می‌کند و به او اجازه دسترسی به خدمات خانه را می‌دهد. سپس R_{Ui} را با S_{key} رمزگذاری می‌کند و برای کاربر می‌فرستد و کاربر مطمئن می‌شود که پیامش به شخص مطمئن یا همان دروازه رسیده است و اعتبار دروازه هم نزد کاربر تائید می‌شود. بدین ترتیب، یک احراز هویت دوطرفه انجام می‌شود.



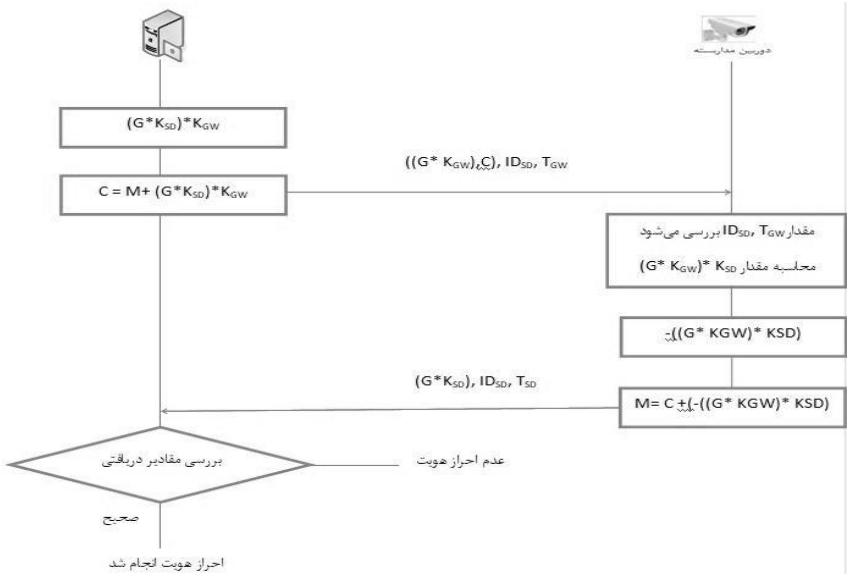
شکل ۳. مرحله ورود و احراز هویت کاربر iأم

احراز هویت بین گره دروازه و دستگاه‌های خانه هوشمند بدین‌صورت است که ابتدا، تمام دستگاه‌های خانه هوشمند باید در مرجع ثبت RA ثبت شوند و یک شناسه یکتا دریافت کنند. پس‌ازآن برای استفاده از هر دستگاه، آن دستگاه توسط گره دروازه احراز هویت می‌گردد و آماده دریافت دستورات اجرایی می‌شود. مراحل ثبت و احراز هویت دستگاه‌ها به ترتیب، در ادامه ذکر می‌شوند:

۱) در مرحله ثبت دستگاه‌ها که توسط مرجع ثبت انجام می‌شود، برای هر دستگاه SD، یک شناسه یکتای ID_{SD} توسط مرجع ثبت درنظر گرفته می‌شود. علاوه بر آن، یک کلید خصوصی به نام K_{SD} و یک کلید عمومی $K_{SD}*G$ تولید می‌شود. این اطلاعات در پایان مرحله ثبت، در حافظه دستگاه SD ذخیره می‌شود. گره دروازه نیز مجهز به اطلاعات کلید خصوصی K_{GW} و کلید عمومی $K_{GW}*G$، و شناسه هر دستگاه هوشمند ID_{SD} می‌شود.

۲) در مرحله احراز هویت بین دستگاه‌ها و گره دروازه، کاربر درخواست استفاده از دستگاه را به‌صورت $(U_{ID}, Service)$ و $E_{RA-GW}(U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T)$ به گره دروازه ارسال می‌کند. پس از برقراری ارتباط و احراز هویت طرفین، گره دروازه درخواست را با استفاده از الگوریتم منحنی بیضوی، با توجه به مزیت طول کوتاه کلید در آن [۱۷]، رمزنگاری کرده و به همراه یک مهر زمانی T_{GW} و شناسه دستگاه موردنظر ID_{SD}، برای دستگاهی که خدمت آن درخواست شده است، ارسال می‌کند.

گره دروازه برای فرستادن پیام M به‌صورت رمزشده به دوربین مداربسته، ابتدا با حاصل‌ضرب کلید عمومی دستگاه هوشمند در کلید خصوصی خودش و حاصل‌جمع این مقدار با پیام اصلی، یک متن رمزی می‌سازد و آن را به همراه یک سری اطلاعات دیگر که در همین بخش به آن اشاره گردید، برای دستگاه موردنظر، ارسال می‌نماید. دستگاه پس از دریافت متن رمز شده، ابتدا شناسه خودش و مقدار مهر زمانی را چک می‌کند.



شکل ۴. مرحله احراز هویت بین دستگاه‌ها و گره دروازه

سپس با کلید خصوصی خودش، بخشی از پیامی که دریافت کرده بود را باز می‌کند و درنهایت، مقدار پیام را می‌یابد. دستگاه به‌منظور انجام احراز هویت دوطرفه، یک مهرزمانی، شناسه خودش و کلید عمومی کلید دروازه را برای آن ارسال می‌کند. گره، این مقادیر را دریافت می‌کند. اگر این مقادیر صحیح باشند، مشکلی در احراز هویت وجود نخواهد داشت ولی اگر تشخیص دهد که اطلاعات دریافتی نادرست بوده است، دستگاه احراز هویت نمی‌شود.

۴. ارزیابی روش پیشنهادی

روش پیشنهادی ابتدا با استفاده از منطق بن که یکی از روش‌های متداول ارزیابی عملکرد احراز هویت است، مورد ارزیابی قرارگرفته است. هر سه مرحله ثبت، ورود/ احراز هویت و درخواست خدمت با استفاده از منطق بن ارزیابی می‌شوند.

برخی از علائم اختصاری که در این بخش استفاده می‌گردند، قبلاً در جدول (۱) معرفی‌شده‌اند و علائم دیگری نیز در این بخش، معرفی خواهند شد. ابتدا پیام‌های ردوبدل شده بین طرفین در روش پیشنهادی باید به فرمول تبدیل شوند، اهداف مشخص شوند و سپس باید با استفاده از قوانین منطق بن، این اهداف اثبات شوند. در شکل (۴)، پیام‌ها و طرفینی که در روش پیشنهادی مورد استفاده قرار گرفته‌اند، مشخص شده مشخص شده‌اند. برای ارزیابی به‌وسیله منطق بن، کافی است همین پیام‌ها و طرفین، ایده‌آل‌سازی شوند و اهداف مشخص گردند و اثبات گردند.

۴-۱. ارزیابی با روش بن

الف- مرحله عمومی

باروز، عبدی و نیدهام، یک منطق احراز هویت را توصیف می‌کنند که در مقاله [۱۶] به‌اختصار به نام منطق بن شناخته می‌شود. سه مرحله اصلی برای تجزیه‌وتحلیل یک پروتکل با استفاده از منطق بن وجود دارد :

مرحله اول،بیان فرض‌ها و هدف‌ها به شکل فرمول است (مرحله وضعیت)،منطق از یک وضعیت شناخته‌شده به سمت وضعیتی می‌رود که به اهداف مسئله دست‌یابیم. مرحله دوم،تغییر شکل دادن پروتکل به فرمول است و در مرحله سوم، یک مجموعه از قوانین استنتاجی که شرایط اساسی نامیده می‌شود به دست می‌آید. شرایط اساسی از فرض‌ها شروع می‌شود و توسط فرمول‌ها به اهداف می‌رسد و زمانی که شرایط به اهداف می‌رسند یعنی فرض اثبات‌شده است و روش پیشنهادی درست کار می‌کند.

با توجه به توضیحاتی که ارائه گردید، در ابتدا پیام‌های ردوبدل شده بین طرفین در روش پیشنهادی باید به فرمول

تبدیل شوند، اهداف مشخص شوند و سپس باید با استفاده از قوانین منطق بن، این اهداف اثبات شود.برای ارزیابی به‌وسیله منطق بن، کافی است همین پیام‌ها و طرفین ایده‌آل‌سازی شوند و اهداف مشخص گردند و اثبات گردند.

بنابراین، ابتدا پیام‌هایی که بین طرفین روش پیشنهادی ردوبدل می‌گردد، به شکل زیر نمایش داده می‌شود:

Message 1: $U\rightarrow RA : U_{ID}, C$

این پیام به این معنی است که، کاربر، یک پیام برای مرجع ثبت فرستاده است که این پیام شامل کدکاربر و متن رمزشده c است.

Message 2: $RA\rightarrow U:\{U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T_{RA}\}K_{RA\text{-}GW}, \{RA_{ID}, U_{ID}, R_{Si}, h(S_{Key},U_{ID}), T_{RA}\}R_{Uis}$

مفهوم این پیام آن است که مرجع ثبت، پیامی برای کاربر فرستاده است که شامل دو بخش است. بخش اول پیامی است که به‌وسیله کلیدی که بین خودش و گره دروازه مشترک است، رمزگذاری شده است و بخش دوم، پیام مربوط به خود کاربر است و با کلید خصوصی کاربر، رمز شده است.

Message 3: $U\rightarrow GW: \{U_{ID}, RA_{ID}, R_{Ui}, R_{Si}, T_{RA}\} K_{RA\text{-}GW}, \{U_{ID}, Service, T_U\} S_{Key}$

فرم عمومی این پیام به این صورت است که کاربر یک پیام برای گره دروازه ارسال می‌کند؛ این پیام شامل دو بخش است. بخش اول، بخشی از پیامی است که در مرحله قبل، مرجع ثبت برای کاربر ارسال کرده بود و بخش دوم، محتوی درخواست خدمت کاربر و شناسه کاربر است.

Message 4: $GW\rightarrow U: \{T_{U+1}, R_{Ui}\} S_{Key}$

در این فرم عمومی، یک پیام از طرف گره دروازه برای کاربر ارسال‌شده است که حاوی مدت زمان اعتبار پیام و رمز مربوط به کاربر است.

ب- هدف

برای اثبات این‌که روش پیشنهادی درست کار می‌کند و اثبات احراز هویت دوطرفه بین کاربر و گره دروازه و کاربر و مرجع ثبت، اهداف زیر تعریف می‌شوند: هدف ۱: $U|\equiv R_{Si}$ ، هدف ۲: $U|\equiv T_{U+1}$. هدف اول به این معنی است که اگر کاربر، R_{Si} را ببیند، یعنی از طرف مرجع ثبت مورد اعتماد، احراز هویت شده است. هدف دوم آن است که اگر کاربر در پیام دریافتی از طرف گره دروازه، مقدار T_{U+1} را دریافت کند، اجازه دارد از لوازمی که درخواست کرده بود استفاده کند و درواقع، توسط گره دروازه احراز هویت شود.

ج- ایده‌آل‌سازی

به‌منظور اعمال منطق بن، باید پیام‌های مرحله عمومی به پیام‌های ایده‌آل تبدیل شوند. برای این کار، شناسه‌ها و متن‌ها تغییر شکل پیدا می‌کنند و فرم ظاهری پیام‌های عمومی به‌صورت زیر تغییر شکل می‌یابد:

Message 1: $U\rightarrow RA: U_{ID}, C$

Message 2: $RA\rightarrow U: \{N_c, R_{Ui}, R_{Si}, T_{RA}\}K_{RA\text{-}GW}, \{N_d, R_{Si}, h(S_{Key},U_{ID}), T_{RA}\}R_{Ui}$

Message 3: $U\rightarrow GW: \{N_c, R_{Ui}, R_{Si}, T_{RA}\} K_{RA\text{-}GW}, \{N_e, T_U\} S_{Key}$

Message 4: $GW\rightarrow U: \{T_{U+1}, R_{Ui}\} S_{Key}$

روند اثبات در منطق بن به معنی از شرایط به هدف رسیدن است. در ابتدا، اگر کاربر (U) و گره دروازه (GW) و مرجع ثبت (RA) به ترتیب با پارامترهای A، B و S نشان داده شوند، فرض‌های اولیه به شکل زیر می‌شوند:

$A|\equiv A\leftrightarrow S, A|\equiv(S\Rightarrow A\leftrightarrow B), A|\equiv\#T_S, A|\equiv\#T_a, A|\equiv R_{Ui}$

$B|\equiv B\leftrightarrow S, B|\equiv(S\Rightarrow A\leftrightarrow B), B|\equiv\#T_S$

$S|\equiv A\leftrightarrow S, S|\equiv B\leftrightarrow S, S|\equiv(A\leftrightarrow B), S|\equiv\#R_{Si}$

اثبات هدف ۱. پس از این‌که پیام ۱ فرستاده می‌شود، A پیامی را دریافت می‌کند (پیام۲) که قادر است بخشی از آن را بفهمد:

$A \lhd \{N_c, R_{Ui}, R_{Si}, T_S\}K_{SB}, \{N_d, R_{Si}, h(S_{Key},A_{ID}), T_S\}K_{RUI}$

A پیامی را که از سمت S دریافت کرده است، باز می‌کند، بخشی از پیام را که با کلید مشترک S و B رمز شده است، به همراه یک پیام درخواست خدمت که خودش تولید می‌کند برای B می‌فرستد و بخش دیگر را که متوجه آن می‌شود، رمزگشایی کرده، و مقدار RSi را می‌بیند:

طبق فرض $A|\equiv R_{Ui}$

$A|\equiv S|\equiv\{N_c, R_{Ui}, R_{Si}, T_S\}K_{SB}, (N_d, R_{Si}, h(S_{Key},A_{ID}), T_S)$

پس بخشی که A می‌تواند بخواند به‌صورت زیر است

$A|\equiv S|\equiv(N_d, R_{Si}, h(S_{Key},A_{ID}), T_S)$

طبق فرض $S|\equiv\#R_{Si}$، و درنتیجه، هدف ۱ به اثبات رسیده است و خواهیم داشت:

$$A|\equiv\#R_{Si} \quad (1)$$

طبق فرض، با جاگذاری U به‌جای A خواهیم داشت: $\#R_{Si}$ $U|\equiv$ که یعنی کاربر احراز هویت شده است و مطمئن است که پیام را از مرجع ثبت دریافت کرده است. بعد از اثبات ۱ و با استفاده از فرض، می‌دانیم که اگر $A|\equiv R_{Ui}$ آنگاه:

$$A|\equiv S_{Key} \quad (2)$$

اثبات هدف ۲. پیام ۳ از طرف A برای B فرستاده می‌شود. B از پیام دریافت شده، می‌تواند آن بخشی را که از طرف S برایش ارسال‌شده است، ببیند. آن را با کلید مشترک BS رمزگشایی می‌کند. از داخل پیام رمزگشایی‌شده، مقدار R_{Si} و R_{Ui} را به دست می‌آورد و با استفاده از آن‌ها، مقدار S_{Key} را محاسبه

می‌کند:

$B \lhd \{N_c, R_{Ui}, R_{Si}, T_S\}\ K_{SB}, \{N_e, T_A\}\ S_{Key}$
$B|\equiv S|\equiv \{N_c, R_{Ui}, R_{Si}, T_S\}\ K_{SB}$
$B \lhd \{N_e, T_A\}\ S_{Key}$

طبق فرض، $B|\equiv B \leftrightarrow S$ است؛ پس B می‌تواند پیامی را که به‌واسطه A از S دریافت کرده، با کلید مشترکشان رمزگشایی کند:

$B|\equiv S|\equiv (N_c, R_{Ui}, R_{Si}, T_S)$
پس $B|\equiv R_{Si}, B|\equiv R_{Ui}$

با دانستن این مقادیر، B مقدار S_{Key} را محاسبه می‌کند. بنابراین:

$B \lhd \{N_e, T_A\}\ S_{Key}$
$B|\equiv (N_e, T_A)$
$B|\equiv T_A$

حال، B یک واحد به مقدار T_A اضافه می‌کند و آن را رمزگذاری کرده و برای A ارسال می‌کند (پیام ۴). A یک پیام از B دریافت می‌کند که با کلید S_{Key} می‌تواند آن را بخواند و به محتوای پیام دست پیدا کند:

$A \lhd \{R_{Ui}, T_{A+1}\}\ S_{Key}$

از اثبات ۱، با استفاده از نتیجه حاصل‌شده در رابطه (۲) داریم: $A|\equiv S_{Key}$. پس هدف ۲ نیز اثبات می‌گردد:

$A|\equiv (R_{Ui}, T_{A+1})$
$A|\equiv T_{A+1}$

با جاگذاری U به‌جای A طبق فرض ابتدایی، خواهیم داشت: $U|\equiv T_{A+1}$. نتیجه ارزیابی با استفاده از منطق بن، در اثبات ۱ و ۲، نشان می‌دهد که روش پیشنهادی پژوهش در مورد احراز هویت دوطرفه کاربر و مرجع ثبت و همچنین کاربر و گره دروازه، به‌صورت صحیح کار می‌کند.

۴-۲. ارزیابی با استفاده از ابزار آویسپا

روش پیشنهادی این تحقیق در ابزار آویسپا شبیه‌سازی‌شده و موردبررسی و ارزیابی قرارگرفته است. این ابزار معمولاً در اثبات کارایی روش‌های مربوط به امنیت در خانه هوشمند استفاده می‌شود. زبان برنامه‌نویسی این ابزار، زبان HLPSL[1] است که یک زبان سطح بالا بوده و برای اجراشدن، ابتدا به زبان HLPSL2IF ترجمه‌شده و سپس به‌عنوان ورودی در چهار مدل برنامه سرویس‌دهنده مورد استفاده قرار می‌گیرد. این مدل‌ها عبارت‌اند از OFMC[2]، CLAtSe[3]، SATMC[4]، TA4SP[5] [۱۲].

ابزار آویسپا، کاربرد زیادی در تجزیه‌وتحلیل پروتکل‌های امنیتی دارد. برای استفاده از این ابزار، مدل‌های پروتکلی باید به زبان HLPSL نوشته شوند. مرحله ثبت کاربر، و ورود/ احراز هویت در HLPSL پیاده‌سازی شده‌اند. در این پیاده‌سازی، سه نقش اصلی در نظر گرفته‌شده‌اند: کاربر که با حرف A (به‌طور مثال، حرف ابتدای Alice) مشخص‌شده است. مرجع ثبت که با حرف S (حرف ابتدای Server) مشخص‌شده است، و گره دروازه که با حرف B (حرف ابتدای Bob) مشخص‌شده است. روش پیشنهادی با استفاده از بک-اِند[6]های OFMG و CL-AtSe در آویسپا پیاده‌سازی شده است.

پس از پیاده‌سازی توسط کدهای زبان HLPSL و اجرای برنامه توسط نرم‌افزار آویسپا، نتایج به‌دست‌آمده که به ترتیب در شکل‌های (۵) و (۶) مشخص است، حاکی از قابل‌اطمینان بودن روش پیشنهادی است.

```
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL
PROTOCOL
 /home/span/span/testsuite/results/testfinal.if
GOAL
 As Specified
BACKEND
 CL-AtSe
STATISTICS
 Analysed  : 357012 states
 Reachable  : 28904 states
 Translation: 0.10 seconds
 Computation: 9.24 seconds
```

شکل (۵). شبیه‌سازی روش پیشنهادی با CL-AtSe

```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/testfinal.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
 searchTime: 1.41s
 visitedNodes: 348 nodes
 depth: 16 plies
```

شکل ۶. شبیه‌سازی روش پیشنهادی با OFMC

[1] High Level Protocol Specification Language (زبان مشخصات پروتکل سطح بالا)
[2] On-the-fly-model-checker
[3] CL-based Attack Searcher
[4] SAT-based Model-Checker
[5] Tree Automated based on Automatic Approximations for the Analysis of Security Protocol
[6] Backend

جهت ارزیابی میزان کارایی عملکرد روش پیشنهادی در مقایسه با روش‌های موجود، نتایج آزمون‌های انجام‌گرفته بر روی روش پیشنهادی و روش‌های موجود، در جدول (۲) نشان داده شده است.

جدول ۲. ارزیابی روش پیشنهادی بر اساس عامل‌های امنیتی

عامل مقایسه	[۸]	[۱۱]	[۱۲]	[۱۴]	روش پیشنهادی
احراز هویت دوطرفه[1]	×	✓	✓	×	✓
رازداری پیش-رو[2]	×	✓	✓	✓	✓
حمله تکرار[3]	✓	×	✓	✓	✓
حمله مردی در میان[4]	✓	×	✓	-	✓
حمله مفقودشدن کارت‌هوشمند[5]	×	✓	✓	-	✓
حمله حدس رمز عبور[6]	×	✓	✓	×	✓
حمله استراق سمع[7]	×	×	×	×	✓
حمله سرک-کشی[8]	×	×	×	✓	✓

نمودار ۱. مقایسه روش پیشنهادی و روش‌های پیشین بر اساس عامل‌های امنیتی

با توجه به نتایج ارائه‌شده در جدول (۲) و نمودار (۱)، روش پیشنهادی از عامل‌های امنیتی بیشتری در مقایسه با روش‌های موجود، پشتیبانی می‌کند. جزئیات بیشتر عامل‌های مقایسه و چگونگی آزمون آن‌ها، در زیر ارائه شده است. جهت بررسی احراز هویت دوطرفه، در روش پیشنهادی، کاربر پیام را به سرویس‌دهنده ارسال می‌کند و سرویس‌دهنده، هویت او را تائید می‌کند و برای کاربر، یک پیام ارسال می‌کند. کاربر قابل‌اطمینان بودن پیام دریافت شده از طرف سرویس‌دهنده را با بررسی T، تائید می‌کند. درنتیجه، یک احراز هویت دوسویه بین کاربر و مرجع ثبت و بالعکس برقرار شده است.

ازنظر رازداری پیش‌رو، اگر کارت هوشمند دزدیده شود و به دست مهاجم بیفتد، و اگر فرض شود که مهاجم، مقدار x را نیز داشته باشد، به‌دلیل نداشتن رمز عبور کاربر نمی‌تواند پیام C را تولیدکند و برای سرویس‌دهنده بفرستد و بنابراین با شکست مواجه می‌شود. ازنظر حمله تکرار، رمز عبوری که توسط کاربر وارد می‌شود و به مرجع ثبت ارسال می‌شود، توسط تابع چکیده‌ساز یک‌طرفه F() درهم می‌شود. بنابراین، اگر مهاجم بتواند به U_{ID} دست پیدا کند، هرگز نمی‌تواند رمز عبور مربوط به آن را بیابد و با شکست مواجه می‌شود.

جهت بررسی حمله مردی در میان، فرض شود که مهاجم، پیام ورود/احراز هویت را بدون این‌که طرفین متوجه شوند، دریافت کند (مثلاً خودش را به‌جای سرویس‌دهنده جا بزند و پیام (A_{ID}, C) را از کاربر بگیرد و آن را تبدیل به (A_{ID}, C) کند و برای سرویس‌دهنده ارسال کند). زمانی که سرویس‌دهنده این پیام را دریافت می‌کند، از طریق رمزگشایی C، مقدار ID کاربر را به دست می‌آورد و با A_{ID} مقایسه می‌کند و متوجه تقلبی بودن این پیام می‌شود و درنتیجه، درخواست کاربر رد می‌شود.

وقتی یک کارت هوشمند گم و یا دزدیده می‌شود، اگر فرض شود که کاربر غیرمجاز می‌تواند با حمله حدس مکرر، رمز عبور کارت هوشمند را حدس بزند، یا بخواهد به‌جای کاربر سعی در ورود به سامانه داشته باشد، زمانی که کارت را وارد پایانه کند، اولین چالشی که با آن مواجه می‌شود، باید ابتدا یک درخواست معتبر به شکل (A_{ID}, C) را تولید کند. چون مهاجم به‌دلیل نداشتن v_i قادر به تولید کردن C نیست، بنابراین نمی‌تواند این درخواست معتبر را بسازد و روش پیشنهادی در مقابل حمله مفقود شدن کارت هوشمند، نیز مقاوم است.

در روش پیشنهادی، اگر مهاجم به درخواست ورود/ احراز هویت (A_{ID}, C) دسترسی پیدا کند، نمی‌تواند رمز عبور را حدس بزند چراکه کلید سری X را ندارد. لذا این روش در مقابل حمله

[1] Mutual authentication
[2] Forward secracy
[3] Replay attack
[4] Man-in-the middle attack
[5] Smart cart loss attack
[6] Password guessing attack
[7] Eavesdropping
[8] Shoulder surfing

حدس رمز عبور، نیز مقاوم است. همچنین اگر کاربری برای اولین بار بخواهد وارد سامانه شود یا احراز هویت شود، ممکن است برنامه‌های استراق سمع بتوانند به شناسه و رمز او دست یابند. روش پیشنهادی در برابر این حمله نیز مقاوم است چراکه تمام پیام‌های مهم مثل پیام پاسخ به درخواست ورود/ احراز هویت و بلیط احراز هویت، به ترتیب با کلیدهای R_{Ui} و K_{SB} که یک کلید متقارن است، رمزگذاری می‌شوند.

ازنظر حمله سرک‌کشی نیز، اگر فرض شود که کاربری توسط سرک‌کشی، اطلاعات یک کاربر مجاز را به دست آورده باشد، به‌دلیل این‌که مقدار R_{Ui} را نمی‌داند، نمی‌تواند پیام پاسخ به درخواست ورودش را که از سمت سرویس‌دهنده برای او ارسال می‌شود، باز کند و درنتیجه، درخواست ورود/ احراز هویت او رد می‌شود.

۵. نتیجه‌گیری

اعتماد نا به‌جا به افراد و عدم احراز هویت صحیح در خصوص فردی که قصد استفاده از خدمات خانه هوشمند را دارد، موجب هدر رفتن سرمایه‌های مالی و شاید اعتبار و آبروی اشخاص می‌شود. بنابراین، به کار بستن راه‌کاری مؤثر جهت اداره نمودن احراز هویت افراد به‌گونه‌ای که بتواند در برابر حملات مخرب بیشتری مقاومت کند و مانع ورود مهاجمین به سامانه خانه هوشمند شود، از اهمیت به‌سزایی برخوردار است.

در این مقاله، روشی مبتنی بر تلفیق رمز یکبار مصرف و کارت هوشمند و الگوریتم منحنی بیضوی جهت احراز هویت افرادی که قصد ورود به سامانه خانه هوشمند را دارند، ارائه گردید. روش پیشنهادی، احراز هویت متقابل بین کاربر و گره دروازه و همچنین اشیا خانه هوشمند و گره دروازه، را انجام می‌دهد. ارزیابی‌های انجام‌شده حاکی از آن است که روش پیشنهادی در مقایسه با روش‌های موجود، قادر است با تعداد حمله متداول بیشتری به خانه هوشمند، مقابله نماید.

۶. مرجع‌ها

[1] Bugeja, J.; Jacobsson, A.; Davidsson, P. "On Privacy and Security Challenges in Smart Connected Homes"; European Intelligence and Security Informatics Conference (EISIC), 2016, 172-175.

[2] Robles, R. J.; Kim, T.h.; Cook, D.; Das, S. "A Review on Security in Smart Home Development"; IJAST. 2010, 15, 14-29

[3] Saleh, E. ; Abou, A. "An IDS for Detection of Active Attacks Against Rouring in Mobile Ad-Hoc Networks"; Journal of advanced defence science and technology. 2010, 1, 15-22.

[4] Ashibani, Y.; Kauling, D.; Mahmoud, Q. H. "A Context-Aware Authentication Framework for Smart Homes"; IEEE 30th Canadian Conf. Electrical and Computer Eng. (CCECE). 2017, 1-5.

[5] Frank, M.; Biedert, R.; Ma, E.; Martinovic, I.; Song, D. "Touchalytics: On the Applicability of Touchscreen Input As A Behavioral Biometric for Continuous Authentication"; IEEE Trans. Inf. Forensics Security. 2012, 8, 136-148

[6] Song, T.; Li, R.; Mei, B.; Yu, J.; Xing, X.; Cheng, X. "A Privacy Preserving Communication Protocol for Iot Applications in Smart Homes"; IEEE Internet Things J 2017, 4, 1844-1852

[7] Vandana, C.; Imam, T.; Dubey, S. "Security Issues in Home Automation"; IJSRCSEIT. 2017

[8] Jeong, J.; Chung, M. Y.; Choo, H. "Integrated OTP-based User Authentication Scheme Using Smart Cards in Home Networks"; Proc. 41st Annual Hawaii Int. Conf. System Sciences (HICSS). 2008, 294-294.

[9] Vaidya, B.; Park, J. H.; Yeo, S.S.; Rodrigues, J. J. "Robust one-time Password Authentication Scheme Using Smart Card for Home Network Environment"; Comput Commu.n 2011, 34, 326-336

[10] Santoso, F. K. ; Vun, N. C. "Securing IoT for smart home system"; Int. Symposium on Consumer Electronics (ISCE). 2015, 1-2.

[11] Chang, C.-C. ; Le, H.D. "A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad Hoc Wireless Sensor Networks"; IEEE T Wirel Commun. 2015, 15, 357-366.

[12] Das, A. K.; Kumari, S.; Odelu, V.; Li, X.; Wu, F.; Huang, X. "Provably secure User Authentication and Key Agreement Scheme for Wireless Sensor Networks"; Secur Commun Netw. 2016, 9, 3670-3687.

[13] Wazid, M.; Das, A. K.; Odelu, V.; Kumar, N.; Susilo, W. "Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment"; IEEE Trans. Depend. Sec. Comput. 2017.

[14] Kumar, P.; Gurtov, A.; Iinatti, J.; Ylianttila, M.; Sain, M. "Lightweight and secure Session-Key Establishment Scheme in Smart Home Environments"; IEEE Sensors J. 2015, 16, 254-264.

[15] Li, Y. "Design of a Key Establishment Protocol for Smart Home Energy Management System"; Fifth Int. Conf. Comput. Intell. Commun. Syst. Netw. 2013, 88-93.

[16] Sierra, JM.; Hernández ,JC.; Alcaide, A.; Torres, J. "Validating the Use of BAN LOGIC"; Int. Conf. Comput. Sci. Appl. 2004,5, 851-858.

[17] Masoumi, M.; Mahdizadeh, H. "The FPGA Implementation of an Efficient Elliplic Curve Cryptographic Process over GF(2163)"; Advanced Defence Sci.& Tech., 2012, 3, 199-211.

[18] Naoui, S.; Elhdhili, M.E.; Saidane, L.A.; "Lightweight and Secure Password Based Smart Home Authentication Protocol: LSP-SHAP"; J NETW SYST MANAG. 2019, 4, 1020-1042.

[19] Shuai, M.; Yu, N.; Wang, H.; Xiong, L.; "Anonymous Authentication Scheme for Smart Home Environment Provable Security"; COMPUT SECUR. 2019, 132-146.

[20] Gurabi, M.A.; Alfandi, O.; Bochem, A.; Hogrefe, D.; "Hardware based Two-Factor User Authentication for the Internet of Things"; IWCMC.2018, 4, 1081-1086.

نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال یازدهم، شماره ۴، زمستان ۱۳۹۹؛ ص ۴۶۳-۴۵۱

«علمی- پژوهش»

طراحی یک حسگر زیستی جدید ضریب شکستی مبتنی بر بلورفوتونی مناسب جهت تشخیص DNA

یدالله شهامت[۱]، جواد خلیل‌زاده[۲*]، علی ریاحی[۱]

۱- پژوهشگر، ۲- دانشیار، دانشگاه جامع امام حسین (ع)

(دریافت: ۹۸/۱۰/۲۴، پذیرش: ۹۸/۱۲/۱۱)

چکیده

در این مقاله یک حسگر زیستی بلور فوتونی جدید جهت اندازه‌گیری ضریب شکست، پیشنهاد و مورد بررسی قرارگرفته است. سه ساختارِ تک، جفت و سه کاواکی طراحی و مطالعه شدند. در این ساختارها یک کاواک مرکزی به‌عنوان کاواک سنجش بین موج‌برهای ورودی و خروجی ساندویچ شده است. به‌منظور شبیه‌سازی و بررسی نحوه انتشار نور در ساختارها از روش تفاضل محدود در حوزه زمان و بسط موج تخت استفاده شده است. جذب مولکول‌های DNA موجود در محلول حسگری (PBS) منجر به تغییر در ضریب شکست مؤثر کاواک‌های سنجش شده و درنتیجه میزان عبوردهی طیفی از موج‌بر تغییر خواهد کرد. با بررسی میزان این تغییرات، فرآیند سنجش و تشخیص میسر می‌شود. با مطالعه اثر پارامترهای مختلف بر طیف خروجی ساختار، به‌منظور دستیابی به بهترین پارامترهای حسگری، مشاهده شد که پارامترهای هندسی ناحیه نقص و همچنین شعاع کاواک‌های کناری کاواک مرکزی، تأثیر قابل ملاحظه‌ای بر طیف ساختارها دارند. نتایج نشان دادند که ساختار تک‌کاواکی بیشینه حساسیت برابر با ۳۴۵ nm/RIU و ساختار سه کاواکی بیشینه فاکتور کیفیت برابر با ۵۳۱ را دارند. در مقایسه با ساختارهای قبلی انجام‌شده، ساختارهای پیشنهادی در این مقاله به نسبت کارایی به مراتب بهتری از خود نشان می‌دهند.

کلید واژه‌ها : بلور فوتونی، زیست حسگر، DNA.

Design of a New Refractive Index Bio-Sensor Based on Photonic Crystal Suitable for DNA Sensing

Y. Shahamat[1], J. Khalilzadeh, A. Riahi

Imam Hossein Comperehensive University

(Received: 14/01/2020; Accepted: 01/03/2020)

Abstract

In this paper, a novel biosensor based on the photonic crystal for refractive index measurements is proposed and investigated. Three designs, known as single-cavity structure, duble and triple-cavities structures, are designed and studies. All the structures were composed of a main hole as a ring resonator localized between the input and output waveguides. Two-dimensional finite-difference time domain and plane-wave expansion methods are employed to study the output power spectrum of the structures. By absorbing DNA molecules in the PBS solution, the refractive index of the sensing holes differ which results to the output transmission spectrum of the structure shift and hence, the sensing process occure. We study the impact of different parameters on the sensing of the structures. Results show that the sensitivity of the sensor depends mainly on the geometrical properties of the defect region of the photonic crystal structure. Results shows that the single cavity and triplet structures have the best sensitivity equal to 345nm/RIU and 531compared to the other proposed sensors, respectivelly.

Keywords: Photonic Crystal, Biosensor, DNA.

*Corresponding Author E-mail: jkhalil@ihu.ac.ir

۱. مقدمه

تروریسم زیستی موضوعی است که در دهه‌های اخیر توجه دولتمردان را به دلیل هراس و نگرانی ناشی از خسارت‌های جبران‌ناپذیری که حملات حوزه زیستی می‌توانند بر کشورها تحمیل کنند، به خود اختصاص داده است. آشکارسازی به کمک ساختارهایی موسوم به حسگرهای زیستی اولین و مهم‌ترین مرحله از سلسله مراحل اقدامات دفاعی در برابر این تهدیدات است. ساختارهای حسگری به خاطر ابعاد بسیار کوچکشان قادر به شناسایی، سنجش و ردیابی میکروارگانیسم‌ها، شناسایی باکتری‌ها، پروتئین‌ها، آنتی‌بادی‌ها، ویروس‌ها و سموم احتمالی در مواد غذایی، آب، خاک و هوا هستند [۴-۱]. از این حسگرها همچنین می‌توان به‌منظور تشخیص عواملی نظیر سارین، سومان و خردل برای جلوگیری از تماس و یا استشمام آن‌ها در مناطق عملیاتی و در صورت تشخیص حملات بیولوژیکی جهت جلوگیری انتشار بیماری‌های عفونی استفاده کرد.

در حالت کلی، یک حسگر زیستی شامل دو جزء گیرنده و مبدل هست. گیرنده وظیفه شناسایی و گزینش مولکول‌های هدف، و مبدل‌ها ساختارهایی به‌منظور تبدیل رویداد تشخیص مولکول‌های هدف به یک سیگنال قابل‌اندازه‌گیری توسط ادوات می‌باشند [۱]. تاکنون حسگرهای زیستی مختلفی با سازوکارهای عملکردی متفاوت توسط محققان ارائه شده‌اند [۸-۵]. در میان آن‌ها، حسگرهای زیستی نور-پایه به دلیل مزایایی همچون وزن ناچیز، قابلیت تکرارپذیری بالا، دقت بسیار بالا، مصونیت در برابر اثرات الکترومغناطیسی، مقاومت در برابر تغییرات دمایی محیط و سرعت پاسخ بالایی که دارند، مورد توجه ویژه هستند. این نوع حسگرها برخلاف دیگر حسگرهای زیستی که بیشتر بر اساس فلورسانس فرآیند تشخیص عوامل را انجام می‌دهند، نیازی به نشان‌دار کردن مولکول‌ها با مواد فلورسنتی نظیر رنگ را ندارند. در واقع عمل تشخیص و سنجش توسط این حسگرها، بر اساس اندازه‌گیری و بررسی تغییرات ضریب شکست اپتیکی ناحیه سنجش ناشی از فعل و انفعالات مولکولی بوده که در آن ناحیه انجام می‌گیرد. به بیانی دیگر، با اتصال مولکول‌های زیستی به دیواره‌های ناحیه سنجش، مشخصات طیف خروجی ساختار به خاطر تغییرات ایجاد شده در ضریب شکستِ محیط سنجش تغییر کرده و از این طریق عملِ تشخیص صورت می‌گیرد. لازم به ذکر است که دیواره‌ها از قبل توسط گیرنده‌های گزینش کننده هدف پوشش داده می‌شوند. تغییرات حاصل‌شده در نور عبوری از ساختار می‌تواند شامل تغییر در طول‌موج، شدت و یا تغییر در فاز باشد. بر همین اساس، سازوکار و روش‌های حسگری مختلفی برای حسگرها تعریف می‌شوند. این روش‌ها عبارت‌اند از: ۱- روش طیفی: در این روش با اندازه‌گیری میزان جابه‌جایی طیف طول‌موجی ساختار، شامل عبوردهی، بازگشتی و یا جذبی، ماده مجهول شناسایی می‌شود. ۲- روش شدتی: در این روش طول‌موج نور فرودی ثابت بوده و با اندازه‌گیری میزان تغییرات درشدت نور خروجی در آن طول‌موج، شناسایی ماده مجهول صورت می‌گیرد. ۳-روش فازی: در این روش با اندازه‌گیری اختلاف‌فاز میان مدهای TM و TE نور فرودی، تشخیص و شناسایی ماده هدف صورت می‌گیرد. در چند سال اخیر زیست حسگرهای نوری متنوعی، نظیر حسگرهای فیبری [۹]، حسگرهای مبتنی بر مشددها [۱۰]، حسگرهای مبتنی بر تشدید پلاسمون سطحی [۱۱]، حسگرهای بلور فوتونی [۱۲] و غیره بر اساس این روش‌ها ارائه شده است [۱۸-۱۳]. در میان حسگرهای اشاره‌شده، حسگرهای مبتنی بر بلورهای فوتونی به خاطر دقت و حساسیت بالا، فرآیند ساخت نسبتاً آسان، قابلیت مجتمع شدن بر روی تراشه‌های مجتمع، تلفات نوری ناچیز و توانایی سنجش از راه دور مورد توجه خاص محققان قرارگرفته‌اند.

در حالت کلی می‌توان گفت بلورهای فوتونی در سه حالتِ یک، دو و سه‌بعدی طراحی و ساخته می‌شوند [۱۲]. در یک بلور فوتونی یک‌بعدی ضریب شکست محیط به‌صورت تناوبی در یک راستا و در حالت دو و سه‌بعدی نیز به ترتیب در دو و سه راستا تغییر می‌کند. از جمله خواص مهم چنین ساختارهایی وجود ناحیه‌ای موسوم به باند فوتونی در آن‌ها است. شکاف باند فوتونی به محدوده طول‌موجی گفته می‌شود که در آن محدوده هیچ فوتونی امکان عبور از ساختار را ندارد. این خاصیت این امکان را برای کاربر فراهم می‌کند تا بتواند نور را باکیفیت بالا در مکان‌هایی موسوم به نقص‌های نقطه‌ای محدود کرده و یا به‌اصطلاح گیر اندازد. علاوه بر محدودسازی انرژی در نقص‌های نقطه‌ای، هدایت آسانِ نوری که طول‌موجش در شکاف باند فوتونی بلور قرار دارد، بدون پخش‌شدگی در بلور، از طریق یک نقص خطی در بلور امکان‌پذیر است [۱۶]. امکان دسترسی به‌سرعت گروه پایین، قابلیت انعطاف‌پذیری خوب در شکل و ابعاد و همچنین امکانِ پیاده‌سازی آسان ساختارهای بلور فوتونی از طریق فن‌آوری مدارات مجتمع نوری سیلیکون-پایه از دیگر ویژگی‌های بلورهای فوتونی به شمار می‌روند [۱۶].

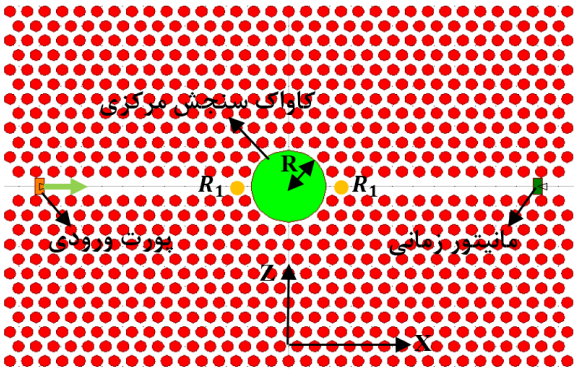
امروزه طراحی نقص‌های نقطه‌ای باقابلیت محدودسازی بالا و نیز هدایت و انتقال نور با تلفات ناچیز از طریق نقص‌های خطی، امکان طراحی و ساخت حسگرهایی با ویژگی‌های حسگری بالا را فراهم کرده است. بر همین اساس، در چند سال اخیر حسگرهای زیستی متنوعی مبتنی بر نقص‌های نقطه‌ای طراحی‌شده است [۲۵-۱۹]. به‌عنوان‌مثال در سال۲۰۱۶، اولیایی و همکارانش یک ساختار حسگری مبتنی بر بلور فوتونی با حساسیت

۲۷۲/۴۳nm/RIU و فاکتور کیفیت ۳۰۰۰ ارائه دادند [۲۶]. ساختار آن‌ها شامل یک نقص نقطه‌ای بود که در مسیر موجبر اصلی از کنار به آن تزویج شده بود. حسگر بلور فوتونی دیگری در سال ۲۰۱۸، توسط دانایی و همکارش ارائه شد [۲۷]. حساسیت و فاکتور کیفیت حسگر آن‌ها به ترتیب ۷۲۰nm/RIU و بین ۲۵ تا ۳۰ گزارش‌شده است.. یک سال بعد، رحمان زاده و همکارانش حسگر بلور فوتونی دیگری ارائه دادند [۲۸]. حساسیت و فاکتور کیفیت حسگر آن‌ها به ترتیب ۳۰۰nm/RIU و ۴۱۸ گزارش‌شده است. اخیراً هم حسگر دیگری مبتنی بر بلور فوتونی توسط بنمرخی و همکارانش با حساسیت ۲۹۲/۴۶ nm/RIU و فاکتور کیفیت حدود ۴۹۷۶۷ گزارش شده است [۲۹]. حسگرهای متعدد دیگری در سال‌های بعد توسط محققان ارائه شده است [۳۰-۳۵].

ما در این مقاله با به‌کارگیری تشدیدگر در بلور فوتونی دوبعدی، یک حسگر زیستی جدید با حساسیت و فاکتور کیفیت بالا ارائه کرده‌ایم. حسگر زیستی معرفی‌شده بر پایه یک کاواک اصلی سنجش است که در بستری از سیلیکون ایجادشده است. با پیوند مولکول‌های DNA مجهول و مولکول‌های DNA سنجشی، ضریب شکست محیط آنالایت تغییر کرده و درنتیجه طول‌موج تشدید جابه‌جا می‌شود. با اندازه‌گیری تغییرات در طیف خروجی ساختار، عمل سنجش و شناسایی عامل انجام می‌گیرد.

۲. معرفی ساختار و پارامترهای حسگری

شکل (۱) شمای پایه حسگر طراحی‌شده را نمایش می‌دهد. این حسگر از زیر لایه سیلیکونی تشکیل شده است که در آن سوراخ‌های هوا با ضریب شکست واحد و شعاع ۰/۳۵a در آرایشی مثلثی ایجاد شده‌اند (a معرف ثابت شبکه است). در این حسگر از دو نقص خطی یکسان به‌عنوان موجبر جهت هدایت نور استفاده شده است. این دو موجبر توسط یک کاواک (نقص) به شعاع R (کاواک سبزرنگ) به همدیگر ارتباط پیدا کرده‌اند. این کاواک نقش کاواک سنجش جهت شناسایی مولکول‌های آنالایت را دارد. ضریب شکست ماده درون کاواک با نماد n نمایش داده می‌شود. به‌منظور تحریک ساختار از یک پالس زمانی با پوش گوسی استفاده شده است که از ابتدای موجبرِ سمت چپ به‌عنوان موجبر ورودی به ساختار تابانده می‌شود. این نور از طریق موجبر به کاواک سنجش رسیده و بعد از تحریک و تشدیدِ آن، به موجبر سمت راست که به‌عنوان موجبر خروجی در نظر گرفته‌شده است منتقل می‌شود. توان نور خروجی توسط یک پایشگر[1] زمانی که در انتهای موجبر سمت راست قرار داده شده است اندازه‌گیری می‌شود. به‌منظور تزویج بهتر نور به کاواک سنجش و افزایش توان نور انتقال داده‌شده به موجبر خروجی، نقص‌های نقطه‌ای با شعاع R_1 در مسیر موجبرها قرار داده شده است (حفره‌های نارنجی‌رنگ).



شکل ۱. ساختار حسگر تک کاواکی مبتنی بر نانو تشدیدگر. در این ساختار موجبر سمت چپ به‌عنوان موجبر ورودی و موجبر سمت راست به‌عنوان موجبر خروجی در نظر گرفته شده‌اند. ماده موردنظر جهت شناسایی درون ناحیه تشدیدگر (ناحیه سبزرنگ) قرار می‌گیرد.

اساس حسگری ساختار پیشنهاد شده بر اساس اندازه‌گیری تغییرات ایجادشده در طیف نور خروجی از موجبر نسبت به تغییر ضریب شکست کاواک سنجش ناشی از اتصال مولکول‌های هدف به دیواره‌های درونی آن هست. با اندازه‌گیری این تغییرات، ماده هدف شناسایی خواهد شد. به‌منظور بررسی کارایی ساختار، پارامتر حساسیت (S) با معادله

$$S = \frac{\Delta\lambda_{res}}{\Delta n_{Analyte}} (nm / RIU) \qquad (۱)$$

تعریف می‌شود، که در آن، $\Delta\lambda_{res}$ معرف میزان جابه‌جایی طیف ساختار برای حالتی است که ضریب شکست محیط آنالایت به‌اندازه $\Delta n_{Analyte}$ تغییر کرده باشد. در این مقاله از بسط موج تخت موسوم به PWE[2] برای محاسبه شکاف باند فوتونی بلور و از روش تفاضل محدود در حوزه زمان[3] (FDTD) برای بررسی نحوه انتشار موج الکترومغناطیسی در ساختارهای پیشنهادی استفاده شده است. با توجه به دوبعدی بودن ساختار پیشنهادی، شبیه‌سازی‌های صورت گرفته در دو بعد با مش بندی‌های $\Delta x = \Delta z = 10$ nm انجام گرفته است. Δx و Δz به ترتیب گام‌های مکانی در امتداد محور x و z هستند. گام زمانی Δt با در نظر گرفتن شرط پایداری برنامه موسوم به‌شرط کوری مطابق رابطه (۲) لحاظ شده است [۳۸-۳۶].

[1] Monitor

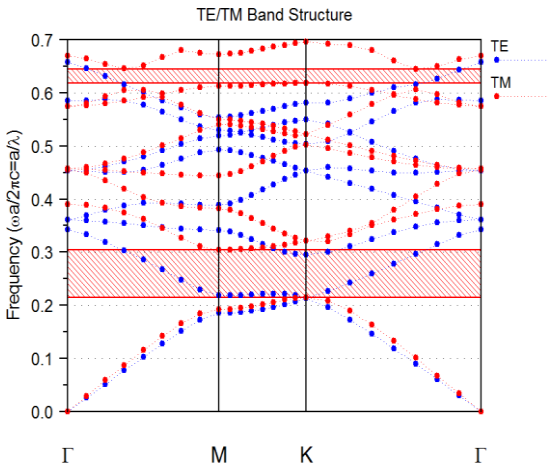
[2] Plane-Wave Expansion
[3] Finite-Difference Time-Domain

$$\Delta t \le \frac{1}{c}\sqrt{\Delta x^2+\Delta z^2} \qquad (۲)$$

که در آن c سرعت نور در فضای آزاد است. در انتها لازم است اشاره‌کنیم که ما در این مقاله برای شبیه‌سازی ساختارهای پیشنهادی از نرم‌افزار فوتونیکی Rsoft استفاده کرده‌ایم که در آن از ماژول BandSOLVE برای محاسبه گاف نوار و از ماژول FullWave برای محاسبه طیف خروجی استفاده شده است. همچنین لازم است اشاره شود که در این بسته نرم‌افزاری لازم است شرط پایداری رفتار طیفی ساختار مطابق با رابطه (۲) ارضاء گردد که این مهم همواره هنگام انجام شبیه‌سازی رعایت شده است.

۲-۱. گاف فوتونی

شکل (۲) ساختار گاف نواری بلور فوتونی کامل، وقتی هیچ نقصی در بلور فوتونی ایجاد نشده است، را برای دو مد TE (خطوط آبی) و TM (خطوط قرمز) نشان می‌دهد. مد TE معرف حالتی است که در آن میدان الکتریکی در امتداد محور کاواک‌های هوا (عمود بر صفحه) و مد TM حالتی است که در آن میدان مغناطیسی موج فرودی در امتداد محور کاواک‌ها قرار دارد.



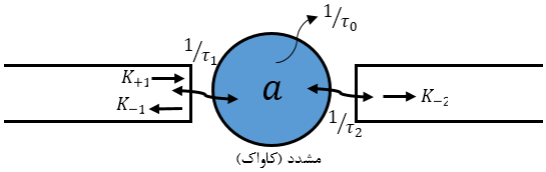
شکل ۲. گاف نوار فوتونی ساختار کامل متشکل از کاواک‌های هوا به شعاع ۰/۳۵a در یک بستر سیلیکونی برای دو مد TE (منحنی‌های آبی‌رنگ) و TM (منحنی قرمزرنگ).

همان‌طور که مشاهده می‌شود، ساختار پیشنهادی برای مد TE هیچ گافی ندارد، درحالی‌که برای مد TM دو ناحیه گاف بین نوارهای صفر و یک در بازه پهن بهنجار شده $(\omega a/2\pi c)$ (۰/۲۲۲ تا ۰/۳۳۱) و نوارهای چهار و پنج در یک بازه باریک (۰/۴۶۹ تا ۰/۶۶۵) وجود دارد. با توجه به اینکه در طراحی حسگرهای مبتنی بر بلورهای فوتونی، ما به دنبال انتقال نور از طریق موج‌برها (به‌عنوان نقص‌های خطی) هستیم، لذا باید مدی را برای منبع نور فرودی انتخاب کنیم که ساختار برای آن مد دارای گاف فوتونی باشد، زیرا تنها در این صورت است که بعد از تحریکِ درگاه ورودیِ حسگر، نور به درون ساختار نشت نکرده و در مسیر موج‌بر منتشر می‌شود. بر این اساس، در ادامه منبع تحریک‌کننده‌ای که دارای مد TM است را به‌عنوان منبع ورودی در نظرخواهیم گرفت. همچنین با توجه به کارکرد حسگر در محدوده فیبرهای مخابراتی ۱۵۵۰ نانومتر، ثابت شبکه برابر با ۴۲۰/۰۵ نانومتر در نظر گرفته شده است.

۲-۲. مدل‌سازی

به‌منظور تحلیل طیف خروجیِ حسگر، رفتار ساختار پایه نمایش داده‌شده در شکل (۱) به کمک نظریه مدهای جفت‌شده(CMT) [1] مدل‌سازی شد. مطابق مدل شکل (۳) ساختار نمایش داده‌شده در شکل (۱) را می‌توان به‌صورت دو موج‌بر مستقیم که توسط یک مشدد یا کاواک به همدیگر ارتباط پیداکرده‌اند در نظر گرفت. وقتی ورودی ساختار توسط یک منبع گوسی تحریک می‌شود، بخشی از این نور که دارای فرکانسی برابر با فرکانس تشدید کاواک است از کاواک عبور کرده و به درگاه خروجی موج‌بر سمت راست منتقل می‌شود. مابقی نور که دارای فرکانسی غیر از فرکانس تشدید کاواک است، بعد از رسیدن به کاواک، از آن منعکس‌شده و به درگاه ورودی برمی‌گردد. حال با فرض اینکه $1/\tau_1$ و $1/\tau_2$ به ترتیب نرخ تزویج نور از موج‌بر ورودی به کاواک و از کاواک به موج‌بر خروجی باشند، آنگاه تحول زمانی دامنه مد بهنجارشده درون کاواک (a) به‌صورت رابطه (۳) خواهد بود.

$$\frac{da}{dt} = (-i\omega_0 - \frac{1}{\tau_0} - \frac{1}{\tau_1} - \frac{1}{\tau_2})a + e^{-i\theta}\sqrt{\frac{2}{\tau_1}}K_{+1} \qquad (۳)$$



شکل ۳. مدل نظری زیست حسگر تک کاواکی، $1/\tau_1$ و $1/\tau_2$ به ترتیب نرخ تزویج نور از موج‌بر ورودی به کاواک و از کاواک به موج‌بر خروجی می‌باشند. $1/\tau_0$ نیز نرخ تلفات نور در کاواک است.

در رابطه (۳)، $1/\tau_0$ نرخ تلفات نور در کاواک، θ و ω_0 نیز به ترتیب فاز نور تزویج شده از کاواک به موج‌بر و فرکانس تشدید کاواک هستند. با توجه به‌رابطه (۳) خواهیم داشت:

$$K_{+1} = \frac{-i(\omega-\omega_0)+\frac{1}{\tau_0}+\frac{1}{\tau_1}+\frac{1}{\tau_2}}{e^{-i\theta}\sqrt{\frac{2}{\tau_1}}}a \qquad (۴)$$

[1] Coupled Mode Theory

پایستگی انرژی در سیستم ایجاب می‌کند که

$$K_{-2}=\sqrt{\frac{2}{\tau_2}}e^{+i\theta'}a \qquad (۵)$$

باشد. با حل معادلات (۳) تا (۵)، ضریب عبور نور از موجبر سمت راست (ξ_{trans}) به‌صورت رابطه (۶) به‌دست خواهد آمد:

$$\xi_{trans}=\frac{\sqrt{\frac{2}{\tau_2}\times\frac{2}{\tau_1}}e^{+i(\theta'-\theta)}}{-i(\omega-\omega_0)+\frac{1}{\tau_0}+\frac{1}{\tau_1}+\frac{1}{\tau_2}} \qquad (۶)$$

در این صورت میزان عبور که برابر با مزدوج مختلط ضریب عبور است، به‌صورت

$$T=\frac{\frac{4}{\tau_1\tau_2}}{(\omega-\omega_0)^2+(\frac{1}{\tau_0}+\frac{1}{\tau_1}+\frac{1}{\tau_2})^2} \qquad (۷)$$

خواهد بود. با توجه به متقارن بودن کاواک $\frac{1}{\tau_2}=\frac{1}{\tau_1}=\frac{1}{\tau}$ است و با توجه به آن میزان عبور به رابطه (۸) کاهش پیدا می‌کند.

$$T=\frac{(\frac{2}{\tau})^2}{(\omega-\omega_0)^2+(\frac{1}{\tau_0}+\frac{2}{\tau})^2} \qquad (۸)$$

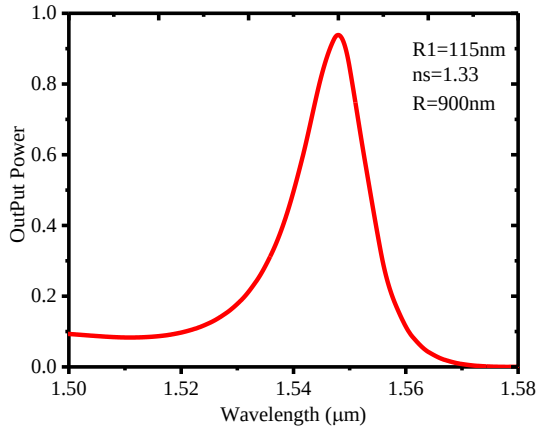
همان‌طور که مشاهده می‌شود بیشینه مقدار عبور در حالت تشدید یعنی: $\omega=\omega_0$ رخ خواهد داد. این مقدار با فرض تلفات ناچیز ($1/\tau_0 \sim 0$) برابر با واحد می‌شود. طول موج تشدید (معادل فرکانس تشدید کاواک (ω_0)) نیز از رابطه تقریبی (۹) به‌دست خواهد آمد.

$$\frac{2\pi}{\lambda_{res}}n_{eff}\times 2L_{eff}+\varphi_r=2m\pi \qquad (۹)$$

که در آن L_{eff} طول مؤثر کاواک و m اعداد صحیح هستند. بر طبق این رابطه، طول‌موج تشدید به پارامترهای هندسی کاواک نظیر طول مؤثر آن و ضریب شکست اپتیکی ماده درون آن وابسته است. به همین جهت، در ادامه، بعد از بررسی نتایج اولیه ساختار تک کاواکی، اثر پارامترهای هندسی مربوط به کاواک سنجش بر روی عبور دهی طیفی ساختار بررسی می‌شود.

۳. شبیه‌سازی ساختار تک کاواکی

در انجام شبیه‌سازی ابتدا کارایی حسگر پیشنهادی از طریق محاسبه طیف خروجی با استفاده از ماژول FullWave مربوط به نرم‌افزار Rsoft مورد بررسی قرار گرفت. این ماژول با حل معادلات ماکسول به کمک روش FDTD، قادر است رفتار نور در نانو ساختارها را شبیه‌سازی کند. شکل (۴) عبوردهی طیفی موجبر خروجی (توان عبوری بهنجارشده از موجبر خروجی) را برای مد TM نشان می‌دهد. در این نمودار، شعاع کاواک مرکزی ۹۰۰ nm، شعاع دو کاواک همسایه آن ۱۱۵ nm و ضریب شکست ماده داخل کاواک ۱/۳۳ در نظر گرفته‌شده است. مطابق این شکل، عبوردهی، قله‌ای تیز به مقدار ۰/۹۴ در طول‌موج ۱/۵۴۸ µm با پهنای ۱۳ nm دارد. این قله معرف طول‌موج ۱/۵۴۸ µm به عنوان طول موج تشدید کاواک است. ضریب کیفیت ($QF=\frac{\lambda_{res}}{FWHM}$) برای این قله برابر با ۱۱۹/۰۷ است، که در آن FWHM معرف تمام پهنای طیفی در نیم بیشینه است. با انطباق[1] نمودار شکل (۴)، مطابق جدول (۱)، نرخ تزویج نور از موجبر ورودی به کاواک، از کاواک به موجبر خروجی و نرخ تلفات نور در کاواک به ترتیب برابر با مقادیر ۷/۵۳۷، ۷/۵۳۷ و ۰/۵۰۶گیگاهرتز به‌دست آمدند.



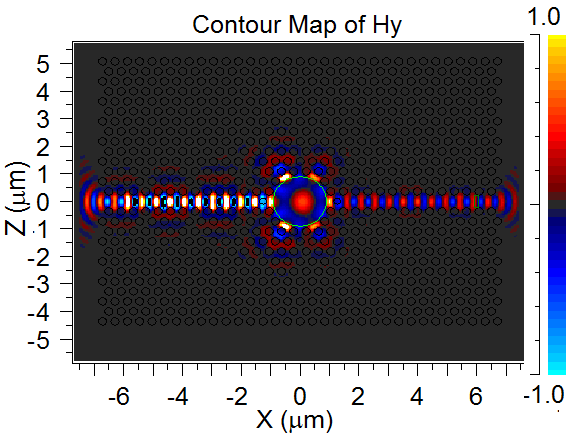
شکل ۴. عبوردهی طیفی از ساختار تک کاواکی پیشنهادشده

جدول ۱. مقادیر مربوط به نرخ تزویج نور از موجبر ورودی به کاواک، از کاواک به موجبر خروجی و نرخ تلفات نور در کاواک.

پارامتر	مقدار بر حسب گیگاهرتز
$1/\tau_1$	۷/۵۳۷
$1/\tau_2$	۷/۵۳۷
$1/\tau_0$	۰/۵۰۶

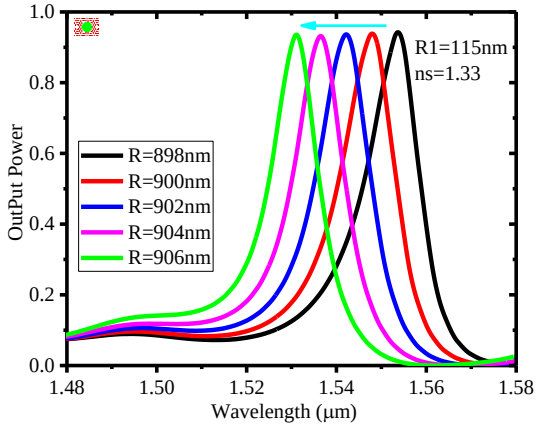
نمایه[2] میدان مغناطیسی در طول‌موج تشدید ۱/۵۴۸ µm برای مد TM در شکل (۵) نشان داده شده است. همان‌طور که مشاهده می‌کنیم در این طول‌موج، نور در کاواک تشدید شده به سمت خروجی هدایت می‌شود. ضریب شکست محیط نمونه در این حالت ۱/۳۳ در نظر گرفته شده است.

[1] Fit
[2] Profile



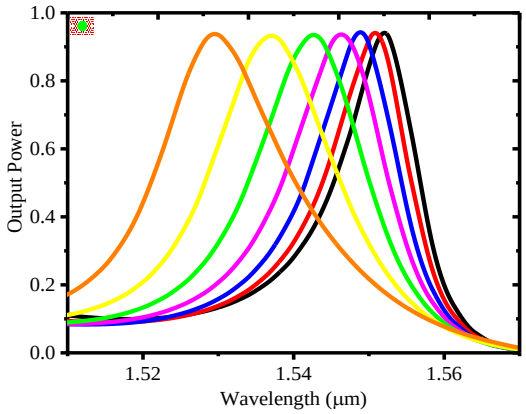
شکل ۵. نمایه میدان مغناطیسی در ساختار تک کاواکی در طول‌موج تشدید ۱/۵۴۸ μm برای مد TM.

مطابق رابطه (۹)، شعاع کاواک مرکزی (R) (که متناسب با طول موثر کاواک است) از طریق تأثیر بر اندازه راه نوری می‌تواند بر مشخصات طیفی ساختار تأثیرگذار باشد. لذا در ادامه به‌منظور بررسی میزان اثرگذاری این پارامتر و همچنین بهبود پارامترهای حسگری، اثر شعاع کاواک و کاواک‌های کناری آن (R_1) بر طیف ساختار بررسی شدند. شکل (۶) عبوردهی طیفی را برای شعاع‌های کاواک سنجش: ۸۹۸، ۹۰۰، ۹۰۲، ۹۰۴ و ۹۰۶ نانومتر نشان می‌دهد. همان‌طور که مشاهده می‌شود با افزایش شعاع کاواک، طول‌موج تشدید به سمت مقادیر کمتر جابجا می‌شود. این در حالی است که مقدار عبور تغییر قابل ملاحظه‌ای ندارد. نتیجه حاصل شده در توافق با رابطه نظری (۹) است. مطابق این رابطه، با افزایش شعاع (ودر نتیجه طول موثر) کاواک، راه نوری کاهش می‌یابد. در واقع افزایش شعاع کاواک باعث جابجایی گاف انرژی به فرکانس های بالاتر می‌شود. به عبارت دیگر با افزایش شعاع کاواک طول‌موجی که می‌تواند از کاواک عبور کند به طول‌موج های پایین منتقل می‌شود مطابق شکل (۶)، با افزایش شعاع از ۸۹۸ nm به ۹۰۶ nm، طول‌موج تشدید از ۱/۵۵۳ μm به ۱/۵۳۱ μm کاهش پیدا می‌کند.



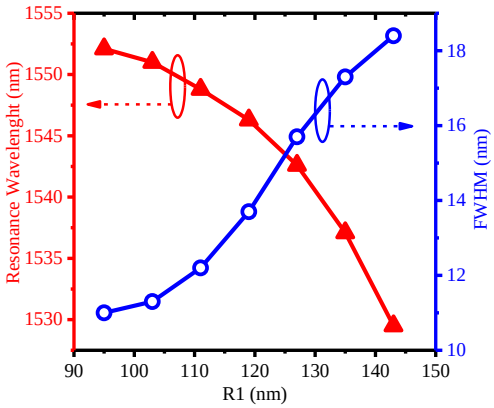
شکل ۶. عبوردهی طیفی ساختار تک کاواکی برای شعاع‌های مختلف مشدد (R).

شکل (۷) عبوردهی طیفی ساختار را برای شعاع‌های مختلف کاواک‌های جانبی از ۹۵ nm تا ۱۴۳ nm برای شعاع ۹۰۰ nm کاواک سنجش نشان می‌دهد. با افزایش شعاع کاواک‌ها، طول‌موج تشدید به‌سمت مقادیر کمتر جابجا می‌شود. این نتیجه نیز مطابق استدلال قبلی برای شکل(۶) قابل توجیه است.



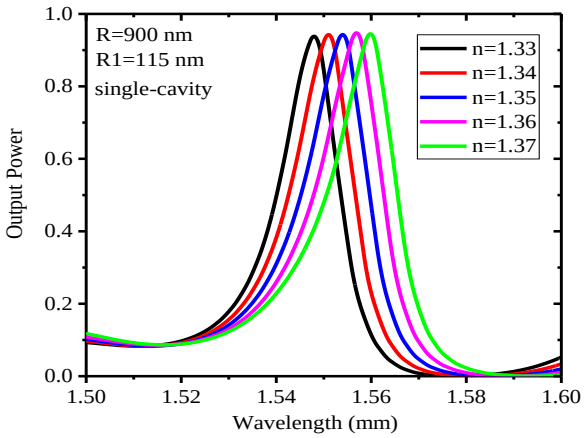
شکل ۷. عبوردهی طیفی ساختار تک کاواکی برای شعاع‌های مختلف کاواک‌های کناری کاواک. در این شکل منحنی‌های سیاه، قرمز، آبی، صورتی، سبز، زرد و نارنجی به ترتیب مربوط به شعاع (R1) های ۹۵، ۱۰۳، ۱۱۱، ۱۱۹، ۱۲۷، ۱۳۵ و ۱۴۳ نانومترند. ضمناً شعاع کاواک سنجش ۹۰۰ nm در نظر گرفته‌شده است.

مطابق شکل (۸)، با افزایش شعاع R_1 از ۹۵ nm به ۱۴۳ nm، طول‌موج تشدید از ۱/۵۵۲ μm به ۱/۵۲۹ μm کاهش پیدا می‌کند. پهنای طیف خروجی نیز از ۱۱ nm به ۱۸/۵ nm افزایش می‌یابد.



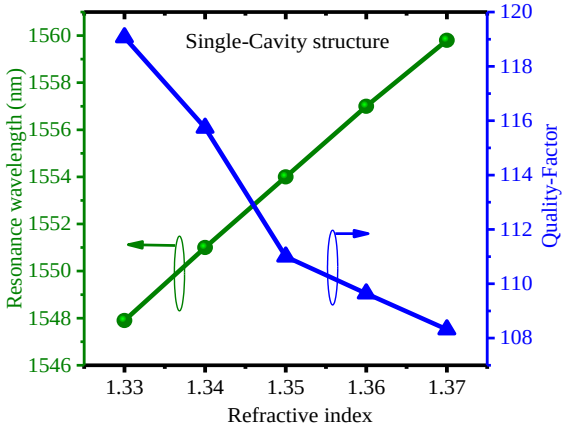
شکل ۸. طول‌موج تشدید (منحنی قرمز) و پهنای عبوردهی طیفی (منحنی آبی) برای مقادیر مختلف شعاع کاواک‌های کناری کاواک سنجش (R_1). شعاع کاواک سنجش ۹۰۰ nm در نظر گرفته شده است.

عبوردهی طیفی ساختار برای ضرایب شکست مختلف (۱/۳۳، ۱/۳۴، ۱/۳۵، ۱/۳۶ و ۱/۳۷) آنالایت در شکل (۹) نشان داده شده است. مطابق این شکل، با افزایش ضریب شکست محیط درون کاواک، طول موج تشدیدی به سمت مقادیر بیشتر شیفت پیدا می‌کند. میزان عبور نیز چندان تغییر نمی‌کند.



شکل ۹. عبوردهی طیفی ساختار تک کاواکی برای مقادیر مختلف ضریب شکست آنالایت.

با تغییر ضریب شکست آنالایت درون کاواک سنجش از ۱/۳۳ به ۱/۳۷، طول‌موج تشدید از ۱/۵۴۸μm به‌صورت خطی به مقدار ۱/۵۵۹۸μm افزایش می‌یابد. این در حالی است که ضریب کیفیت، همانطور که در شکل (۱۰) نشان داده شده است، روند کاهشی دارد. بهعبارت دیگر با افزایش ضریب شکست ماده درون کاواک، طیف خروجی پهن‌تر می‌شود. برای چنین ساختاری مقدار حساسیت برابر با $295\ nm.RIU^{-1}$ به‌دست آمد.

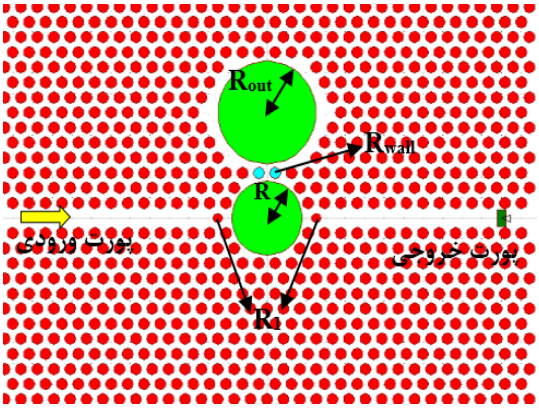


شکل ۱۰. طول‌موج تشدید (منحنی سبز رنگ) و فاکتور کیفیت (منحنی آبی) ساختار تک کاواکی برای مقادیر مختلف ضریب شکست آنالایت درون کاواک سنجش مرکزی. برای این ساختار شعاع کاواک‌های کناری کاواک ۱۱۵ nm لحاظ شده‌اند.

همچنین با تغییر ضریب شکست ماده درون کاواک سنجش، به‌ازای شعاع‌های مختلف کاواک‌های کناری (R_1)، مشاهده شد که بیشترین حساسیت برابر با ۳۴۵ nm/RIU برای شعاع ۱۰۳nm حاصل می‌شود.

۴. شبیه‌سازی ساختار دو کاواکی

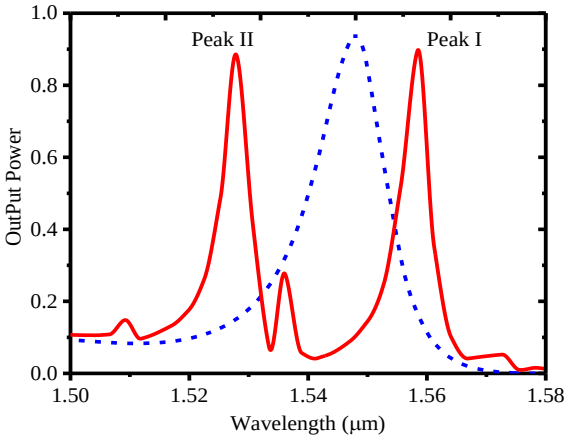
در این شبیه‌سازی به‌منظور افزایش پارامترهای حسگری، ساختار دوم شامل دو کاواکِ مستقیماً تزویج شده باهم (موسوم به ساختار دو کاواکی) مطابق شکل (۱۱) طراحی و مورد بررسی قرار گرفت. در این ساختار، شعاع کاواک دوم R_{out} و شعاع کاواک‌های دیواره مشترک دو کاواک (کاواک‌های آبی‌رنگ) با R_{wall} نمایش داده شده‌اند. نور بعد از ورود به کاواک اول در صورت داشتن شرایط لازم می‌تواند از طریق کاواک‌های مشترک به کاواک دوم تزویج شده و در نتیجه طول راه نوری درماده افزایش می‌یابد. با این افزایش انتظار می‌رود پارامترهای حسگری نیز بالا رود.



شکل ۱۱. ساختار دو کاواکی حسگر زیستی پیشنهاد شده.

شکل (۱۲) عبوردهی طیفی موج‌بر خروجی ساختار دو کاواکی را برای شعاع کاواک مرکزی ۹۰۰nm، شعاع کاواک‌های کناری ۱۱۵ nm و شعاع کاواک بیرونی (R_{out}) ۱۲۰۷ nm نشان می‌دهد. شعاع کاواک‌های آبی‌رنگ (R_{wall}) نیز برابر با ۱۳۸ nm بوده و ضریب شکست ماده داخل کاواک‌ها ۱/۳۳در نظر گرفته شده است. همان‌طور که مشاهده می‌شود قله‌ای که قبلاً برای ساختار تک کاواکی (نمودار آبی‌رنگ شکل (۱۲)) وجود داشت در این حالت به یک دره تبدیل شده است. علت چنین رویدادی را در اختلاف راه نوری باید جست. درواقع با اضافه کردن کاواک دوم به ساختار تک کاواکی، به‌عنوان مثال، نوری با طول‌موج ۱/۵۴۸μm بعد از تشدید در کاواک اول از طریق کاواک‌های واقع در مرز مشترک به کاواک دوم نشت خواهد کرد. در صورتی‌که این نور بتواند در آن کاواک تشدید شود راه نوری معادل π رادیان دیگر را تجربه خواهد کرد. به‌بیان‌دیگر، نور در کل مسیر مواجهه با جفت کاواک‌ها اختلاف فاز 3π رادیان پیدا خواهد کرد. وجود چنین اختلاف‌فازی، باعث خواهد شد که نور اجازه عبور از ساختار را نداشته باشد. به همین دلیل، قله ساختار قبلی برای چنین ساختاری به دره تبدیل می‌شود. علاوه بر این‌ها، به‌طور هم‌زمان دو قله جدید (در دو طرف قله قبلی) در

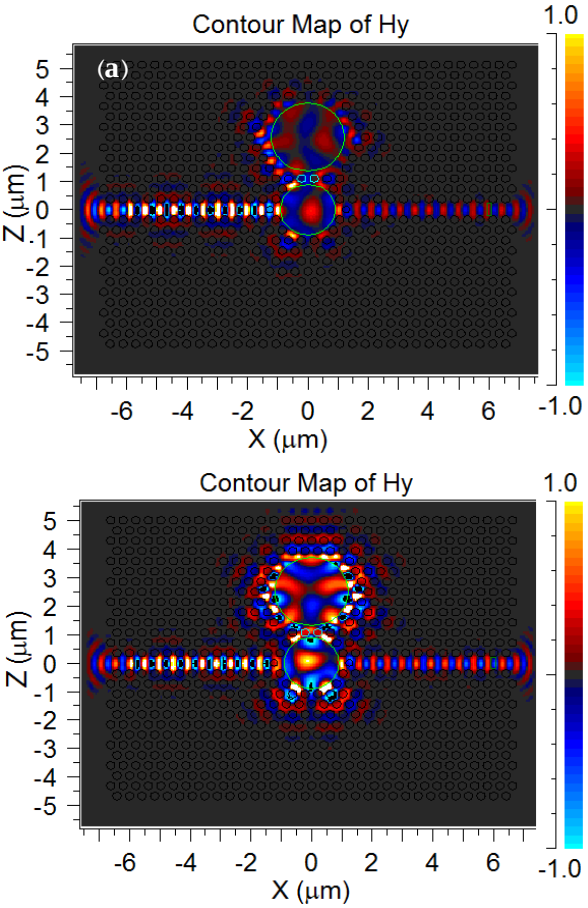
طول‌موج‌های ۱/۵۵۸ µm و ۱/۵۲۷۸ µm طیف ساختار دو کاواکی به‌وجود آمده‌اند. مزیت اصلی ساختار دو کاواکی نسبت به ساختار قبلی این است که اگرچه میزان عبور در طول‌موج‌های تشدید آن‌ها تفاوت محسوسی باهمندارد اما پهنای طیفی ساختار دو کاواکی به طور قابل ملاحظه‌ای نسبت به ساختار تک کاواکی کاهش یافته است. این مزیت موجب حسگری بهتر ساختار دو کاواکی می‌شود.



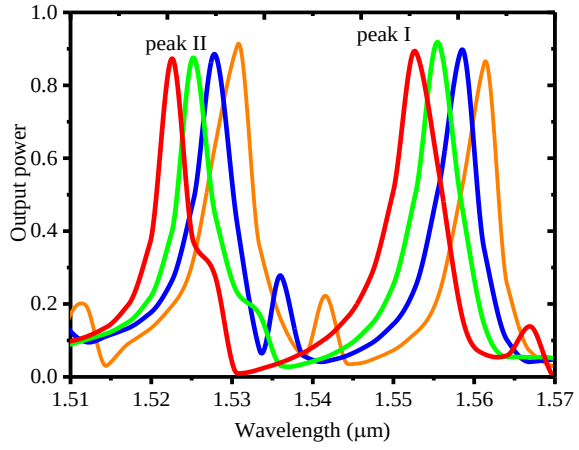
شکل ۱۲. عبوردهی طیفی ساختار دو کاواکی (منحنی قرمز رنگ) و ساختار تک کاواکی (منحنی آبی خط‌چین). در این نمودار شعاع کاواک مرکزی ۹۰۰ nm، کاواک بیرونی ۱۲۰۷ nm و شعاع کاواک‌های کناری کاواک مرکزی ۱۱۵ nm می‌باشند.

نمایه میدان‌های مغناطیسی در طول‌موج‌های مربوط به قله‌های ۱ و ۲ به‌ترتیب در شکل‌های (۱۳-الف) و (۱۳-ب) نشان داده شده است. همان‌طور که مشاهده می‌شود در این طول‌موج‌ها، نور با کاواک‌ها تداخل سازگار داشته و درنتیجه به سمت خروجی هدایت می‌شود.

شعاع کاواک بیرونی یکی از پارامترهای مهم است که می‌تواند بر وقوع تشدید تاثیرگذار باشد. بنابراین اثر آن بر طیف ساختار دوکاواکی بررسی شد. شکل (۱۴) عبوردهی طیفی ساختار با شعاع ۹۰۰ nm کاواک مرکزی و شعاع‌های مختلف کاواک بیرونی (از ۱۲۰۳ nm تا ۱۲۱۳ nm) را نشان می‌دهد. ضریب شکست ماده آنالایت در اینجا ۱/۳۳ در نظر گرفته شده است. نتایج بدست آمده نشان می‌دهند که با افزایش شعاع کاواک، طول‌موج‌های متناظر با قله‌های ۱و۲ به‌طور هم‌زمان به‌سمت مقادیر کمتر جابجا می‌شوند. خلاصه میزان این تغییرات در جدول ۲ ارائه شده است. مطابق این جدول، با افزایش شعاع R_{out} از ۱۲۰۳nm تا ۱۲۱۳nm، طول‌موج تشدید متناظر با قله۱ (قله۲) از ۱۵۶۱/۳ nm (۱۵۳۰/۸ nm) به ۱۵۵۲/۷ nm (۱۵۲۲/۶ nm) کاهش می‌یابد.



شکل ۱۳. نمایه میدان‌های مغناطیسی در طول‌موج‌های (الف) ۱/۵۴۸۰µm و (ب) ۱/۵۲۷۸µm به‌ترتیب متناظر با قله‌های ۱ و ۲ شکل(۱۲) برای مد TM.

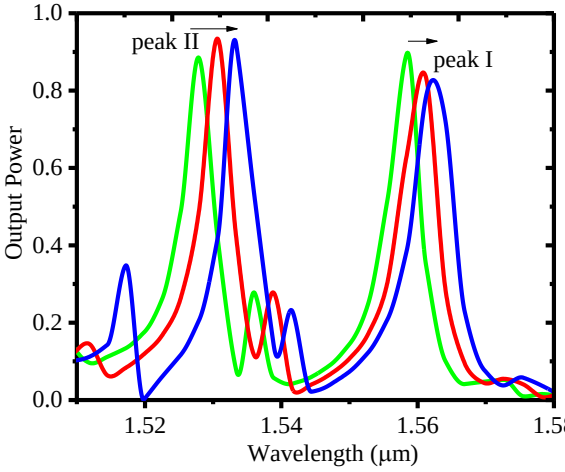


شکل ۱۴. عبوردهی طیفی ساختار دو کاواکی(با شعاع کاواک مرکزی ۹۰۰nm) برای شعاع‌های مختلف کاواک بیرونی. نمودار قرمز، سبز، آبی و نارنجی به ترتیب متناظر با شعاع‌های ۱۲۱۳، ۱۲۱۱، ۱۲۰۷ و ۱۲۰۸ نانومتر هستند. در این نمودار شعاع کاواک مرکزی ۹۰۰ nm در نظر گرفته شده است.

جدول ۲. طول‌موج تشدید مربوط به قله۱ و قله۲ برای مقادیر مختلف شعاع کاواک بیرونی.

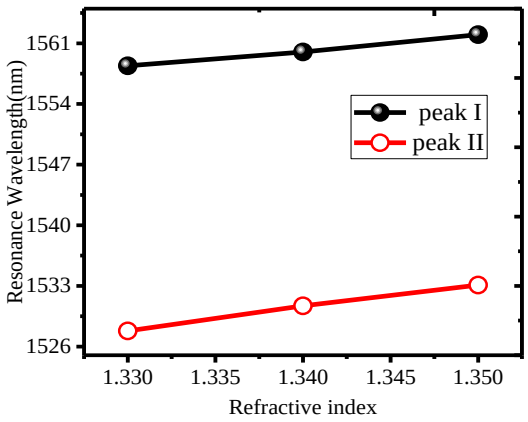
R_{out} (nm)	طول‌موج تشدید PeakI (nm)	طول‌موج تشدید PeakII (nm)
۱۲۰۳	۱۵۶۱/۳	۱۵۳۰/۸
۱۲۰۷	۱۵۵۸/۵	۱۵۲۷/۸
۱۲۱۱	۱۵۵۵/۴	۱۵۲۵/۲
۱۲۱۳	۱۵۵۲/۷	۱۵۲۲/۶

شکل (۱۵) نیز عبوردهی طیفی ساختار دوکاواکی را برای ضرایب مختلف (۱/۳۳، ۱/۳۴ و ۱/۳۵) آنالایت با شعاع کاواک بیرونی ۱۲۰۷nm نشان می‌دهد. همان‌طور که مشاهده می‌شود با افزایش ضریب شکست آنالایت، طول‌موج‌های قله۱ و قله۲ به‌سمت مقادیر بیشتر جابجا می‌شوند.



شکل ۱۵. عبوردهی طیفی ساختار دو کاواکی برای مقادیر مختلف ضریب شکست آنالایت. منحنی سبز، قرمز و آبی به‌ترتیب مربوط به ضرایب شکست آنالایت ۱/۳۳، ۱/۳۴ و ۱/۳۵ هستند.

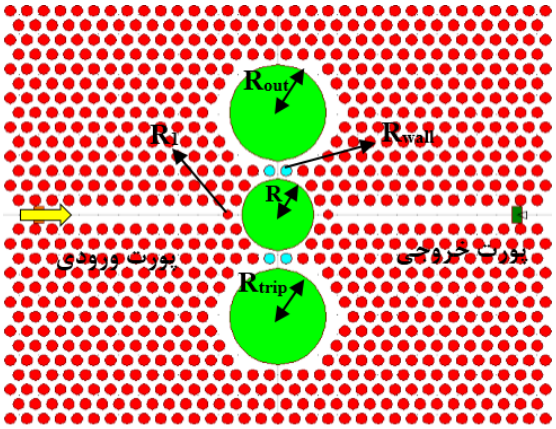
نتایج حاصل از میزان تغییرات طیف دوکاواکی ناشی از تغییرات در ضریب شکست آنالایت در شکل (۱۶) ارائه شده است. مطابق این شکل، با افزایش ضریب شکست آنالایت از ۱/۳۳ تا ۱/۳۵، طول‌موج تشدید متناظر با قله۱ (قله۲) از ۱/۵۵۸۴ μm (۱/۵۲۷۸ μm) به ۱/۵۶۲۰μm (۱/۵۳۳۱ μm) افزایش می‌یابد. مقدار حساسیت برای قله۱ و قله۲ به‌ترتیب ۱۸۰ $nm.RIU^{-1}$ و ۲۵۶ $nm.RIU^{-1}$ به‌دست آمد.



شکل ۱۶. طول‌موج تشدید متناظر با قله۱ و قله۲ برای مقادیر مختلف ضریب شکست آنالایت.

۵. شبیه‌سازی ساختار سه کاواکی

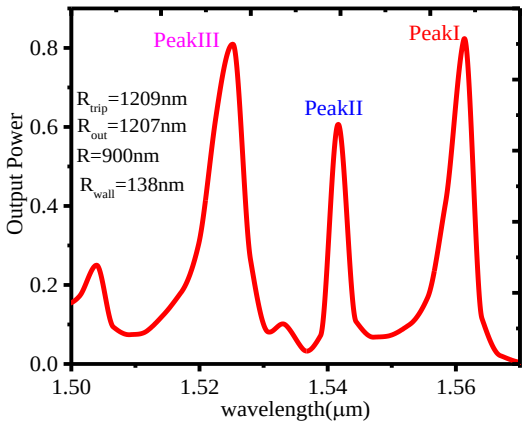
نتایج ساختار دو کاواکی بیانگر این بود که افزایش راه نوری از طریق اضافه کردن یک کاواک دیگر می‌تواند منجر به ایجاد دو قله در طیف شود. بر این اساس، ساختار سومی موسوم به ساختار سه کاواکی مطابق شکل (۱۷) طراحی شد. اضافه کردن کاواک سوم می‌تواند راه نوری طولانی‌تری را پیش روی نور نهاده و از این طریق منجر به ظهور قله‌های بیشتری در طیف شود. در این ساختار ، شعاع کاواک سوم با نماد R_{trip} مشخص شده است.



شکل ۱۷ ساختار سه کاواکی پیشنهادشده. شعاع کاواک مرکزی R، شعاع کاواک دوم R_{out} و شعاع کاواک سوم با نماد R_{trip} مشخص‌شده‌اند.

شکل (۱۸) عبوردهی طیفی ساختار سه کاواکی را برای شعاع کاواک مرکزی ۹۰۰ nm، شعاع R_1 (۱۱۵ nm)، شعاع کاواک بیرونی ۱۲۰۷ nm و شعاع کاواک سوم ۱۲۰۹ nm نشان می‌دهد. شعاع کاواک‌های آبی‌رنگ (R_{wall}) نیز برابر با ۱۳۸ nm و ضریب شکست ماده داخل کاواک‌ها ۱/۳۳ هست. همان‌طور که مشاهده می‌کنیم برای چنین ساختاری سه قله (قله۱، قله۲ و قله۳)

به‌ترتیب درطول‌موج‌های ۱/۵۶۱۴، ۱/۵۴۱۷ و ۱/۵۲۵۱ میکرومتر به‌ترتیب با پهناهای ۴/۵، ۲/۹ و ۵/۹ نانومتر به‌وجود آمده‌اند. فاکتور کیفیت نیز برای قله۱، قله۲ و قله۳ به‌ترتیب برابر با ۳۴۶، ۵۳۱ و ۲۸۵ به‌دست آمدند.



شکل ۱۸. عبوردهی طیفی ساختار سه کاواکی.

نتایج حاصل از تغییرات ضریب شکست آنالایت در کاواک‌های ساختار فوق نیز نشان دادند که مقدار حساسیت برای قله‌های ۱ و ۲ و ۳ به ترتیب ۹۰nm.RIU^{-1}، ۲۸۰nm.RIU^{-1} و ۲۹۰ nm.RIU^{-1} هستند. در جدول (۳) مقایسه‌ای بین نتایج حاصل از پارامترهای حسگری حسگرهای پیشنهادی در این مقاله با ساختارهای قبلی انجام شده است. همان‌طور که مشاهده می‌کنیم در ساختارهای پیشنهادی، کارایی حسگر بهبود یافته است.

جدول ۳. مقایسه حساسیت و فاکتور کیفیت ساختارهای قبلی با ساختارهای ارائه‌شده در این مقاله.

فاکتور کیفیت	حساسیت (nm/RIU)	سال	مرجع
۳۰۰۰	۲۷۲/۴۳	۲۰۱۶	**[۲۶]**
۲۵-۳۰	۷۲۰	۲۰۱۸	**[۲۷]**
۴۱۸	۳۰۰	۲۰۱۹	[۲۸]
۴۹۷۶۷	۲۹۴/۴۶	۲۰۱۹	**[۲۹]**
۱۱۹	۳۴۵	*	**ساختار تک کاواکی**
~۳۸۳	۲۶۵	*	**ساختار دو کاواکی**
۳۴۶	۹۰	*	**ساختار سه کاواکی (قله۱)**
۵۳۱	۲۸۰	*	**ساختار سه کاواکی (قله۲)**
۲۸۵	۲۹۰	*	**ساختار سه کاواکی (قله۳)**

۶. ساختار مناسب برای تشخیص DNA

یکی از کاربردهای حسگرهای پیشنهادی فوق‌الذکر، استفاده از آن‌ها به‌منظور تشخیص و شناسایی پیوند میان تک‌رشته‌های مولکول‌های DNA هدف[1] است. بدین منظور مایع PBS[2] با ضریب شکست ۱/۳۳۳ به‌عنوان محیط حسگری[3] در نظر گرفته می‌شود. با تشکیل پیوند میان دو مولکول DNA تک‌رشته‌ای[4] (ss-DNA)، یعنی مولکول تک‌رشته‌ای DNA کشف کننده هدف که روی سطح درونی کاواک‌ها ثابت هستند و مولکول DNA هدف (مجهول) که در مایع PBS قرار دارند و قرار است شناسایی شوند، ساختار دو رشته‌ای (ds-DNA) تشکیل می‌گردد. تشکیل چنین پیوندهایی منجر به تغییر غلظت مولی محلول PBS خواهد شد و از این طریق ضریب شکست اپتیکی آن ناحیه نیز تغییر خواهد کرد. ضریب شکست محیط آنالایت (n_s^a) بعد از جذب مولکول‌های DNA هدف مطابق رابطه (۱۰) به‌دست می‌آید [۳۹-۴۱].

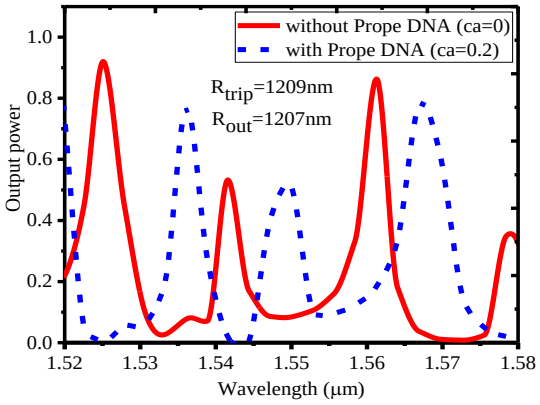
$$n_S^a = n_S + c_a \frac{dn}{dc} \qquad (۱۰)$$

که در آن، c_a غلظت مولکول‌های جذب‌شده، n_s ضریب شکست محیط آنالایت قبل از ایجاد پیوند و dn/dc نرخ افزایش ضریب شکست محیط آنالایت بعد از جذب هست که برای محیط PBS برابر با ۰/۱۸۲ cm^3g^{-1} است. کلیه ساختارهای حسگری پیشنهاد شده در این مقاله برخلاف روش‌هایی نظیر لومینسانس شیمیایی، الکترودهای فعال الکتروشیمیایی و فلوئورسنت که در آن از برچسب جهت تشخیص مولکول‌های هدف استفاده می‌شوند و به همین خاطر جزء دسته برچسبی محسوب می‌شوند، از نوع بدون برچسب هستند. چراکه در آن‌ها از ویژگی‌های بیوفیزیکی مولکول DNA، یعنی ضریب شکست نوری آن‌ها جهت شناسایی استفاده می‌گردد.

به‌منظور توضیحی تکمیلی، باید اشاره کرد که در روش‌های با برچسب، مولکول دیگری جهت شناسایی به‌صورت شیمیایی یا اتصال موقت به مولکول هدف متصل می‌گردد که این اتفاق می‌تواند باعث تغییر در ویژگی‌های ذاتی مولکول خارجی شود. روش‌های با برچسب اغلب کند، مخرب و دارای حساسیت پایین بوده و ادوات مربوطه دارای ابعاد نسبتاً بزرگی هستند. استفاده از روش‌های برچسب‌گذاری باعث کاهش طول عمر حسگر، و تک منظوره شدن آن‌ها می‌شود. اما در مقابل، روش‌های بدون برچسب دارای مزایایی مثل قابلیت اطمینان، حساسیت بالا، ارزان بودن و سهولت در مجتمع‌سازی هستند، ضمن آنکه آسیب به آنالیت موردنظر نیز در این روش به حداقل مقدار خود می‌رسد [۴۲-۴۸].

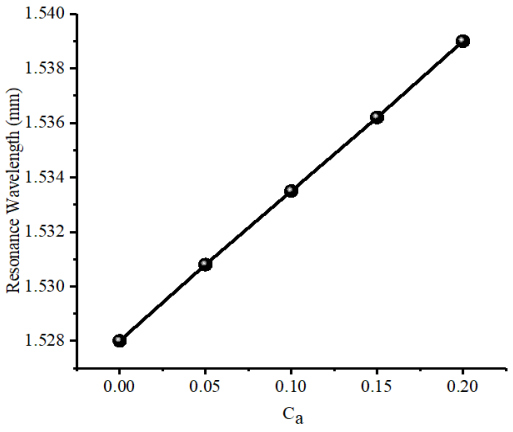
[1] Target DNA
[2] Phosphate Buffer Saline
[3] Sensing medium
[4] Ssingle strand target DNA (ss-DNA)

شکل (۱۹) عبوردهی طیفی از ساختار سه کاواکی را قبل از اضافه کردن مولکول‌های DNA جستجوگر و بعد از اضافه کردن آن نشان می‌دهد. در این شکل منظور از پیوند کامل[1] معرف زمانی است که دو تک رشته از DNA (ss-DNA) یکی به‌عنوان جستجوگر و دیگری به‌عنوان هدف پیوند برقرار کرده و یک ساختار دو رشته‌ای پیچه‌ای[2] (ds-DNA) تشکیل می‌دهند. این اتفاق زمانی رخ می‌دهد که دو تک رشته مشابه هم باشند.



شکل ۱۹. طیف عبوری از ساختار سه کاواکی در حالت با و بدون DNA.

شکل (۲۰) طول‌موج تشدید ساختار سه کاواکی را برای غلظت مولکول‌های جذب‌شده نشان می‌دهد. همانطور که مشاهده می‌کنیم، با افزایش غلظت، طول‌موج تشدید قله یک به‌صورت خطی به‌سمت مقادیر بیشتر جابجا می‌شود. مطابق این شکل، حساسیت این قله که برابر با شیب نمودار است برابر با $0.5\ nm/cm^3.g^{-1}$ همچنین مقدار R^2 برابر با ۰/۹۹۹ بدست آمد.



شکل ۲۰. طول‌موج تشدید متناظر با قله۱ برای مقادیر مختلف غلظت مولکول‌های جذب‌شده (Ca).

[1] Complementary Target
[2] Double-stranded (dsDNA) helix structure

۷. نتیجه‌گیری

هدف از این تحقیق بررسی و طراحی یک حسگر زیستی مبتنی بر بلور فوتونی است. به همین منظور سه ساختار بلور فوتونی شامل کاواک‌های هوا در محیط زمینه سیلیکونی مورد بررسی شده و شبیه‌سازی شدند. مطالعه نظری عبوردهی طیفی حسگر پیشنهادی براساس نظریه جفت‌شدگی مدها انجام شد. همچنین به‌منظور بررسی و مطالعه نحوه انتشار نور و به‌دست آوردن طیف خروجی ساختارها از روش FDTD استفاده شد. نتایج نشان دادند که ساختار تک کاواکی دارای حساسیت بالاتری نسبت به دیگر ساختارها است. این در حالی است که بهترین فاکتور کیفیت مربوط به ساختار سه کاواکی بود. در بخش آخر بررسی، از ساختار سه کاواکی به منظور آشکارسازی مولکول‌های DNA استفاده شد. نتایج نشان دادند که حسگرهای پیشنهادی قابلیت استفاده در کاربردهای مختلفی نظیر آشکارسازی عوامل بیولوژیک، آنزیم‌ها و عوامل شیمیایی را دارند.

۷. مرجع‌ها

[1] Bohunicky, B.; Mousa, S. A. “Biosensors: The New Wave in Cancer Diagnosis”; NanoTech. Sci. Appl. 2011, 4, 1.

[2] Minaei, M. E.; Saadati, M.; Najafi, M.; Honari, M. “Immobilization and Hybridization of DNA/DNA of the rfbE Gene Escherichia Coli O157:H7 on Gold Electrode Surface for the Detection of Specific Sequences by Electrochemical Impedance Spectroscopy Method”; J. Adv. Defence Sci. & Tech. 2014, 4, 279-283.

[3] Bahabady, A. M.; Olyaee, S. “Two-Curve-Shaped Biosensor for Detecting Glucose Concentration and Salinity of Seawater Based on Photonic Crystal Nano-Ring Resonator”; Sens. Lett. 2015, 13, 774-777.

[4] Jafari, A.; Rahmatnezamabad, A. “Controlling Band Gap of One Dimensional Photonic Crystals via the Nonlinear Characteristic of Layers”; J. Adv. Defence Sci. & Tech. 2019, 2, 169-175.

[5] Yang, X.; Zhang. A.Y; Wheeler, D.A.; Bond, T.C.; Gu C, Li Y. “Direct molecule-specific glucose detection by Raman spectroscopy based on photonic crystal fiber”; Anal. Bioanal. chem. 2012, 402(2), 687-691.

[6] Salahandish, R.; Zargartalebi, H.; Janmaleki, M.; Khetani, S.; Azarmanesh, M.; Ashani, M.M.; Aburashed, R.; Vatani, M.; Ghaffarinejad, A.; Sanati- Nezhad, A. “Reproducible and Scalable Generation of Multilayer Nanocomposite Constructs for Ultrasensitive Nanobiosensing”; Adv. Materials Tech. 2019 Sep 12:1900478.

[7] Salahandish, R.; Ghaffarinejad, A.; Omidinia, E.; Zargartalebi, H.; Majidzadeh, A. K.; Naghib, S.M.; Sanati-Nezhad, A. “Label-free ultrasensitive detection of breast cancer miRNA-21 biomarker employing electrochemical nano-genosensor based on sandwiched AgNPs in PANI and N-doped grapheme”; Biosens. Bioelectron. 2018 Nov 30, 120, 129-136.

[8] Shushama, K. N.; Rana, M. M.; Inum, R.; Hossain, M. B. “Graphene Coated Fiber Optic Surface Plasmon Resonance Biosensor for the DNA Hybridization Detection: Simulation Analysis”; Opt. Commun. 2017, 383, 186-190.

[9] Caucheteur, C.; Guo, T.; Albert, J. “Review of Plasmonic Fiber Optic Biochemical Sensors: Improving the Limit of Detection”; Anal. Bioanal. Chem. 2015, 407, 3883-3897.

[10] Ksendzov, A.; Lin, Y. “Integrated Optics Ring-Resonator Sensors for Protein Detection”; Opt. lett. 2005, 30, 3344-3346.

[11] Rodrigo, D.; Limaj, O.; Janner, D.; Etezadi, D.; De Abajo, F. J.; Pruneri, V.; Altug, H. “Mid-Infrared Plasmonic Biosensing with Graphene”; Science. 2015, 349, 165-168.

[12] Mokari, M.; Shahamat, Y.; Alamatsaz, M.H.; Babaei-Brojeny, A.A.; Moeini, H. “The effect of material nonlinearity on the band gap for TE and TM modes in square and triangular lattices”; Iranian J. Phys. Research. 2018; 18(3).

[13] Wu, L.; Chu, H. S.; Koh, W. S.; Li, E. P. “Highly Sensitive Graphene Biosensors Based on Surface Plasmon Resonance”; Opt. express. 2010, 18, 14395-14400.

[14] Jia, G. Y.; Huang, Z. X.; Zhang, Y. L.; Hao, Z. Q.; Tian, Y. L. “Ultrasensitive Plasmonic Biosensors Based on Halloysite Nanotubes/MoS2/Black Phosphorus Hybrid Architectures”; J. Mater. Chem. C. 2019, 7, 3843-3851.

[15] Yen, Y. C.; Chiu, N. F. “Plasmonic Biosensor Detected Human Chorionic Gonadotropin with Naked Eye in Optical Sensors”; Inter. Soc. Opt. Photonics. 2019, 11028, 1102823.

[16] Chow, E.; Grot, A.; Mirkarimi, L. W.; Sigalas, M.; Girolami, G. “Ultracompact Biochemical Sensor Built with Two-Dimensional Photonic Crystal Microcavity”; Opt. Lett. 2004, 29, 1093-1095.

[17] Shahamat, Y.; Vahedi, M. “Mid-Infrared Plasmonically Induced Absorption and Transparency in a Si-Based Structure for Temperature Sensing and Switching Applications”; Opt. Commun. 2019, 430, 227-233.

[18] Luo, Y.; Fan, R.; Zhang, Y.; Wu, Q.; Ren, Z.; Peng, B. “Novel Optical Fiber Refractive Sensor Fabricated with an Alcohol-Filled Photonic Crystal Fiber Based on a Mach–Zehnder Interferometer”; Opt. Fiber Tech. 2019, 48, 278-282.

[19] Kim, S.; Lee, J.; Jeon, H.; Kim, H.J. “Fiber-coupled surface-emitting photonic crystal band edge laser for biochemical sensor applications”; Appl. Phys. Lett. 2009, 94, 133503.

[20] Dündar, M. A.; Ryckebosch, E.C.; Nötzel, R.; Karouta, F.; Van ijzendoorn, L.J.; Van der Heijden, R.W. “Sensitivities of InGaAsP photonic crystal membrane nanocavities to hole refractive index”; Opt. express.2010, 18 (5), 4049–4056.

[21] Pal, S.; Guillermain, E.; Sriram, R.; Miller, B.L; Fauchet, P.M. “Silicon photonic crystal nanocavity-coupled waveguides for error-corrected optical biosensing”; Biosens. Bioelectron. 2011, 26 (10), 4024–4031.

[22] Sriram, R.; Baker, J.E.; Fauchet, P.M.; Miller, B.L. “Two dimensional photonic crystal biosensors as a platform for label-free sensing of biomolecules, infrontiers in Biological Detection: From Nanosensors to Systems V”; Inter. Soc. Opt. Photonics. 2013, 8570, 857007.

[23] Olyaee, S., Bahabady, A.M.; Leitgeb, E. “A diamond-shaped bio-sensor based on two-dimensional photonic crystal nano-ring resonator”; In2014 9th International Symposium on Communication Systems, Networks & Digital Sign (CSNDSP). 2014 Jul 23, 434-437.

[24] Bendib, S.; Zegadi, A.; Djeffal, N. “Improved sensitivity of 2D annular photonic crystal biosensor working at THz frequency range”; Opt. Quant. Electron. 2016 Dec 1; 48(12):528.

[25] Arunkumar, R.; Suganya, T.; Robinson, S. “Design and analysis of photonic crystal elliptical ring resonator based pressure sensor”; Photonics Opt. Tech. 2017 Mar, 3, 30-34.

[26] Olyaee, S.; Mahmood, S.; Mohsenirad, H. “Label-free detection of glycated haemoglobin in human blood using silicon-based photonic crystal nanocavity biosensor”; Journal of Modern Optics. 2018, 63, 1274-1279.

[27] Danaie, M.; Kiani, B. “Design of a label-free photonic crystal refractive index sensor for biomedical applications”; Photonic. Nanostruct. 2018 Sep 1, 31, 89-98.

[28] Fatemeh Rahman, Z.; Kaatuzian, H.; Danaie, M. “Hybrid Photonic Crystal Cavity as a Sensitive Label-Free Biosensor”; 27th Iranian Conference on Electrical Engineering (ICEE), 2019, 18-22.

[29] Benmerkhi, A.; Bouchemat, M.; Bouchemat, T. “Computational Study of Photonic Crystal Resonator for Biosensor Application”; Frequenz. 2019 Sep 25, 73, 307-316.

[30] Shruti, S.; Sinha, R.K.; Bhattacharyyab, R. “Photonic crystal slab waveguide-based infiltrated liquid sensors: design and analysis”; J. Nanophotonics. 2011, 5, 053505.

[31] Zhanga, L.; Cao, T.; Li, Z.G.; Qin, K.R. and Yan, W.P. “Study of photonic crystal cavity sensor integrated with microfluidic channel in the visible region”; Proceedings; SPIE 8561; Advanced sensor systems and applications; Beijing; 2012; 85610A:1–7.

[32] Dutta, H.; Pal, S. “Design of a highly sensitive photonic crystal waveguide platformfor refractive index based biosensing”; Opt. Quant. Electron. 45, 2013, 907–917.

[33] Bagci, F.; Akaoglu, B. “Enhancement of Refractive Index Sensitivity in Photonic Crystal Waveguide-Based Sensors by Selective Infiltration”; Acta. Phys. Pol. A. 2013.

[34] Faida, B.; Touraya, B.; Mohamed, B.; and Nicole, P. “Optofluidic sensor using two-dimensional photonic crystal waveguides”; Phys. J. Appl. Phys. 201 62: 11201.

[35] Dutta, H.S.; Pal, S. “Design of a highly sensitive photonic crystal waveguide platform for refractive index based biosensing”; Opt. Quant. Electron. 2013, 45, 907–917.

[36] Taflove, A.; Oskooi, A.; Johnson, S. G.; editors. “Advances in FDTD Computational Electrodynamics”; Photonics and Nanotech. Artech house; 2013.

[37] Shahamat, Y.; Vahedi, M. “Designing a Photonic Crystal Based Optical Wavelength Division Demultiplexer for Communication Applications”; Majlesi J. Telecomm. Devices. 2019, 8(1), 1-5.

[38] Shahamat, Y.; Ghaffarinejad, A.; Vahedi, M. “Plasmon Induced Transparency and Refractive Index Sensing in Two Nanocavities and Double Nanodisk Resonators”; Optik. 2019 Oct 14:163618.

[39] Tamersit, K.; Djeffal, F. “Double-Gate Graphene Nanoribbon Field-Effect Transistor for DNA and Gas Sensing Applications: Simulation Study and Sensitivity Analysis”; IEEE Sensors J. 2016, 16, 4180-4191.

[40] Hossain, M.; Rana, M. “Graphene Coated High Sensitive Surface Plasmon Resonance Biosensor for Sensing DNA Hybridization”; Sens. Lett. 2016, 14, 145-152.

[41] Diéguez, L.; Darwish, N.; Mir, M.; Martínez, E.; Moreno, M.; Samitier, J. “Effect of the Refractive Index of Buffer Solutions in Evanescent Optical Biosensors”; Sens. Lett. 2009, 7, 851-855.

[42] Shushama, K. N.; Rana, M. M.; Inum, R.; Hossain, M. B. "Graphene Coated Fiber Optic Surface Plasmon Resonance Biosensor for the DNA Hybridization Detection: Simulation Analysis"; Opt. Commu. 2017, 383, 186-190.

[43] Mertens, Johann.; Celia, R.; Montserrat, C.; Daniel, R.; Jose Angel Martín, G.; Carlos, B.; Javier, T. "Label-free detection of DNA hybridization based on hydration-induced tension in nucleic acid films"; Nature nanotechnology, 2008, 3, 301.

[44] Kataoka, H.; Chiho.; Yuji, M. "Label-free detection of DNA by field-effect devices"; IEEE Sensors Journal, 2011, 11, 3153-3160.

[45] Kaye.; Savannah.; Zheng, Z.; Mollye, S.; Krishnan, Ch.; Paula M. Koelle, Robert, L, Upender, M, Yongbin, L, Jianjun, W. "Label-free detection of DNA hybridization with a compact LSPR-based fiber-optic sensor"; Analyst, 2017, 142, 1974-1981.

[46] Juan-Colás.; José.; Steven, J.; Thomas F. Krauss. "Dual-mode Electro-Optical techniques for biosensing applications: A Review"; Sensors, 2017, 17, 2047.

[47] Syahir.; Amir.; Kenji, U.; Kin-ya, Tomizaki.; Kotaro, K.; Hisakazu, M. "Label and label-free detection techniques for protein microarrays"; Microarrays, 2015, 228-244.

[48] Chen.; Xueping.; Yu, L.; Jiaoqi, H.; Wei, L.; Junfu, H.; Yang, Z.; Weiling, F. "Label-free techniques for laboratory medicine applications"; Frontiers in Laboratory Medicine, 2017, 82-85

راهنمای تهیه و تدوین مقالات

نویسنده‌ها باید ابتدا به پایگاه مجله: www.adst.ihu.ac.ir مراجعه و ثبت‌نام نموده و پس از دریافت کد کاربری و رمز عبور، اقدام به بارگذاری (upload) فایل مقاله نمایند. مقاله ارسال‌شده نباید قبلاً در هیچ مجله داخلی و یا خارجی چاپ شده باشد و در حین داوری توسط این مجله، برای مجله دیگری ارسال شود. برای تسریع داوری مقاله، نویسندگان مشخصات ۵ داور متخصص را به دفتر فصل‌نامه پیشنهاد نمایند. ارائه نشانی الکترونیکی تمام نویسندگان در هنگام بارگذاری مقاله الزامی است. مقاله مطابق با قالب مجله از نظر نوع، قلم، سایز قلم، درج شکل‌ها و... باید به زبان فارسی و با استفاده از نرم‌افزار Word 2010 حداکثر در ۱۵صفحه به صورت دو ستونی با عرض هر ستون ۸/۲cm و حاشیه‌ها از هر طرف ۲cm تهیه شود. نام و اندازه قلم در صفحه اول و متن مقاله در جدول زیر ارائه شده‌اند. صفحه نخست مقاله باید شامل عنوان مقاله، نام نویسنده‌ها، چکیده و کلیدواژه‌ها در دو بخش فارسی و لاتین باشد. متن اصلی مقاله باید شامل بخش‌های مقدمه، روش تحقیق (یا بخش تجربی)، نتایج و بحث و مرجع‌ها باشد. شماره مرجع مورد استفاده به ترتیب و در کنار متن مربوطه به صورت عدد فارسی داخل کروشه آورده شود (مثال [۲]). معادله‌های ریاضی و مکانیسم‌ها به ترتیب اشاره در متن به صورت عدد داخل پرانتز شماره‌گذاری شوند. عنوان جدول‌ها در بالای آن‌ها و نام شکل‌ها در زیر آن‌ها به صورت راست چین شماره‌گذاری شود. در ارجاع به معادلات، شکل‌ها و جدول‌ها در داخل متن قبل از انتهای جمله، عدد مربوط در داخل پرانتز قرار گیرد مانند "شکل (۵)" در صورت ارجاع به شکل و جدول در انتهای متن کل عبارت و عدد داخل پرانتز قرار گیرد مانند (شکل ۵)".

صفحه اول مقاله		نام قلم	اندازه قلم
بخش فارسی	عنوان مقاله (حداکثر۱۵ کلمه، وسط‌چین)	B Zar Bold	16
	نام نویسنده‌ها (نویسنده پاسخگو با ستاره مشخص شود)	B Lotus Bold	12
	درجه علمی نویسندگان و محل انجام تحقیق	B Lotus	10
	چکیده (حداکثر ۱۵۰ کلمه، تک ستونی)	B Nazanin	11
	واژه‌های کلیدی (حداکثر۶ کلمه)	B Nazanin Bold	11
بخش لاتین	عنوان مقاله (حداکثر۱۵ کلمه، وسط‌چین)	Times New Roman Bold	14
	نام نویسنده‌ها (نویسنده پاسخگو با ستاره مشخص شود)	Times New Roman Bold	10
	محل انجام تحقیق	Times New Roman	9
	چکیده (تک ستونی)	Times New Roman Italic	10
	واژه‌های کلیدی (حداکثر۶ کلمه)	Times New Roman	10
	پست الکترونیکی نویسنده پاسخگو (به صورت پاورقی)	Times New Roman	8
متن مقاله		نام قلم	اندازه قلم
متن مقاله (Single Space)		B Nazanin	11
کلمه‌های انگلیسی داخل متن		Times New Roman	9
عنوان بخش‌ها (مثال: ۳.)		B Nazanin Bold	12
عنوان زیر بخش‌ها (مثال: ۳-۱.)		B Nazanin Bold	11
شماره جدول‌ها و شکل‌ها (راست چین)		B Nazanin Bold	10
توضیحات جدول‌ها و شکل‌ها		B Nazanin	10
مرجع‌ها		Times New Roman	8

قالب مرجع‌ها باید مطابق قالب نشریه از لحاظ قلم، شیوه ترتیب ارائه نام نویسندگان، عنوان و نشانی مقاله و نیز از لحاظ نقطه‌گذاری و ویرگول باشد. عنوان مقاله به صورت Title Case تنظیم شود. نام نشریه‌ها به صورت اختصاری بر اساس استاندارد ISI نوشته شوند (از طریق جستجو در ISI Journal Title Abbreviation). در صورت ارائه نام محققین در پیشینه تحقیق و در مقدمه، از ارائه سال و زیرنویس نام محقق پرهیز شود و شماره مرجع بلافاصله بعد از نام محقق آورده شود. استفاده از عبارت "در [؟]" یا "در مرجع [؟] " در داخل متن صحیح نیست و بعد از ارائه مطلب، باید در انتهای جمله ارجاع داده شود. کلیه مرجع‌ها باید به زبان انگلیسی نوشته شوند. از آوردن عبارت .et al خودداری شود و نام کلیه نویسندگان نوشته شود. فاصله بین هر مرجع با مرجع بعدی 6 pt باشد. نگارش مرجع‌های مختلف مطابق با قالب نشریه باید به گونه‌های زیر باشد.

- مقاله‌ها:

[1] Deno, N. C.; Richey, H. G.; Liu, J. S.; Lincoln, D. N. "Sucrose Synthesis"; J. Am. Chem. Soc. 1965, 87, 4533-4538.

- مقاله‌های ارائه‌شده در اجلاس‌های بین‌المللی:

[1] Hacigumus, H.; Lyer, B.; Mehrotra, S. "Providing Database as a Service"; Proc. Int. Conf. Data Eng. 2002, 29-38.

- کتاب‌ها:

[1] Anastas, P. T.; Warner, J. C. "Green Chemistry: Theory and Practice"; Oxford University Press: Oxford, 1998.

- گزارش‌های ثبت اختراع (پتنت):

[1] Stern, M. K.; Cheng, B. K. M. "Process for Preparing N-(p-nitroaryl)amides via Reaction of Nitrobenzene with Nitriles"; US Patent 5,380,946, 1995.

- پایان‌نامه‌ها:

[1] Enander, R. T. "Lead Particulate and Methylene Chloride Risks in Automotive Refinishing"; Ph.D. Thesis, Tufts University, Medford, MA, 2001.

- پایگاه‌های اینترنتی:

[1] Weisstein, E. W. "Molecular Orbital Theory"; http://scienceworld.wolfram.com/chemistry/MolecularOrbitalTheory.html, 2005.

فرم اشتراک

نشریه علمی

علوم و فناوری‌های پدافند نوین

۱۳۶۵
دانشگاه جامع امام حسین(ع)

علاقه‌مندان به اشتراک مجله می‌توانند فرم زیر را تکمیل و به یکی از روش‌های (فکس، ایمیل و یا صندوق پستی) بـه دفتر مجله ارسال نمایند.

هزینه اشتراک برای چهار شماره در سال مبلغ ۱/۶۰۰/۰۰۰ریال می‌باشد که بایستی به حساب جاری ۵۰۰۶۰/۱۸ بانک سپه، شعبه دانشگاه امام حسین(ع) (کد شعبه ۸۴۸) به نام درآمدهای پژوهشی دانشگاه جامع امام حسین(ع)، واریز و اصل فـیش بـانکی آن را به‌همراه فرم اشتراک تکمیل شده به دفتر مجله ارسال نمایید.

شخصی:☐موسسه‌ای: ☐ نام: نام خانوادگی: تاریخ درخواست اشتراک:

شغل:

نشانی کامل: .....

تلفن: ..... دورنگار:..... آدرس الکترونیکی:.....

شماره‌های درخواستی:

وضعیت درخواست اشتراک : جدید ☐ تمدید ☐ در صورت تمدید، کد اشتراک قبلی: .....

لطفاً در صورت تغییر نشانی و یا عدم دریافت به‌موقع نشریه، مراتب را در اسرع وقت به دفتر مجله اعلام فرمایید.

نشانی: تهران، بزرگراه شهید بابایی، دانشگاه جامع امام حسین (ع)، دانشکده و پژوهشکده فنی و مهندسی، ساختمان باقرالعلوم (ع)،
نشریه علمی علوم و فناوری‌های پدافند نوین
تلفن و نمابر: ۷۴۱۸۹۱۹۵ **صندوق پستی:** ۱۹۴-۱۶۵۸۵
www.adst.ihu.ac.ir **www.padafandn@ihu.ac..ir** **info@adst.ir**

محل الصاق تصویر فیش واریزی هزینه اشتراک

Editorial

1) **S. M. Alavi** (Associate Professor, Imam Hossein University)
2) **M. R. Alizadeh Pahlavani** (Associate Professor, Malek Ashtar University of Technology)
2) **M. H. Beheshty** (Professor, Iran Polymer and Petrochemical Institute)
3) **S. GH. Eslami** (Professor, University of Tehran)
4) **H. Fakhraian** (Professor, Imam Hossein University)
5) **R. A. Izadifard** (Assistant Professor, Imam Khomeini International University)
6) **M. H. Keshavarz** (Professor, Malek Ashtar University of Technology)
7) **H. Khodarahmi** (Professor, Imam Hossein University)
5) **A. M. Latifi** (Associate Professor, Baqiatallah University of Medical Sciences)
8) **M. Mardani Sharbabak** (Assistant Professor, Imam Hossein University)
9) **A. Mirghadri** (Associate Professor, Imam Hossein University)
11) **M. Mohammad Pouramini** (Professor, Shahid Beheshti University)
12) **P. Parvin** (Professor, Amir Kabir Universityof Technology)
13) **Gh. Riazi** (Professor, University of Tehran)
14) **A. Shaabani** (Professor, Shahid Beheshti University)
15) **M. Saleh Esfahani** (Assistant Professor, Imam Hossein University)
16) **M. Semnani Rahbar** (Associate Professor, Imam Hossein University)
17) **A. Vafaee Sefat** (Professor, Imam Hossein University)
18) **A. A. Yousefi** (Professor, Iran Polymer and Petrochemical Institute)

Consultants and Reviewers

1) **F. Basalighe** (Shahroud University of Technology)
2) **S. Mollaei** (University of Bonab)
3) **M. Malekshahi** (Birjand University of Technology)
4) **S. Peyman** (Imam Hossein University)
5) **E. Zamani Bidokhti** (Shahroud University of Technology)
6) **M. Hoseinpour** (Amirkabir University of Technology)
7) **H. Aghabarati** (Amirkabir University of Technology)
8) **R. Kamgar** (University of Shahrekord)
9) **H. Aalami** (Imam Hossein University)
10) **M. Velayati** (Semnan University)
11) **S. M. Seyyedbarzegar** (Shahroud University of Technology)
12) **M. Mirzaei** (Babol Noshirvani University of Technology)
13) **Sh. Dehghan** (Qazvin Islamic Azad University)
14) **A. Hajizadeh** (Aalborg University)
15) **M. Behrouzian nezhad** (Islamic Azad University Of Shadegan)
16) **M. Abbasi** (Imam Hossein University)
17) **M. Naghavi** (Imam Hossein University)
18) **M. Parsaei** (Shiraz University of Technology)
19) **H. Abdoli** (Bu-Ali Sina University)
20) **A. Ghafoori** (Imam Hossein University)
21) **D. Javaheri** (Islamic Azad University Science and Research Branch)
22) **A. Mirghadri** (Imam Hossein University)
23) **M. Ilchi** (Atomic Energy Organization of Iran)
24) **S. Oliaei** (Shahid Rajaee Teacher Training University)
25) **M. Jani** (Shahid Beheshti University)
26) **M. Karimi** (Atomic Energy Organization of Iran)
27) **R. Ghaffarpour** (Imam Hossein University)
28) **J. Khalilzadeh** (Imam Hossein University)
29) **M. R. Alizadeh Pahlavani** (Malek Ashtar University of Technology)
30) **R. A. Izadifard** (Imam Khomeini International University)
31) **M. Mardani Sharbabak** (Imam Hossein University)
32) **H. Fakhraeian** (Imam Hossein University)

Cooperating Institutions and Associations

1. **Chemistry & Chemical Engineering Research Center of Iran**
2. **Iran Polymer and Petrochemical Institute**
3. **Institute for Colorants, Paint and Coatings**
4. **MalekAshtar University of Technology**
5. **Baqiatallah University of Medical Sciences**
6. **Building and Housing Research Center**

1986
ImamHosseinUniversity

Journal of
Advanced Defence Science and Technology

Volume 11, Number 4, 2021
ISSN: 2676-2935

Managing Director: Rohollah Razavinezhad
Editor-in-Chief: Hossein Fakhraian
Administrative Director: Saeed Zardar

- Publisher: Faculty of Engineering, Imam Hossein University
- Administrative Assistant: Amirmahdi Dadashzadeh
- Editor and Top Rated: Mehraban Esmaeilzadeh
- Printing: Sepah Print Center

This journal is indexed in the following sites:

- *Islamic World Science Citation (www.isc.gov.ir)*
- *Regional Library of Science and Technology, Shiraz (www.ricest.ac.ir)*
- *Database Bank of Scientific Publications (www.magiran.com)*
- *Scientific Information Database (www.SID.ir)*
- *Google Scholar (www. scholar.google.com)*
- *Civilica (www.civilica.com)*

Address: Babaii Highway, Imam Hossein Comprehensive University, Tehran, I.R.Iran
P.O.Box: 16585-187 Phone and Fax: +98-21-74189195
www.adst.ihu.ac.ir **Padafandn@ihu.ac.ir**