مجله علمی پژوهشی «علوم و فناوری‌های پدافند نوین»
سال هشتم، شماره ۱، بهار ۱۳۹۶؛ ص ۶۹-۶۱

مهندسی مجموعه ویژگی برای تشخیص حملات سیل‌آسا در VoIP مبتنی بر SIP

حسن اصغریان[۱]، احمد اکبری[۲*]، بیژن راحمی[۳]

۱- دکترای، ۲- دانشیار، دانشگاه علم و صنعت ایران، ۳- دانشیار، دانشگاه اوتاوا، کانادا

(دریافت: ۹۴/۱۰/۲۹، پذیرش: ۹۵/۰۷/۲۳)

چکیده

پروتکل SIP به عنوان پروتکل اصلی لایه کنترل در شبکه‌های نسل آینده و کاربردهای چند رسانه‌ای نظیر ویدئو کنفرانس، تلویزیون و تلفن اینترنتی (VoIP) مطرح شده است. اصلی‌ترین حملات موجود در VoIP با عنوان حملات سیل‌آسا شناخته می‌شوند که بیش از ۹۸ درصد آن‌ها به علت مشکلات پیاده‌سازی و پیکربندی و کمتر از دو درصد آسیب‌پذیری‌های مربوطه به علت ضعف پروتکل به وقوع می‌پیوندند. در این مقاله یک مجموعه ویژگی برای تشخیص ناهنجاری در کاربردهای مبتنی بر SIP به طور کلی و به طور خاص VoIP مهندسی شده است. منظور از مهندسی ویژگی، استفاده از دانش موجود در داده‌های مربوط به لایه‌های مختلف SIP با هدف ساخت ویژگی‌های قابل استفاده در الگوریتم‌های یادگیری ماشین است. برای این منظور پس از استخراج داده از عملکرد حالت طبیعی SIP در VoIP، این داده‌ها در قالب یک مجموعه ویژگی سازمان‌دهی شده است. عملکرد مجموعه ویژگی پیشنهادی با به‌کارگیری دو روش یادگیری ماشین مختلف سنجیده شده است. این سنجش عملکرد با به‌کارگیری سه مجموعه دادگان اختصاصی مختلف در SIP انجام شده است و کیفیت خروجی از نظر نرخ تشخیص و نرخ هشدار نادرست حاکی از عملکرد مناسب مجموعه ویژگی پیشنهادی است.

کلیدواژه‌ها: مهندسی ویژگی، امنیت SIP، حملات اختلال در سرویس‌دهی، حملات سیل‌آسای SIP

Engineered Feature Set to Detect Flooding Attacks in SIP Based VoIP

H. Asgharian, A. Akbari*, B. Raahemi

Iran University of Science and Technology

(Received: 19/01/2016; Accepted: 14/10/2016)

Abstract

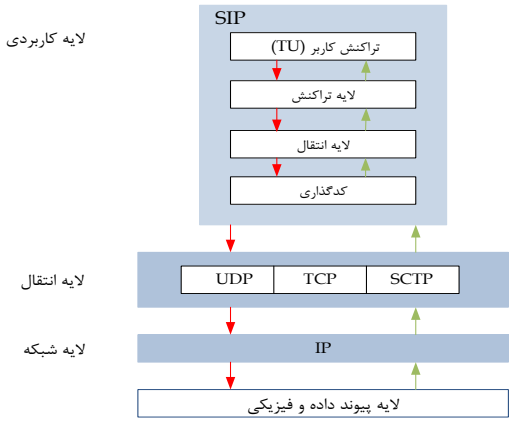
The main signaling protocol of next generation networks especially in multimedia applications (e.g. video conference, IPTV and VoIP) is session initiation protocol (SIP). Different types of Denial of Service (DoS) attacks are applicable to SIP entities because of the stateful functionality and text based nature of SIP. More than 98 percent of these attacks against SIP entities are caused by misconfiguration and implementation shortcomings. In this paper, a feature set for using in anomaly detection systems by feature engineering approach is generated. The knowledge of SIP packets, SIP internal state machine and normal behavior of this protocol were employed to create features that make machine learning algorithms work. The performance of the engineered feature set is evaluated with two different classifiers by applying three different data sets. The experimental results show the performance of proposed feature set in terms of detection and false alarm rate.

Keywords: Feature Engineering, SIP Security, Denial of Service VoIP Attack, SIP Flooding Attacks

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

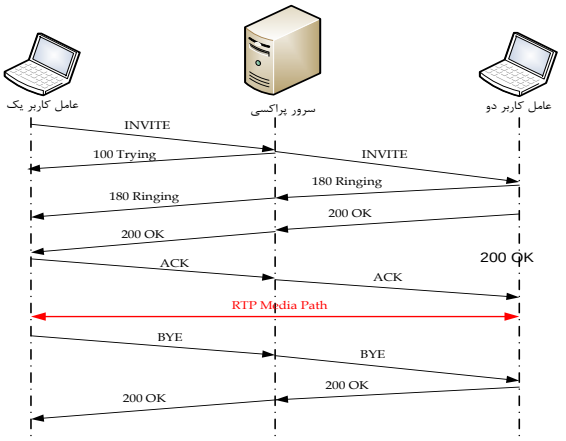
۱. مقدمه

اصلی‌ترین پروتکل لایه کنترل در سرویس‌های چندرسانه‌ای و شبکه‌های نسل آینده که برای ایجاد، نگهداری و خاتمه دادن به نشست‌های چندرسانه‌ای به‌کار گرفته می‌شود، پروتکل SIP[1] است [۱ و ۲]. این پروتکل به عنوان پروتکل اصلی سیگنالینگ در شبکه‌های نسل آینده نیز معرفی شده است ولی پیچیدگی ذاتی و عملکرد حالتمند این پروتکل موجب شده است که آسیب‌پذیری های متعددی در آن وجود داشته باشد. نتیجه پژوهش‌های منتشر شده بر روی SIP حاکی از آن است که بیش از ۹۸ درصد از مشکلات امنیتی و حملات بر روی این پروتکل به علت مشکلات پیاده‌سازی و پیکربندی نادرست بوده است [۳]. این مسئله با در نظر گرفتن رشد شبکه‌های چندرسانه‌ای و توسعه شبکه‌های باند پهن ارتباطی و نیز حرکت به سمت سرویس‌های متنوع مخابراتی نرم‌افزار محور و کاربردهای جدید، سبب شده است که توجه به امنیت پروتکل‌های کنترلی به ویژه در زمینه ابرهای چندرسانه‌ای و ابرهای سرویس جدید نظیر ابرهای حسگری در اینترنت اشیه، اهمیت ویژه‌ای پیدا کرده است. همان‌طور که در شکل ۱) نمایش داده شده است، این پروتکل ساختاری حالتمند در لایه کاربردی دارد و با به‌کارگیری ماشین حالت داخلی خود، موجب انتقال مطمئن بسته‌های مبتنی بر این پروتکل به صورت مستقل از لایه انتقال می‌شود. ماهیت متنی SIP شبیه به پروتکل SNMP و HTTP است که اطلاعات اصلی مربوط به مسیریابی را به صورت متن در سرآیند خود حمل می‌کند [۳].



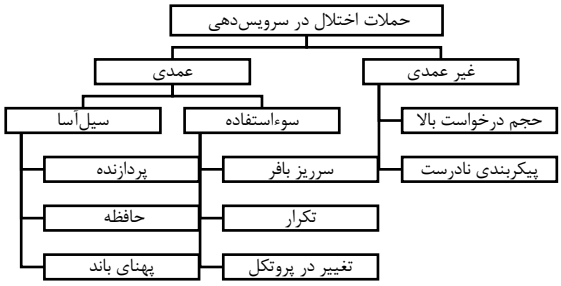
شکل ۱. ساختار لایه‌ای و حالتمند SIP در لایه کاربردی [۴]

عملکرد حالت طبیعی سیگنالینگ مربوط به یک کاربرد VoIP مبتنی بر SIP در شکل ۲) نمایش داده شده است. همان‌طور که مشاهده می‌شود، تمامی درخواست‌های SIP با حداقل یک پیام پاسخ روبه‌رو می‌شوند. ماشین حالت موجودیت‌های مربوط به این پروتکل برای هر درخواست ورودی یک زمان‌بند[1] تنظیم می‌نماید که با انقضای این زمان‌بند، پیام مربوطه تکرار می‌شود [۴]. همچنین تمامی موجودیت‌های حالتمند SIP ملزم به نگهداری اطلاعات مربوط به نشست‌های خود تا پایان تماس هستند [۲]. نشست‌های SIP نیز به دو دسته تراکنش و مکالمه تقسیم‌بندی می‌شوند. منظور از تراکنش در SIP، یک درخواست به همراه تمامی پاسخ‌های مربوط به آن است. همچنین یک مکالمه شامل تمامی ارتباطات بین دو طرف تماس است.



شکل ۲. عملکرد حالت طبیعی پروتکل SIP [۶]

ساختار حالتمند و ماهیت متنی SIP موجب شده است که حملات مختلف اختلال در سرویس‌دهی[2] (DoS) با هدف اشغال منابع اصلی موجودیت‌های مبتنی بر این پروتکل معرفی شوند. دسته‌بندی حملات اختلال در سرویس‌های مبتنی بر SIP در شکل ۳) نمایش داده شده است [۵]. همان‌طور که در شکل مشخص شده است، اصلی‌ترین حملات سیل‌آسای SIP به سه دسته اصلی حملات پردازنده‌ای، حملات حافظه‌ای و حملات پهنای باند تقسیم‌بندی می‌شوند [۶].



شکل ۳. طبقه‌بندی حملات اختلال در سرویس‌دهی SIP [۷]

به‌کارگیری روش‌ها و الگوریتم‌های یادگیری ماشین برای تشخیص حالت‌های غیر طبیعی عملکرد پروتکل‌های شبکه‌ای یا ناهنجاری‌های موجود در کاربردهای مبتنی بر آن‌ها یکی از

[1] Session Initiation Protocol

[1] Timer
[2] Denial of Service (DoS)

رویکردهای اصلی در حوزه امنیت شبکه‌های رایانه‌ای است [۸]. هر چند نمی‌توان با قطعیت کامل موفقیت هر روش یادگیری ماشین را به مجموعه ویژگی‌های به‌کار رفته در آن منتسب دانست، ولی صحت و دقت عملکرد یک سامانه یادگیری ماشین وابستگی بسیار زیادی به عملکرد ویژگی‌های آن دارد. منظور از ویژگی، اطلاعاتی است که از روی سابقه ترافیک موجود و وضعیت فعلی آن، برای پیشبینی حالت‌های بعدی سامانه قابل استفاده باشد. هر قدر ویژگی‌های تولیدی برای پیشبینی وضعیت ترافیک، عمومیت بیشتری داشته باشند، با الگوریتم‌های ساده‌تر و احتمالاً سربار پردازشی کمتری به نتیجه بهتر از نظر دقت تشخیص و نرخ هشدار نادرست رسیده می‌شود [۸]. به طور کلی فرایند تولید و ساخت ویژگی در کاربردهای مختلف دارای پیچیدگی و هزینه بالایی است. از این فرایند با عنوان مهندسی ویژگی یاد می‌شود.

با توجه به اینکه بررسی علت حملات سیل‌آسای SIP نشان داده است که بیش از ۹۸ درصد این آسیب‌پذیری‌ها به علت مشکلات پیاده‌سازی و پیکربندی و کمتر از دو درصد آسیب پذیری‌های مربوطه به علت ضعف پروتکل بوده است [۹]، در این مقاله یک مجموعه ویژگی برای تشخیص ناهنجاری در سامانه‌های تلفنی (VoIP) مبتنی بر SIP مهندسی شده است. برای این منظور پس از استخراج داده از عملکرد حالت طبیعی SIP، این داده‌ها در قالب یک مجموعه ویژگی سازمان‌دهی شده است. همچنین عملکرد مجموعه ویژگی پیشنهادی با به‌کارگیری دو روش یادگیری ماشین مختلف سنجیده شده است. این سنجش عملکرد با به‌کارگیری سه مجموعه دادگان اختصاصی مختلف در SIP انجام شده است.

در ادامه، پس از مرور مرتبط‌ترین فعالیت‌های موجود، مجموعه ویژگی پیشنهادی معرفی شده است و عملکرد آن با به‌کارگیری دو روش مختلف در بخش چهارم سنجیده شده است. درنهایت در بخش انتهایی مقاله، جمع‌بندی و فعالیت‌های پژوهشی پیشنهادی آینده آورده شده است.

۲. پیشینه تحقیق

روش‌های تشخیص نفوذ در سامانه‌های مبتنی بر SIP به روش‌های آماری و روش‌های یادگیری ماشین طبقه‌بندی شده است [۹]. یکی از روش‌های آماری قابل استفاده برای تشخیص نفوذ، تعریف حد آستانه بر روی تعداد تغییر حالت‌های ماشین حالت SIP است که نیازمند تنظیم دقیق پارامترهای مربوطه بر اساس ترافیک پس‌زمینه است [۱۰]. بلوم[1] فیلترها روشی برای کاهش پیچیدگی مکانی نگهداری داده‌های مختلف هستند که با توجه به حجم بالای داده‌های موجود در سرآیند بسته‌های SIP برای تشخیص نفوذ مناسب هستند. با ایجاد تغییر در تعریف این فیلترها و نگهداری شمارنده به جای مقدار باینری کلاسیک در این فیلترها، تشخیص حملات سیل‌آسا در SIP امکان‌پذیر است [۱۱]. مشکل اصلی استفاده از فیلترهای بلوم به عنوان روش تشخیص ناهنجاری، ایجاد هشدار نادرست به علت به‌کارگیری تابع درهم‌ساز[2] در الگوریتم آن است که با به‌کارگیری فهرست سفید امکان حداقل‌سازی آن در چارچوب‌های امنیتی وجود دارد [۱۲]. روش آماری دیگر برای تشخیص حملات سیل‌آسا در SIP تعریف فاصله مجاز بین تعداد پیام‌های مختلف مرتبط است که با به‌کارگیری روش‌های کلاسیک ریاضی نظیر فاصله هلینگر به‌کار گرفته شده است [۱۳و ۱۴]. اصلی‌ترین نقص این کلاس از روش‌های تشخیص نفوذ مربوط به تنظیم حد آستانه پویا در آن‌ها است.

به‌کارگیری روش‌های یادگیری ماشین با تعریف مجموعه ویژگی بر اساس ایجاد یک ماشین حالت جدید برای SIP و توسعه سامانه تشخیص نفوذ مبتنی بر مشخصه رویکرد دیگری است که برای تشخیص حملات اختلال در سرویس‌دهی SIP ارائه شده است [۱۵]. همچنین استخراج داده‌های قابل استفاده از سرورهای پروکسی، ثبت‌نام و رکوردهای مربوط به سامانه صدور صورت حساب در قالب مجموعه ویژگی‌های قابل استفاده برای تشخیص حملات سیل‌آسا در SIP هر چند قابل استفاده است ولی با توجه به تعداد و هزینه محاسباتی بالا قابلیت استفاده زمان واقعی را ندارد [۱۶]. ارائه یک روش و رویکرد سامانه‌ای برای تولید ویژگی از سرآیند SIP با تشخیص انواع حملات اختلال در سرویس‌دهی نگاهی است که می‌تواند به صورت مستقل از نوع حملات و سامانه های یادگیر صورت بگیرد [۹]. تولید ویژگی با توجه به عملکرد حالت طبیعی ماشین حالت SIP و با در نظر گرفتن سناریوهای حمله انجام شود [۹].

به‌کارگیری روش‌های تشخیص مبتنی بر محاسبات آماری و روش‌های یادگیری ماشین، در معماری‌های امنیتی جلوگیری از نفوذ در کاربردهای مبتنی بر SIP بخش دیگری از فعالیت‌های مرتبط را به خود اختصاص می‌دهد. بر این اساس یک سامانه دو لایه برای مقابله با حملات اختلال در سرویس‌دهی در SIP با به‌کارگیری روش تشخیص مبتنی بر ویژگی‌های تولید شده بر اساس ماشین حالت پروتکل تعریف شده است [۱۷]. در لایه اول هدف شناسایی حملات مربوط به رسانه است که با پیاده‌سازی یک دیوار آتش پویا از ورود ترافیک اضافی به سامانه جلوگیری می‌کند. سپس در لایه دوم دفاعی، فیلترهای مخصوص SIP قرار

[1] Bloom

[2] Hash

داده شده است که وظیفه این فیلترها شناسایی حملات سیگنالینگ در SIP است. نقطه قوت طرح پیشنهادی در پیاده‌سازی سخت‌افزاری عملیات فیلترینگ آن است که کارایی بالایی را برای آن به ارمغان آورده است ولی این مسئله کاربرد طرح پیشنهادی را محدود می‌سازد [۱۷]. روش مشابه دیگر برای تشخیص و مقابله با حملات اختلال در سرویس VoIP در لایه اول تلاش برای جلوگیری از حملات سیل‌آسا در لایه کاربردی SIP و نیز در لایه‌های دیگر شبکه بر روی سرور انجام می‌دهد و در لایه دوم نیز اقدام به مقاوم‌سازی پروکسی سرور SIP با بهره‌گیری از ماژول‌های امنیتی اختصاصی کرده است [۱۸]. بررسی نحوه تأثیر حملات اختلال در سرویس بر روی کارایی موجودیت‌های مبتنی بر SIP و ارائه راهکار امنیتی برای مقابله با این نوع حملات تلاش دیگری است با ایجاد تغییرات در معماری ارائه سرویس انجام شده است [۱۹]. همان‌طور که عنوان شد یکی از بزرگ‌ترین مشکلات VoIP، موضوع حملات اختلال در سرویس مبتنی بر حملات سیل‌آسا است که راهکاری عملیاتی برای این موضوع ارائه نشده است و به‌کارگیری راهکارهای مبتنی بر سابقه (فهرست سفید) رویکرد عمومی دیگری است که برای جلوگیری از حملات سیل‌آسا و کاهش آثار مخرب آن‌ها پیشنهاد شده است [۱۹].

در مقاله حاضر با هدف تولید ویژگی‌ها برای تشخیص حملات سیل‌آسا در SIP، از روش مهندسی ویژگی بهره گرفته شده است. ویژگی‌های پیشنهادی در مقاله حاضر قابلیت به‌کارگیری در سامانه‌های تشخیص نفوذ مختلف را به صورت مستقل از نوع سامانه دارا هستند. همچنین انعطاف‌پذیری و کیفیت آن‌ها به گونه‌ای است که در شرایط مختلف ترافیکی و با استفاده از روش های یادگیری ساده‌تر، قادر به شناسایی انواع حملات سیل‌آسا هستند. در ادامه این مقاله به معرفی رویکرد پیشنهادی برای تولید ویژگی مناسب برای تشخیص حملات اختلال در سرویس دهی در SIP پرداخته شده است.

۳. مهندسی ویژگی برای تشخیص حملات سیل‌آسای SIP

موفقیت یک روش و الگوریتم یادگیری ماشین، ارتباط مستقیم با ویژگی‌های به‌کار رفته در آن دارد. به عبارت دیگر نتایج نهایی حاصل شده از به‌کارگیری روش‌های تشخیص ناهنجاری مبتنی بر یادگیری ماشین به صورت مستقیم از کمیت و کیفیت ویژگی‌های ورودی تأثیر می‌پذیرد. هر چند نمی‌توان به صورت قطعی موفقیت یک سامانه تشخیص ناهنجاری را به مجموعه ویژگی آن نسبت داد، ولی تولید و ساخت هوشمندانه ویژگی برای پیش‌بینی حالت های خاص، امکان به‌کارگیری مدل‌های ساده‌تر، منعطف‌تر و رسیدن به نتایج بهتر را نتیجه می‌دهد. در این مقاله با استفاده از دانش موجود در داده‌های مربوط به کاربردهای مختلف مبتنی بر SIP، سه گام زیر برای تولید و ساخت مجموعه ویژگی پیشنهادی به‌کار گرفته شده است:

۱- استخراج داده‌های خام برای تولید ویژگی؛

۲- ساخت و تولید ویژگی با طبقه‌بندی و بسته‌بندی داده‌های خام؛

۳- بررسی عملکرد ویژگی با توجه به مدل یادگیری انتخابی.

در گام اول برای ساخت ویژگی، استخراج داده‌های خام از روی ترافیک VoIP، در سه سطح مختلف بسته‌های SIP (اعم از درخواست و پاسخ)، تراکنش‌های SIP و مکالمه‌های آن استخراج شده است. داده‌های اصلی استخراجی از ترافیک SIP شامل موارد زیر هستند که در یک بازه زمانی مشخص جمع‌آوری می‌شوند:

۱- تعداد و نوع پیام‌های درخواست،

۲- تعداد و نوع پیام‌های پاسخ،

۳- تعداد و مدت زمان تراکنش‌ها،

۴- تعداد پیام‌های موجود در یک تراکنش خاص،

۵- تعداد تراکنش‌های در جریان،

۶- تعداد مکالمه‌های فعال،

۷- مدت زمان مکالمه‌ها.

در گام دوم و سوم از فرایند مهندسی ویژگی با در نظر گرفتن عملکرد طبیعی SIP، ساخت ویژگی‌های مورد نظر انجام شده است. سنجش کیفیت ویژگی‌های تولیدی به صورت مستقل از مدل مورد نظر برای یادگیری و با به کارگیری بر روی مجموعه دادگان موجود انجام شده است. ویژگی‌های تولید شده با به‌کارگیری و تحلیل داده‌های استخراجی به صورت خلاصه در جدول (۱) آورده شده است

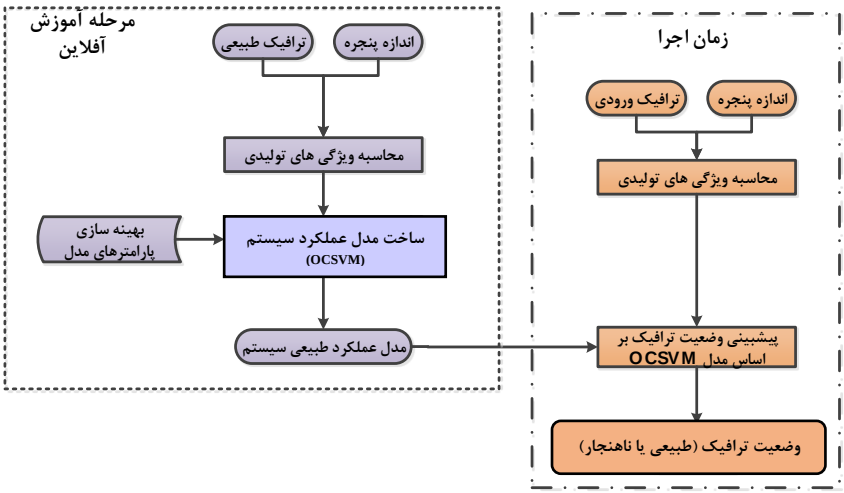
۴. ارزیابی مجموعه ویژگی تولیدی و تحلیل نتایج

در این بخش بررسی کیفیت مجموعه ویژگی تولیدی به صورت مستقل از مدل یادگیر انجام شده است. برای این منظور با هدف نمایش استقلال کارایی مجموعه ویژگی پیشنهادی از مدل یادگیر، دو روش مختلف برای کلاسه‌بندی به‌کار گرفته شده است. در روش اول از یک ماشین بردار پشتیبان تک کلاسی[1] (OCSVM) استفاده شده است. این مدل تنها با به‌کارگیری داده های وضعیت طبیعی پروتکل و به صورت آفلاین آموزش داده می شود. این مدل در زمان اجرا هر گونه انحراف از عملکرد وضعیت طبیعی را با عنوان ناهنجاری گزارش می‌دهد. روش آموزش و به‌کارگیری این مدل در شکل (۴) نمایش داده شده است.

[1] One Class Support Vector Machine

جدول ۱. مجموعه ویژگی تولیدی برای تشخیص حملات سیل‌آسا در SIP

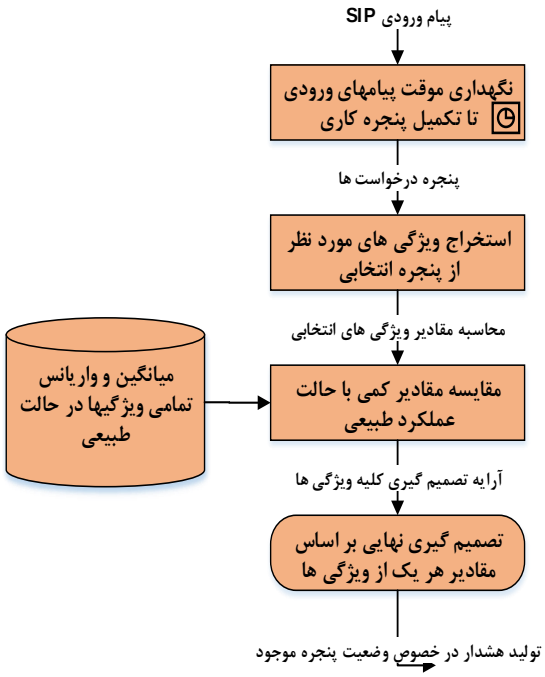
#	ویژگی پیشنهادی	شرح
۱	$\frac{Number\ of\ Requests}{Number\ of\ Packets}$	با توجه به اینکه در یک ارتباط طبیعی، به ازای هر درخواست حداقل یک پاسخ تولید می‌شود، انتظار می‌رود که حداکثر نیمی از بسته‌های SIP از نوع درخواست باشند.
۲	$\frac{Number\ of\ Invite}{Number\ of\ Requests}$	نظر به اینکه تمامی موجودیت‌های مبتنی بر SIP باید به درخواست‌های INVITE پاسخ بدهند، عمده حملات موجود بر روی SIP بر اساس این درخواست ترتیب داده می‌شوند. از آنجایی که تراکنش‌های SIP دارای چند درخواست مختلف و پاسخ به آن‌ها هستند، در یک اتصال طبیعی SIP، نسبت پیام‌های INVITE به کل درخواست‌ها به عنوان یک ویژگی برای شناسایی حالت ناهنجار در نظر گرفته شده است.
۳	$\frac{Number\ of\ 4xx}{Number\ of\ Responses}$	خطاهای کلاینت در موجودیت‌های مبتنی بر SIP با پاسخ‌های کلاس ۴۰۰ مشخص می‌شوند. این پیام های پاسخ در صورت بروز خطا در تحلیل و پردازش منطقی یا نحوی پیام درخواست SIP تولید می شوند. افزایش پیام‌های پاسخ خطا به نسبت کلیه پاسخ‌های موجود، معیاری است که در حالت عادی نباید در ترافیک دیده شود.
۴	$\frac{Number\ of\ 2xx}{Number\ of\ Requests}$	کلاس پیام‌های موفقیت در SIP با شماره ۲۰۰ مشخص می‌شوند. در حالت طبیعی به ازای هر درخواست موفق، یک پاسخ 2xx تولید می‌شود. به همین سبب نسبت پیام‌های پاسخ موفق به کل درخواست‌های ورودی معیاری است که می‌تواند بیانگر عملکرد طبیعی سامانه مبتنی بر SIP باشد.
۵	$\frac{Number\ of\ Transaction}{Number\ of\ Packets}$	پروتکل SIP یک پروتکل حالتمند است که موجودیت‌های مبتنی بر این پروتکل، وضعیت تراکنش‌های خود را با اختصاص حافظه تا مشخص شدن وضعیت نهایی نگهداری می‌کنند. در حالت طبیعی مدت زمان یک تراکنش در حد چند میلی‌ثانیه است و در پروتکل این زمان تا سه دقیقه (۱۸۰ ثانیه) قابل طولانی شدن است (مجموع زمانبندهای مختلف). در حالت عملکرد طبیعی سامانه، هر تراکنش متشکل از یک درخواست و حداقل سه پاسخ است که در حالتی که مهاجم قصد طولانی کردن تراکنش‌ها را داشته باشد، تعداد بسته‌های متعلق به یک تراکنش افزایش می‌یابد.
۶	$\frac{Number\ of\ Receiver}{Number\ of\ Packets}$	تمامی ارتباطات در پروتکل SIP شامل دو بخش تماس گیرنده و تماس شونده است. همچنین تعداد تماس‌های هم‌زمان یک URI عددی محدود است. افزایش تعداد تماس‌های هم‌زمان در یک بازه زمانی محدود از یک فرستنده یا به سمت یک گیرنده به معنای وضعیت ناهنجار در شبکه است (حمله Brute Force).



شکل ۴ . به‌کارگیری ویژگی‌های تولیدی با روش یادگیری مبتنی بر OCSVM

در روش دوم برای نمایش کارایی مجموعه ویژگی تولیدی از یک مدل بسیار ساده مبتنی بر محاسبات آماری استفاده شده است. برای این منظور، مقدار میانگین و واریانس هر یک از شش ویژگی تولیدی در ترافیک طبیعی محاسبه و در زمان اجرا اگر مقدار ویژگی تولیدی خارج از بازه خطای منحنی نرمال باشد (بیشتر از مجموع واریانس و میانگین حالت طبیعی و یا کوچک‌تر از اختلاف آن‌ها)، به عنوان ناهنجار مشخص می‌شود. درنهایت با بررسی وضعیت هر شش ویژگی در هر پنجره زمانی، در خصوص ناهنجار بودن ترافیک پنجره مورد نظر تصمیم‌گیری می‌شود (شکل ۵). نظر به اینکه یکی از عوامل تأثیرگذار در سنجش کارایی عملکرد روش‌های یادگیری، داده‌های ورودی است، به همین سبب سنجش کیفیت مجموعه ویژگی تولیدی با سه مجموعه دادگان مختلف که تنوع کاملی از حملات SIP را دارند، انجام شده است. مجموعه دادگان اول در دانشگاه علم و صنعت ایران جمع‌آوری شده است و شرح جزئیات جمع‌آوری آن در گزارشات قبلی آورده شده است [۷، ۲۰و ۲۱]. دو مجموعه دادگان دیگر در مؤسسه INRIA جمع‌آوری شده است که شرح مربوط به نحوه تولید آن قبلا گزارش شده است [۲۲].

جدول (۲) به صورت خلاصه ترافیک‌های استفاده شده در این بخش از مقاله حاضر را برای سنجش کیفیت مجموعه ویژگی پیشنهادی نمایش می‌دهد. ترافیک‌های انتخابی به گونه‌ای گزینش شده‌اند که تنوع کامل حملات سیل‌آسای SIP را اعم از مبتنی بر پهنای باند، مبتنی بر حافظه و مبتنی بر پردازنده دارا باشند.



شکل ۵. به‌کارگیری ویژگی‌های تولیدی با روش یادگیری ماشین مبتنی بر خطای منحنی نرمال

جدول ۲. مجموعه دادگان به‌کار گرفته شده در بخش ارزیابی عملکرد

#	عنوان	تعداد بسته‌ها	زمان مجموعه داده (ثانیه)	شرح
۱	NRG-Flooding	۱۸۷۰۲	۳۰۰	این مجموعه دادگان شامل ترکیبی از انواع حملات سیل‌آسا در SIP است.
۲	NRG-INVITE	۲۰۲۴۳	۳۰۰	این مجموعه دادگان شامل حملات سیل‌آسای مبتنی بر INVITE در دو سناریوی ساده و پیشرفته است.
۳	NRG-RINGING	۱۶۲۸۷	۳۰۰	این مجموعه دادگان شامل حملات مبتنی بر RINGING برای اشغال حافظه قربانی است.
۴	INRIA-OPENSIPS	۲۳۳۹۶	۱۸۰	این مجموعه دادگان شامل حملات سیل‌آسای ساده و پیشرفته بر روی پروکسی سرور OPENSIPS است.
۵	INRIA-ASTERISK	۲۱۰۹	۱۸۰	این مجموعه دادگان شامل حملات سیل‌آسای ساده و پیشرفته بر روی پروکسی سرور ASTERISK است.

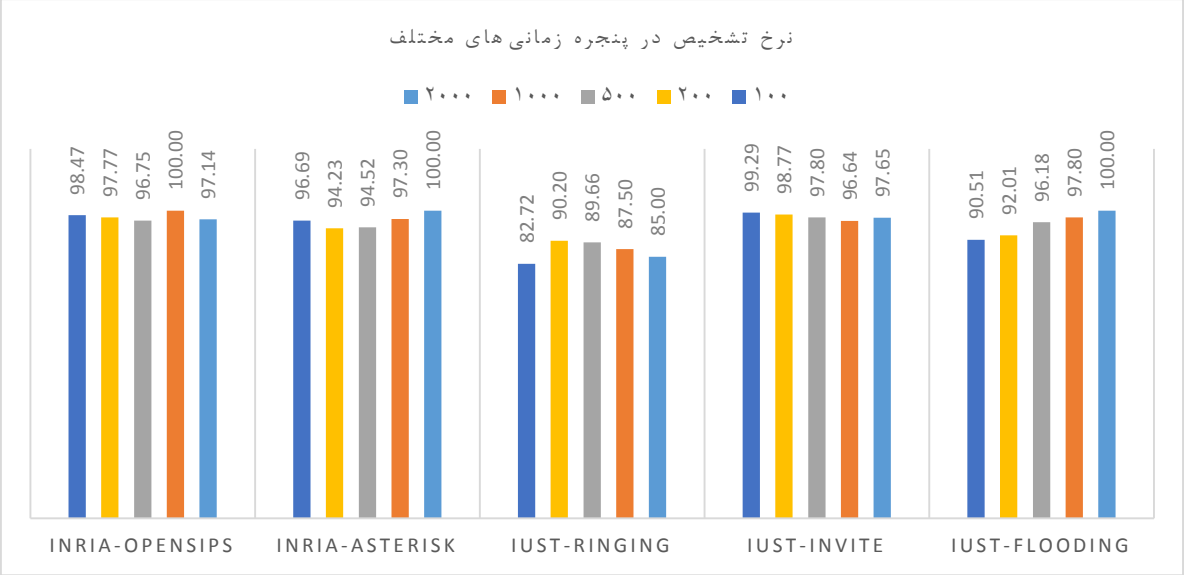
سنجش کارایی مجموعه ویژگی پیشنهادی با به‌کارگیری مجموعه دادگان جدول (۲) و با استفاده از دو روش پیشنهادی برای تشخیص ناهنجاری و با اندازه‌گیری نرخ هشدار نادرست و نرخ تشخیص ناهنجاری انجام شده است. لازم به ذکر است که مقادیر گزارش شده در شکل‌های (۶، ۷ و ۸) با انجام تحلیل ROC[1] بر روی نتایج حاصل از به‌کارگیری روش کلاس‌بندی مورد نظر به‌دست آمده است.

همان‌طور که در شکل (۶ و ۷) نمایش داده شده است، کارایی روش تشخیص ناهنجاری پیشنهادی (نرخ تشخیص و نرخ هشدار نادرست) با به‌کارگیری مجموعه ویژگی تولیدی در تمامی انواع ترافیک‌های تولیدی، عملکرد قابل قبولی داشته است. همچنین نگاه به مقدار هشدار نادرست تولیدی در روش پیشنهادی نیز حاکی از عملکرد مناسب مجموعه ویژگی تولیدی است. به عبارت دیگر در تمامی دسته ترافیک‌های مربوط به حملات مختلف، با انتخاب پنجره زمانی مناسب می‌توان کارایی تقریباً کامل مجموعه ویژگی تولیدی را با روش کلاس‌بندی

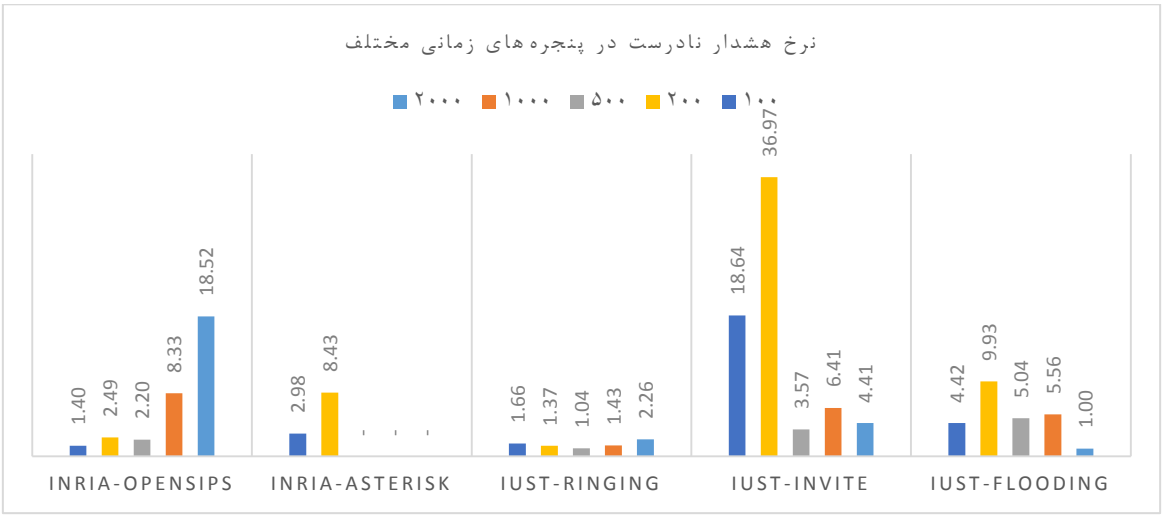
[1]Receiver Operating Curve

عمومی انتخابی داشت. نکته‌ای که در خصوص اندازه پنجره زمانی باید اشاره کرد آن است که انجام عملیات پردازشی بر روی بسته های ورودی به صورت گروهی انجام می‌شود که این موضوع موجب ایجاد تأخیر در ایجاد تماس‌های جدید می‌شود. به عبارت دیگر انتخاب پنجره زمانی با اندازه ۲۰۰ میلی‌ثانیه موجب می‌شود که ایجاد تماس‌های جدید با ۲۰۰ میلی‌ثانیه تأخیر برقرار شوند. با توجه به اینکه محاسبه و به‌کارگیری مجموعه ویژگی‌های پیشنهادی به صورت کاملاً بدون حالت و صرفاً بر روی پیام‌های موجود در پنجره زمانی اخیر انجام می‌شود، تنها پارامتر مهم در انتخاب اندازه پنجره زمانی، نوع کاربرد چندرسانه‌ای است. در کاربردهای تلفنی مانند مقاله حاضر، انتخاب اندازه پنجره کمتر از یک ثانیه هم از نظر کارایی (دقت تشخیص و نرخ هشدار نادرست) و هم از نظر پیچیدگی محاسباتی (تکمیل عملیات پردازش در هر پنجره زمانی)، کیفیت لازم را دارد. همچنین لازم به ذکر است که نتایج گزارش شده در این بخش بدون انجام هیچ بهینه‌سازی و تنظیماتی بر روی روش کلاس‌بندی OCSVM به دست آمده است.

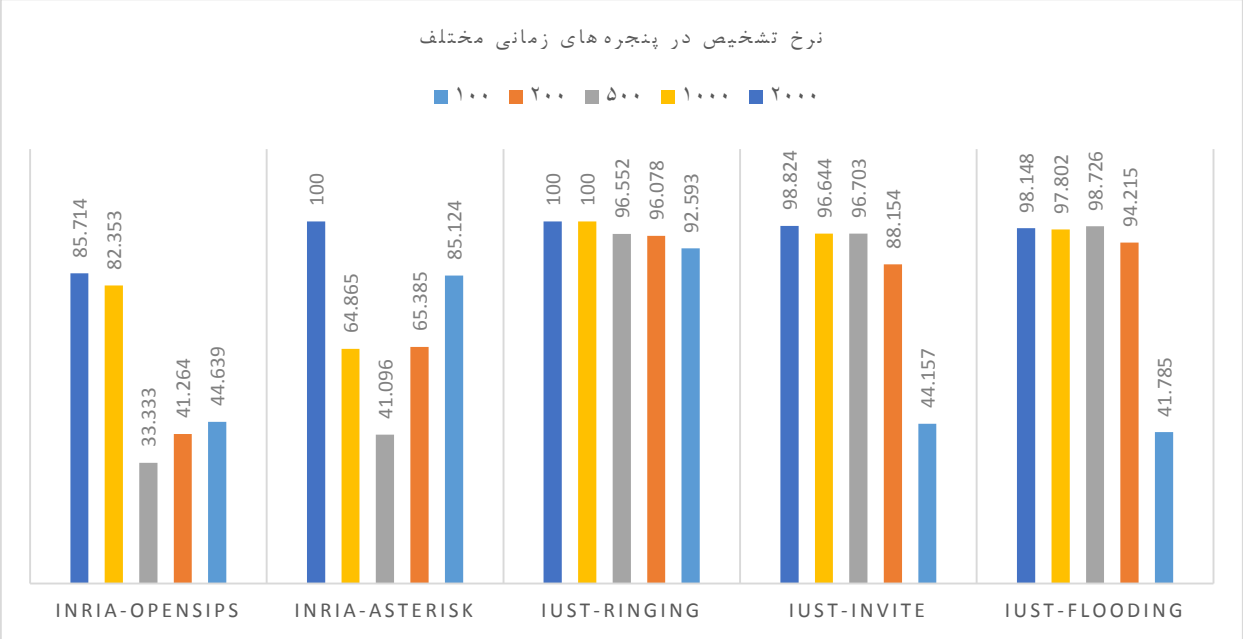
رویکرد مشابه برای نمایش کارایی مجموعه ویژگی پیشنهادی با به‌کارگیری روش کلاس‌بندی خطای منحنی نرمال نیز به‌کار گرفته شد. از آنجایی که هدف از ارزیابی این بخش نمایش کارایی مجموعه ویژگی تولیدی است، تحلیل ROC در این روش به گونه ای انجام شده است که سامانه دارای هشدار نادرست نباشد. همان‌طور که در شکل ۸) نمایش داده شده است، عملکرد تقریباً کامل مجموعه ویژگی‌های پیشنهادی را می‌توان با انتخاب اندازه پنجره زمانی مناسب به‌دست آورد



شکل ۶ . نرخ تشخیص به‌کارگیری مجموعه ویژگی پیشنهادی (روش: OCSVM)



شکل ۷. نرخ هشدار نادرست به‌کارگیری مجموعه ویژگی پیشنهادی (روش: OCSVM)



شکل ۸. نرخ تشخیص به‌کارگیری مجموعه ویژگی پیشنهادی (روش: خطای نرمال)

۵. نتیجه‌گیری

با توجه به اهمیت پروتکل SIP در شبکه‌های نسل آینده و سرویس‌های چندرسانه‌ای و نظر به آسیب‌پذیر بودن موجودیت‌های این پروتکل نسبت به انواع حملات اختلال در سرویس‌دهی و به طور خاص حملات سیل‌آسا، در این مقاله یک مجموعه ویژگی برای تشخیص این حملات پیشنهاد شده است. تولید ویژگی در این مقاله با به‌کارگیری رویکرد مهندسی ویژگی و با استخراج داده از سرآیند متنی SIP و با در نظر گرفتن تعریف تراکنش و مکالمه در این پروتکل انجام شده است. به‌کارگیری مجموعه ویژگی تولیدی در دو روش مختلف تشخیص ناهنجاری با سه مجموعه دادگان متفاوت از انواع حملات سیل‌آسای SIP، کارایی مناسب مجموعه ویژگی پیشنهادی را از نظر نرخ تشخیص ناهنجاری (با میانگین بیش از ۹۴ درصد) و نرخ هشدار نادرست (با میانگین کمتر از ۳ درصد) در یک پنجره زمانی انتخابی (۵۰۰ میلی‌ثانیه) برای به‌کارگیری در سامانه‌های تشخیص ناهنجاری و به‌کارگیری در چارچوب‌های امنیتی مختلف نشان می‌دهد. در ادامه فعالیت‌های پژوهشی این مقاله، به دنبال تولید ویژگی مناسب برای تشخیص حملات پیام‌های بدفرم[1] و تماس‌های مزاحم[2] (SPIT) بر روی پروتکل SIP است.

۶. مراجع

[1] Baset, S. A.; Gurbani, V. K.; Johnston, A. B.; Kaplan, H.; Rosen, B.; Rosenberg, J. D. "The Session Initiation Protocol (SIP): An Evolutionary Study"; J. Communications 2012, 7, 89-105.

[2] RFC3261, SIP: Session Initiation Protocol, 2002.

[3] Keromytis, A. D. "Voice Over IP Security: A Comprehensive Survey of Vulnerabilities and Academic Research"; Springer, 2011.

[4] Asgharian, H.; Akbari, A.; Raahemi, B. "Detecting Flood-Based Attacks Against SIP Proxy Servers and Clients Using Engineered Feature Sets"; Int. J. Inform. & Communication Tech. Research 2016, 8, 33-41.

[5] Ehlert, S.; Geneiatakis, D.; Magedanz, T. "Survey of Network Security Systems to Counter SIP-based Denial-of-Service Attacks"; Elsevier Computers & Security, 2010, 29, 25-243.

[6] Sisalem, D.; Floroiu, J.; Kuthan, J.; Abend, U.; Schulzrinne, H. "SIP Security"; Wiley, 2009.

[7] Asgharian, Z.; Asgharian, H.; Akbari, A.; Raahemi, B. "Detecting Denial of Service Message Flooding Attacks in SIP Based Services"; Amirkabir J. Tech. 2012, 44, 74-81.

[8] Domingos, P. "A Few Useful Things to Know About Machine Learning"; ACM Communications 2012, 55, 78-87.

[9] Asgharian, H.; Akbari, A.; Raahemi, B. "Feature Engineering for Detection of Denial of Service Attacks in Session Initiation Protocol"; Security and Communication Networks 2015, 8, 1587-1601.

[1] Malformed
[2] Spam over Internet Telephone (SPIT)

[10] Asgharian, Z.; Asgharian, H.; Akbari, A.; Raahemi, B. "A Framework for SIP Intrusion Detection and Response Systems"; Proc. of Int. Symposium on Computer Networks and Distributed Systems, 2011.

[11] Geneiatakis, D.; Vrakas, N.; Lambrinoudakis, C. "Utilizing Bloom Filters for Detecting Flooding Attacks Against SIP Based Services"; Computers & Security 2009, 28, 578–591.

[12] Roha, B. H.; Kimb, J. W.; Ryub, K. Y.; Jea-Tek, R. "A Whitelist-Based Countermeasure Scheme Using a Bloom Filter Against SIP Flooding Attacks"; Computers & Security 2013, 37, 46-61.

[13] Tang, J.; Cheng, Y.; Zhou, C. "Sketch Based SIP Flooding Detection Using Hellinger Distance"; Proc. of Global Telecommunications Conference (GLOBECOM), 2009.

[14] Rahul, A.; Prashanth, S. K.; Kumar, B. S.; Arun, G. "Detection of Intruders and Flooding in VoIP Using IDS, Jacobson, Fast and Hellinger Distance Algorithms"; IOSR 2012, 2, 30-36.

[15] Ehlert, S.; Wang, C.; Magedanz, T.; Sisalem, D. "Specification-Based Denial-of-Service Detection for SIP Voice-over-IP Networks"; Proc. of 3rd Int. Conf. on Internet Monitoring and Protection, 2008.

[16] Nassar, M.; State, R.; Olivier, F. "Monitoring SIP Traffic Using Support Vector Machines"; Proc. of 11th Int. Symposium on Recent Advances in Intrusion Detection, 2008.

[17] Ormazabal, G.; Nagpal, S.; Yardeni, E.; Schulzrinne, H. "Secure SIP: A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems"; In Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks, Springer, 2008, 107-132.

[18] Ehlert, S.; Zhang, G.; Geneiatakis, D.; Kambourakis, G.; Dagiuklas, T.; Markl, J.; Sisalem, D. "Two Layer Denial of Service Prevention on SIP VoIP Infrastructures"; Elsevier Computer and Communication, 2008, 31, 2443-2456.

[19] Deng, X.; Shore, M. "Advanced Flooding Attack on a SIP Server"; Availability, Reliability and Security"; Proc. of Int. Conf. on Availability, Reliability and Security, 2009.

[20] Alidoosti, M.; Asgharian, H.; Akbari, A. "Security Framework for Designing SIP Scanner"; Proc. of Iranian Conf. on Electrical Eng. 2013.

[21] Pourmohseni, S.; Asgharian, H.; Akbari, A. "Detecting Authentication Misuse Attacks Against SIP Entities"; Proc. of 10th Int. ISC Conf. on Information Security and Cryptology, 2013.

[22] Nassar, M.; State, R.; Festor, O. "Labeled VoIP Data-Set for Intrusion Detection Evaluation"; Lecture Notes in Computer Science Networked Services and Applications - Engineering, Control and Management, 2010, 6164, 97-106.