نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دوازدهم، شماره ۲، تابستان ۱۴۰۰؛ ص ۲۰۴- ۱۹۷

علمی- پژوهشی

پیش‌بینی پیام رمز نشده در شبکه GSM با استفاده از اطلاعات کانال منطقی SACCH

مهدی تیموری

دانشیار دانشگاه تهران

(دریافت: ۱۳۹۹/۰۴/۱۶، پذیرش: ۱۳۹۹/۰۶/۱۷)

چکیده

استاندارد GSM یک استاندارد تلفن همراه سلولی کماکان پرکاربرد در جهان است. در این استاندارد از خانواده رمزهای A۵ جهت محافظت از داده‌های ارسالی و دریافتی کاربران استفاده می‌شود. تقریباً تمام الگوریتم‌های حمله کاربردی به رمزهای قوی A۵/۱ و A۵/۳ با فرض معلوم بودن بخشی از پیام‌های رمز نشده کاربران طراحی شده‌اند. در این مقاله برای اولین بار روشی جهت پیش‌بینی پیام رمز نشده در کانال منطقی SACCH ارائه می‌شود. روش پیشنهادی مبتنی بر الگوسازی توالی ارسال پیام در مسیر فروسوی کانال SACCH با استفاده از یک زنجیره مارکوف مرتبه اول است. با آزمایش روش پیشنهادی بر روی داده‌های یک شبکه واقعی، برای حدود ۹۹٪ نشست‌ها، پیام رمز نشده به‌صورت صحیح تخمین زده شده است. همچنین متوسط موقعیت پیام رمز نشده صحیح در میان تخمین‌ها برابر ۳/۲۱ است که باعث می‌شود، سرعت رمزشکنی حدود یک‌سوم سرعت رمزشکنی در حالت ایده‌آل باشد.

کلیدواژه‌ها: شبکه GSM؛ رمزگذاری خانواده A۵، پیش‌بینی پیام رمزنشده؛ کانال منطقی SACCH.

Prediction of Plaintext in GSM Network Using the SACCH Logical Channel

M. Teimouri
University of Tehran
(Received: 06/07/2020; Accepted: 07/09/2020)

Abstract

The GSM cellular standard is still widely used worldwide. In this standard, the A5 ciphering algorithms are employed for protecting user data. A5/1 and A5/3 are two variants of A5 ciphering algorithms that are proven to be very powerful. Most known attacks on these ciphering algorithms assume some known plaintext data. In this paper, for the first time, a method of plaintext prediction is proposed for the SACCH logical channel. The sequence of downlink SACCH messages is modeled by a first-order Markov chain. Experiments on a real-world network show a 99% success rate. Moreover, the average position of correct plaintext in all predicted plaintexts is equal to 3.21. So, the speed of cipher cracking is around one-third of the speed of an ideal plaintext prediction system.

Keywords: GSM Network, A5 Ciphering Algorithms, Plaintext Prediction; SACCH Logical Channel

* Corresponding Author E-mail: mehditeimouri@ut.ac.ir

۱- مقدمه

استاندارد GSM[1] یک استاندارد تلفن همراه سلولی است که تا سال ۲۰۱۴ در بیش از ۲۱۹ کشور و منطقه جهان مورد استفاده قرار گرفته است. در این استاندارد از کانال‌های فرکانسی با پهنای باند ۲۰۰ kHz در باندهای فرکانسی ۹۰۰ MHz و ۱۸۰۰ MHz استفاده می‌شود. علاوه بر یک فرکانس اصلی به نام C0، هر ایستگاه مرکزی در این سیستم از تعدادی کانال ترافیکی در کنار این فرکانس اصلی استفاده می‌نماید. ساختار دسترسی در چنین شبکه‌ای به‌صورت TDMA[2]/FDMA[3] است. هر کانال فرکانسی در این استاندارد به ۸ شیار زمانی تقسیم می‌شود. این ۸ شیار زمانی با یک شماره فریم مشخص می‌گردند [۱].

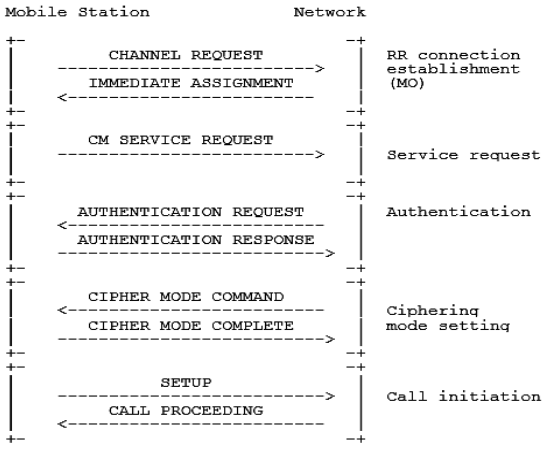
کانال‌های فیزیکی مطابق با قواعد مشخصی به کانال‌های منطقی اختصاص داده می‌شوند. کانال‌های منطقی به سه دسته کلی کانال‌های ترافیکی (TCH[4])، کانال‌های کنترلی (CCH[5]) و کانال پخش سلول (CBCH[6]) تقسیم می‌شوند. دو نوع کانال TCH وجود دارد که توسط نرخ بیت از یکدیگر مجزا می‌شوند: TCH تمام‌نرخ (TCH/F[7]) و TCH نیم‌نرخ (TCH/H[8]). با استفاده از TCH نیم‌نرخ می‌توان تعداد کاربران را نسبت به TCH تمام‌نرخ به دو برابر افزایش داد. این افزایش تعداد کاربران در قبال کاهش کیفیت صوت و یا کاهش نرخ ارسال داده صورت می‌گیرد [۲].

کانال‌های کنترلی برای ارسال داده سیگنالینگ و یا هم‌زمانی به‌کار می‌روند. این کانال‌ها به سه دسته کلی تقسیم می‌شوند. کانال پخش BCH[9] برای ارسال اطلاعات هم‌زمانی (در قالب کانال‌های منطقی FCCH[10]، SCH[11] و BCCH[12]) استفاده می‌شود. کانال کنترلی مشترک CCCH[13] برای فراخوانی موبایل (در قالب PCH[14])، اختصاص کانال کنترلی یا ترافیکی اختصاصی (در قالب AGCH[15]) و یا ارسال درخواست اولیه برای سرویس توسط موبایل (در قالب RACH[16]) استفاده می‌شود. کانال کنترلی اختصاصی DCCH[17] نیز برای سیگنالینگ اختصاصی (در قالب کانال SDCCH[18])، سیگنالینگ کمکی (یا همراه) آهسته مانند کنترل توان (در قالب SACCH[19]) و سیگنالینگ کمکی سریع در حالت برقراری کانال ترافیکی (در قالب FACCH[20]) استفاده می‌شود. کانال سیگنالینگ SDCCH برای ارائه سرویس‌هایی مانند سرویس پیام کوتاه مورد استفاده قرار می‌گیرد. علاوه بر این، این کانال می‌تواند مقدمه‌ای برای اختصاص یک کانال ترافیکی باشد. بعد از ورود به کانال ترافیکی، وظیفه SDCCH را کانال منطقی FACCH به عهده می‌گیرد [۲].

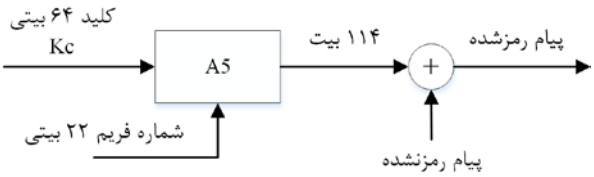
در عمل، پس از احراز هویت کاربر، کانال‌های ترافیکی و کانال کنترلی اختصاصی توسط الگوریتم‌های خانواده A۵ (به‌خصوص رمزگذاری‌های A۵/۱ و A۵/۳) رمزگذاری می‌شوند. به عنوان مثال، در شکل (۱)، فرایند برقراری تماس از سمت کاربر نمایش داده شده است. همان‌طور که ملاحظه می‌شود، در این فرایند، بعد از ورود به کانال اختصاصی و پس از شروع رمزگذاری، موبایل و شبکه به‌ترتیب با ارسال پیام‌های آماده‌سازی[21] و روند تماس[22] فرایند ایجاد تماس را برقرار می‌سازند. در صورتی که تماس موفق باشد، پس از اختصاص کانال ترافیکی توسط شبکه با استفاده از فرمان تخصیص[23]، پیام‌های بعدی ارسالی از سوی شبکه به موبایل پیام‌های اعلام زنگ‌خوردن[24] و اتصال[25] خواهد بود. لازم به‌ذکر است که در این شکل، پیام‌های کانال SACCH نمایش داده نشده است. از همان ابتدای ورود به کانال اختصاصی SDDCH، این پیام‌ها در کانال کمکی SACCH بین کاربر و شبکه ردوبدل می‌گردند [۳].

برای یک سیستم مراقبت یا شنود غیرفعال[26] که دسترسی به متغیرهای الگوریتم رمزگذاری ندارد، اولین قدم اجرای یک حمله و دستابی به کلید مورد استفاده است [۴]. بسیاری از الگوریتم‌های عملی حمله به رمزهای A۵/۱ و A۵/۳ یک فرض بسیار مهم دارند. آن‌ها فرض می‌کنند که برای بخشی از پیام رمزشده دریافتی، پیام رمزنشده[27] متناظر نیز در دسترس است. با استفاده از این موضوع که رمزهای خانواده A۵ از نوع رمزهای جریانی[28] هستند و با توجه به شکل (۲)، با XOR کردن پیام رمزشده و پیام رمزنشده، می‌توان به بلوک‌های ۱۱۴ بیتی خروجی الگوریتم A۵ یا همان جریان کلید[29] دست یافت. برای یافتن کلید Kc نیز با استفاده از این بلوک‌های ۱۱۴ بیتی معلوم حمله انجام می‌شود [۵].

[1] Global System for Mobile Communication
[2] Time-Division Multiple Access
[3] Frequency-Division Multiple Access
[4] Traffic Channel
[5] Control Channel
[6] Cell Broadcast Channel
[7] Full-Rate
[8] Half-Rate
[9] Broadcast Channel
[10] Frequency Correction Channel
[11] Synchronization Channel
[12] Broadcast Control Channel
[13] Common Control Channel
[14] Paging Channel
[15] Access Grant Channel
[16] Random-Access Channel
[17] Dedicated Control Channel
[18] Stand-alone Dedicated Control Channels
[19] Slow Associated Control Channel
[20] Fast Associated Control Channel
[21] SETUP
[22] CALL PROCEEDING
[23] ASSIGNMENT COMMAND
[24] ALERTING
[25] CONNECT
[26] Passive
[27] Plaintext
[28] Stream
[29] Keystream



شکل ۱. مثالی از یک نشست به همراه فرایند احراز هویت و رمزگذاری [۳].



شکل ۲. فرایند رمزگذاری در GSM [۵].

اولین حمله به الگوریتم A5/1 توسط بیریوکوف و شامیر در سال ۱۹۹۹ طراحی شد [۶]. این حمله نیاز به معلوم بودن دو دقیقه از جریان کلید دارد. واگنر و همکارانش این دو دقیقه را به دو ثانیه کاهش دادند [۷]. با این حال زمان پردازش لازم برای رمزشکنی در این طرح‌ها بسیار زیاد است. طرح اکدال و جوهانسون با فرض معلوم بودن دو الی پنج دقیقه جریان کلید، در طی چند دقیقه می‌تواند موفق به شکستن رمز A5/1 شود که کماکان زمان زیادی است [۸].

از آنجا که معلوم بودن جریان کلید مستلزم معلوم بودن اطلاعات رمزنشده است، طرح‌هایی برای حمله به A5/1 بدون معلوم بودن جریان کلید و صرفاً با در دسترس بودن داده رمز شده ارائه شده است. برای مثال در یکی از این طرح‌ها با داشتن هشت ثانیه از اطلاعات رمزشده می‌توان با استفاده از ۲۰۰ کامپیوتر و ۷۰ TB حافظه در زمان واقعی[1] فرایند رمزشکنی را اجرا نمود [۱].

با پیشرفت فناوری و قدرتمندتر شدن سخت‌افزارهای پردازشی، توجه به الگوریتم‌های رمزشکنی مبتنی بر معلوم بودن جریان کلید بیشتر شد. در سال ۲۰۱۰، نول روشی برای رمزشکنی A5/1 ارائه داد که تنها نیاز به معلوم بودن ۶۴ بیت متوالی از یک پیام رمزنشده دارد [۹]. مشابه این طرح در سال ۲۰۱۸ با استفاده از GPU پیاده‌سازی شده است [۱۰].

[1] Real-Time

همان‌طور که نول اشاره کرده است، پیش‌بینی پیام رمز نشده می‌تواند به روش‌های مختلف انجام شود [۹]. ساده‌ترین راه استفاده از فریم‌های زائد[2] ارسالی توسط شبکه است. مشکل این روش این است که با گذر زمان و معلوم‌شدن مشکلات امنیتی سیستم‌های مبتنی بر GSM، ارسال این پیام‌های زائد ثابت در بسیاری از شبکه‌ها عملاً متوقف شده است. به همین دلیل نول اشاره می‌کند که برای رسیدن به پیام‌های معلوم می‌توان به سراغ کانال SACCH رفت که در آن پیام‌های سیستمی مشخص ارسال می‌شود.

تا جایی که ما اطلاع داریم تاکنون هیچ روشی برای پیش‌بینی پیام‌های رمزنشده ارائه نشده است؛ هرچند اولاسکی در سال ۲۰۱۱ [۱۱] و همچنین اخیراً ژنگ در سال ۲۰۱۹ [۱۲] اشاره کرده‌اند که این پیام‌ها با الگوهای مشخصی که وابسته نوع پیاده‌سازی شبکه است، ارسال می‌شوند. در این مقاله، برای اولین بار روشی برای پیش‌بینی پیام رمزنشده در کانال منطقی SACCH ارائه می‌شود. نوآوری‌های این کار را می‌توان به این صورت خلاصه نمود:

- برای اولین بار روشی آماری برای پیش‌بینی پیام رمزنشده در کانال SACCH ارائه می‌گردد که با احتمال بالا می‌تواند چهار بلوک ۱۱۴ بیتی رمزنشده را پیش‌بینی نماید.
- روش پیشنهادی بر روی یک داده واقعی اعمال شده و نتایج مورد ارزیابی قرار می‌گیرند.

ساختار مقاله به این شرح است. در ادامه و در بخش دوم، جزئیاتی از نحوه ارسال اطلاعات در کانال منطقی SACCH مورد بررسی قرار می‌گیرد. در بخش سوم، روش پیشنهادی برای پیش‌بینی پیام رمزنشده ارائه می‌شود. سپس در بخش چهارم عملکرد روش پیشنهادی بر روی یک داده واقعی مورد ارزیابی قرار می‌گیرد. در پایان و در بخش پنجم نیز جمع‌بندی صورت خواهد گرفت.

۲- نحوه تولید و ارسال اطلاعات در کانال SACCH

همان‌طور که در مثال شکل (۱) دیدیم، برای ارائه یک سرویس در شبکه GSM باید فرایندهایی اجرا شود. اجرای فرایندها نیز در حقیقت یک توالی از پیام‌ها هستند که در مسیر فراسو[3] و فروسوی[4] کانال‌های SDCCH و SACCH ارسال می‌گردند. این پیام‌ها، اصطلاحاً پیام‌های لایه ۳ نام دارند. هر پیام لایه ۳ شامل یک یا چند المان اطلاعاتی می‌باشد. هر یک از این المان‌های

[2] Dummy
[3] Uplink
[4] Downlink

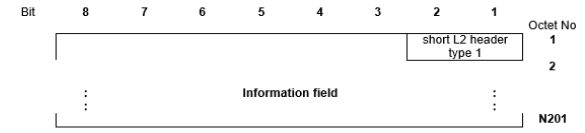
اطلاعاتی می‌تواند شامل یک یا چند متغیر باشد [۱۳]. دو بایت اول تمام پیام‌های استاندارد لایه ۳ دارای ساختار یکسانی هستند. بیت ۱ تا ۴ در هشت‌تایی اول مشخص‌کننده پروتکل پیام است. در تمامی پیام‌های مربوط به نشست‌های صوتی، به‌روزرسانی موقعیت و ارسال پیام کوتاه بیت ۵ تا ۸ در هشت‌تایی اول همگی برابر صفر هستند. هشت‌تایی دوم، نوع پیام را مشخص می‌کند. این هشت بیت در کنار بیت ۱ تا ۴ در هشت‌تایی اول تعیین‌کننده نوع پیام لایه ۳ است.

پیام‌های لایه ۳ در قالب یک یا چند پیام لایه ۲ ارسال می‌گردند [۱۴]. اطلاعات لایه ۲، در پنج قالب مختلف ارسال می‌شوند. در قالب Bbis کل اطلاعات لایه ۲، همان اطلاعات لایه ۳ است. قالب Bbis صرفاً در کانال‌های منطقی BCCH و CCCH استفاده می‌شود. در کانال‌های DCCH نیز از چهار قالب پیام لایه۲ به نام‌های A، B، B4 و Bter استفاده می‌شود. قالب A و B کاملاً شبیه هم هستند. تنها تفاوت آن‌ها در این است که طول اطلاعات لایه ۳ در قالب A صفر است، در حالی که این عدد در قالب B مخالف صفر است (در حقیقت قالب A زمانی استفاده می‌شود که اطلاعاتی برای ارسال در DCCH وجود نداشته باشد). در این دو قالب، بعد از اطلاعات لایه ۳، بیت‌های پُرکننده می‌آیند. برای پر کردن بایت‌های قرار گرفته در قسمت بیت‌های پُرکننده از بیت‌های ۰۰۱۰۱۰۱۱ استفاده می‌شود. طبق استاندارد [۱۴]، ممکن است از بیت‌های تصادفی برای بیت‌های پُرکننده نیز استفاده شود.

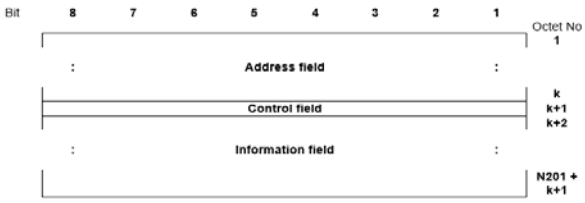
قالب دیگری از پیام لایه ۲، قالب Bter است. قالب Bter می‌تواند در کانال‌های منطقی SACCH و در حالتی که اطلاعاتی برای ارسال وجود دارد استفاده شود. در این حالت، مطابق شکل ۳، دو بیت اول چنین قالبی برابر صفر است و با توجه به اینکه، بیت اول قالب A و B برابر یک است، می‌توان این قالب را از قالب‌های A و B جدا نمود. قالب آخر برای پیام لایه ۲، B۴ نام دارد و ساختار آن مطابق شکل (۴) است. این قالب برای ارسال پیام‌های UI[1] در لینک فروسوی SACCH استفاده می‌شود.

هر پیام لایه۲ توسط یک پیام لایه ۱ منتقل می‌شود [۱۵]. در کانال‌های منطقی BCCH، CCCH و DCCH هر پیام لایه ۱ متشکل از ۲۳ بایت (معادل ۱۸۴ بیت) است. این ۲۳ بایت در قالب ۴۵۶ بیت کدشده و توسط ۴ برست در لایه فیزیکی کدگذاری و ارسال می‌گردد [۱۶]. مطابق با شکل (۵)، در کانال منطقی SACCH، بایت شماره ۳ تا ۲۳ (یعنی B ۲۱) حاوی پیام‌های لایه ۲ است. در این حالت، دو بایت اول پیام لایه ۱ برای مبادله اطلاعات مربوط به هم‌زمانی و توان موبایل به کار می‌رود.

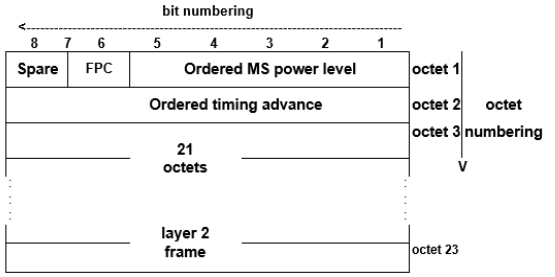
[1] Unnumbered Information



شکل ۳. ساختار بسته‌های لایه ۲ در قالب Bter [۱۴].



شکل ۴. ساختار بسته‌های لایه ۲ در قالب B۴ [۱۴].



شکل ۵. بسته‌های لایه ۱ در کانال فروسوی SACCH [۱۵].

موبایل و ایستگاه مرکزی (BTS[2]) باید در کانال منطقی SACCH ارسال دائمی اطلاعات داشته باشند [۳]. دلیل این موضوع این است که این کانال برای سنجش برقراری ارتباط به کار می‌رود. در مسیر فروسوی این کانال، زمانی که اطلاعات دیگری برای ارسال وجود نداشته باشد، پیام‌های سیستمی نوع ۵ و ۶ (در قالب پیام‌های لایه ۲ نوع UI) ارسال می‌گردد. اگر بیت EXT IND در پیام سیستمی نوع ۵ برابر ۱ باشد، پیام سیستمی نوع bis ۵ هم در مسیر فروسوی کانال SACCH ارسال می‌گردد. پیام سیستمی نوع ter ۵ نیز ممکن است توسط BTS ارسال شود.

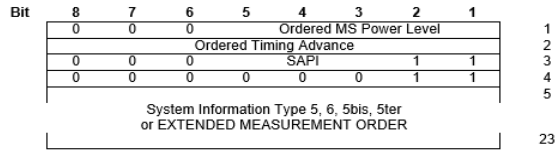
در صورتی که از پیام لایه ۲ با قالب Bter استفاده شود، پیام سیستمی نوع ۱۰ و یا اطلاعات اندازه‌گیری[3] می‌تواند در مسیر فروسو ارسال گردد. در کانال فروسوی SACCH پیام فرمان اندازه‌گیری توسعه‌یافته[4] نیز می‌تواند توسط BTS به موبایل ارسال شود.

در مسیر فراسوی کانال SACCH نیز موبایل مرتباً پیام گزارش اندازه‌گیری[5] را (در قالب پیام‌های لایه ۲ نوع UI) ارسال می‌نماید. موبایل می‌تواند در مسیر فراسو پیام گزارش اندازه‌گیری توسعه‌یافته[6] و همچنین گزارش اندازه‌گیری تقویت شده[7] را نیز ارسال نماید. فاصله بین دو پیام گزارش اندازه‌گیری متوالی نباید بیش از یک پیام لایه ۲ باشد.

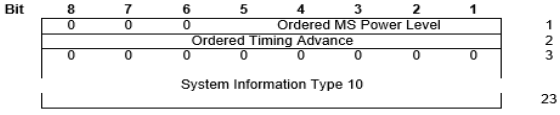
[2] Base Transceiver Station
[3] Measurement Information
[4] Extended Measurement Order
[5] Measurement Report
[6] Extended Measurement Report
[7] Enhanced Measurement Report

۳- روش پیشنهادی برای پیش‌بینی پیام رمزنشده در کانال SACCH

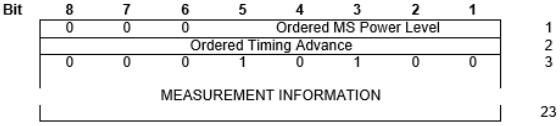
همان‌طور که در بخش قبل گفته شد، در مسیر فراسوی کانال SACCH، پیام گزارش اندازه‌گیری توسعه‌یافته، گزارش اندازه‌گیری تقویت‌شده و یا پیام گزارش اندازه‌گیری ارسال می‌شود. ۱۲۸ بیت (معادل B ۱۶) در این پیام‌ها می‌توانند مقادیر مختلفی اختیار کنند که بسیاری از آن‌ها از یک پیام به پیام دیگر تغییر می‌کنند. لذا احتمال وقوع بسیار پایینی برای هر یک از حالت‌های چنین پیامی وجود دارد. با توجه به این موضوع، بهتر است در مسیر فراسوی کانال SACCH به دنبال پیش‌بینی پیام رمزنشده نباشیم. در مسیر فروسوی کانال SACCH، یکی از پیام‌های سیستمی نوع ۵ و ۶ (و احتمالاً ۵bis و ۵ter) ارسال می‌گردد. احتمال ارسال پیام سیستمی نوع ۱۰، اطلاعات اندازه‌گیری[1] و یا فرمان اندازه‌گیری توسعه‌یافته نیز وجود دارد. ساختار این هفت پیام از یک BTS به BTS دیگر متفاوت هستند، اما انتظار داریم که در یک BTS ساختار این پیام‌ها ثابت باشد. با این حال، دو اول بایت لایهٔ ۱ نیز می‌تواند از یک پیام SACCH به پیام دیگر تغییر نماید. هرچند اگر سرعت حرکت موبایل پایین باشد، انتظار داریم مقدار این دو بایت مانند دو بایت پیام قبلی باشد و یا هر کدام از مقادیر TA[2] و سطح توان فرمان‌داده‌شده یک واحد کم یا زیاد شوند (مجموعاً ۹ حالت که احتمال حالت اول بسیار بالاتر از سایر حالت‌ها است). در شکل‌های (۸- ۶) پیام رمز نشده محتمل در مسیر فروسوی SACCH نمایش داده شده‌اند.



شکل ۶. پیام‌های رمزنشده محتمل در مسیر فروسوی SACCH متناظر با پیام‌های سیستمی نوع ۵، ۶، ۵bis و ۵ter و یا فرمان اندازه‌گیری توسعه افته.



شکل ۷. پیام رمزنشده محتمل در مسیر فروسوی SACCH متناظر با پیام سیستمی نوع ۱۰.



شکل ۸. پیام رمزنشده محتمل در مسیر فروسوی SACCH متناظر با پیام اطلاعات اندازه‌گیری.

با استفاده از توضیحات فوق و همچنین مشاهدات انجام‌شده بر روی شبکه‌های GSM موجود، به طور خلاصه می‌توان گفت:

- تمامی هفت پیام مورد اشاره می‌تواند توسط یک BTS ارسال شود.
- توالی ارسال این پیام‌های وابسته به پیاده‌سازی BTS است؛ با این حال توالی ارسال این پیام‌ها توسط یک الگوی مشخص کنترل شود.
- با توجه به ساختار این پیام‌ها، به نظر می‌رسد محتوای اطلاعات لایه ۲ و ۳ این پیام‌ها برای یک BTS (و در طی یک بازه زمانی که در آن ساختار شبکه تغییر نکند) ثابت می‌باشد. تنها استثناء در این میان پیام اطلاعات اندازه‌گیری است. اگر طول محتوای این پیام بزرگ‌تر از مقدار طول اطلاعات پیش‌بینی‌شده در پیام‌های UI باشد، محتوای این پیام در قالب چند پیام مستقل ارسال می‌شود.
- در طی یک نشست، محتوای اطلاعات لایه ۱ (دو بایت سرایند لایه ۱) مختص به نشست و متفاوت با نشست‌های دیگر است. اما در طی یک نشست انتظار داریم که از یک پیام SACCH به پیام دیگر (به فاصله ۱۰۲ فریم یا حدود ۰/۴۷ s) محتوای اطلاعاتی سرایند لایه ۱ تغییر نکند و یا تغییری جزئی داشته باشد (هر یک از مقادیر TA و سطح توان حداکثر یک واحد کم و یا زیاد شوند).

روش پیشنهادی برای پیش‌بینی پیام رمزنشده در مسیر فروسوی کانال SACCH به این شرح است:

- ابتدا با مشاهده داده‌های ارسالی پیش از شروع رمزگذاری در نشست‌های مختلف، ارسال پیام در مسیر فروسوی کانال SACCH را با استفاده از یک زنجیره مارکوف مرتبه اول با دست‌کم هفت حالت مختلف الگوسازی می‌کنیم. روش الگوسازی به این شکل است که در شروع تمام درایه‌های این ماتریس احتمال انتقال حالت را با صفر مقداردهی می‌کنیم. به ازای هر دو پیام متوالی ارسالی در کانال SACCH، اگر پیام اول و دوم به‌ترتیب متناظر با حالت‌های شماره i و j در الگوی مارکوف باشند، عنصر سطر iام و ستون jام ماتریس احتمال انتقال حالت را یک واحد افزایش می‌دهیم. پس از اتمام بازه مشاهده، هر سطر این ماتریس را بر مجموع اعداد آن سطر تقسیم

[1] به‌دلیل این‌که طول محتوای این پیام می‌تواند بزرگ‌تر از مقدار طول اطلاعات پیش‌بینی‌شده در پیام‌های UI باشد، ممکن است محتوای این پیام در قالب چند پیام مستقل از نوع اطلاعات اندازه‌گیری ارسال شود.

[2] Timing Advance

می‌کنیم. به این ترتیب تخمینی از ماتریس احتمال انتقال حالت این الگوی مارکوف را به‌دست می‌آوریم.

- بعد از الگوسازی کامل زنجیره مارکوف، برای هر نشست، آخرین پیام ارسالی پیش از شروع رمزگذاری در مسیر فروسو را به‌عنوان حالت فعلی زنجیره مارکوف در نظر می‌گیریم.
- حالت‌های بعدی زنجیره مارکوف را با احتمالات متناظر به عنوان پیام‌های رمزنشده محتمل در نظر می‌گیریم.
- متناظر با هر یک از پیام‌های محتمل، مجموعاً ۹ حالت مختلف برای سرایند پیام لایه ۱ در نظر می‌گیریم. احتمال وقوع این ۹ حالت را به شکل شهودی و به این ترتیب تعریف می‌کنیم: احتمال اینکه مقادیر TA و سطح توان تغییر نکنند برابر ۷۰٪؛ احتمال اینکه تنها یکی از مقادیر TA یا سطح توان تغییر کند برابر ۵٪ (چهار حالت)؛ احتمال این‌که هر دو مقدار TA و سطح توان تغییر کند برابر ۲/۵ ٪ (چهار حالت).
- با ضرب احتمال وقوع پیام در احتمال وقوع سرایند، احتمال وقوع تمام پیام‌های ارسالی در کانال SACCH را تعیین کرده و به‌ترتیب نزولی، پیام‌های ۴۵۶ بیتی کدشده متناظر با آن‌ها را به عنوان پیش‌بینی‌های محتمل برمی‌گردانیم.

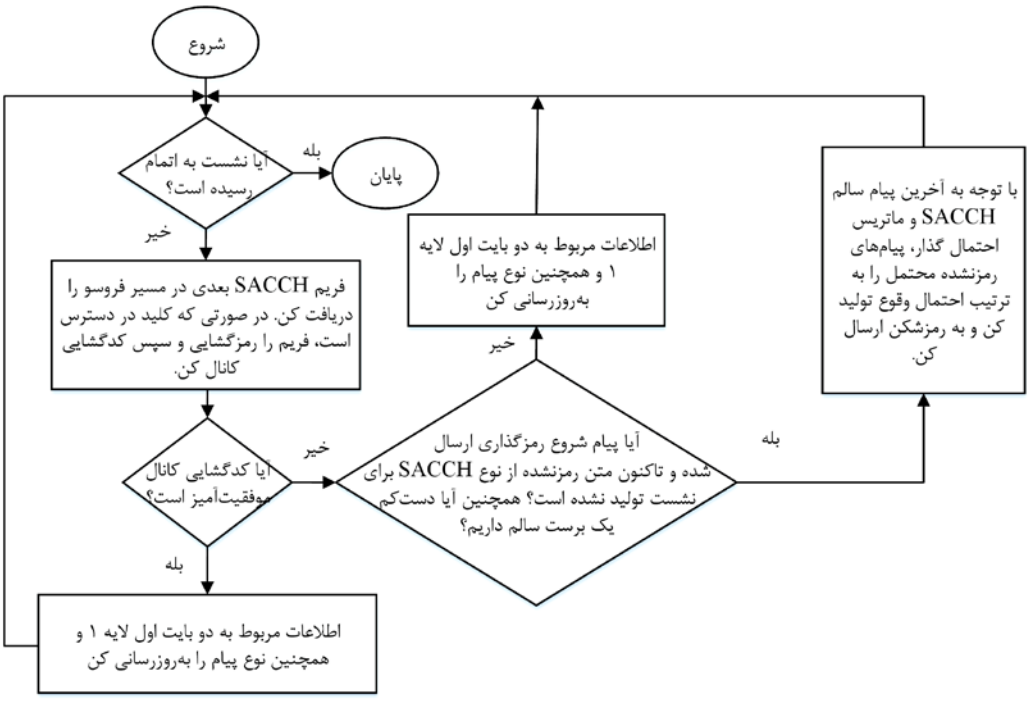
در شکل (۹)، بلوک دیاگرام روش پیشنهادی نمایش داده شده است.

۴- ارزیابی روش پیشنهادی

در این بخش عملکرد روش پیشنهادی را بر روی یک نمونه داده واقعی مورد بررسی و ارزیابی قرار می‌دهیم. این نمونه داده شامل ۶۶۴ نشست مختلف می‌باشد. این نمونه‌ها توسط رادیوی نرم‌افزاری تشریح‌شده در [۱۷] دریافت شده‌اند. متغیرهای رمزگذاری تمامی این نشست‌ها معلوم است. با این حال، از این اطلاعات صرفاً برای ارزیابی صحت عملکرد روش پیشنهادی استفاده می‌شود.

ماتریس احتمال مربوط به زنجیره مارکوف در شروع برابر یک ماتریس تمام صفر تعریف می‌شود. با ملاحظه توالی اطلاعات ارسالی در مسیر فراسوی کانال SACCH، این ماتریس در طی بررسی نشست‌ها به‌روزرسانی می‌گردد. با مشاهده توالی پیام‌های دریافتی در این BTS، مشخص می‌شود که تنها سه نوع پیام سیستمی نوع ۵، 5ter و ۶ ارسال می‌شود. الگوی مارکوف به‌دست‌آمده در این حالت به‌صورت شکل (۱۰) است.

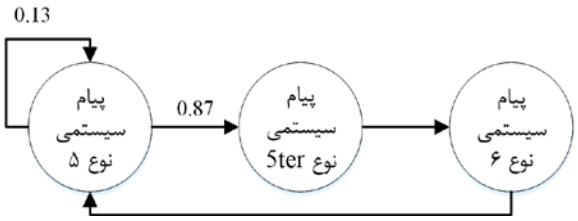
با استفاده از روش پیشنهادی، در تنها ۷ نشست موفق به تخمین درست پیام رمزنشده نیستیم. به عبارت دیگر در حدود ۹۹٪ نشست‌ها، موفق به تخمین درست پیام رمزنشده شده‌ایم. دلیل عدم موفقیت در ۷ نشست از ۶۶۴ نشست این است که سطح توان فرمان‌داده‌شده پس از شروع رمزگذاری بیش از یک واحد کم یا زیاد شده است؛ چیزی که در ساختار پیشنهادی ما مد نظر قرار نگرفته است و البته احتمال رخ دادن آن پایین است.



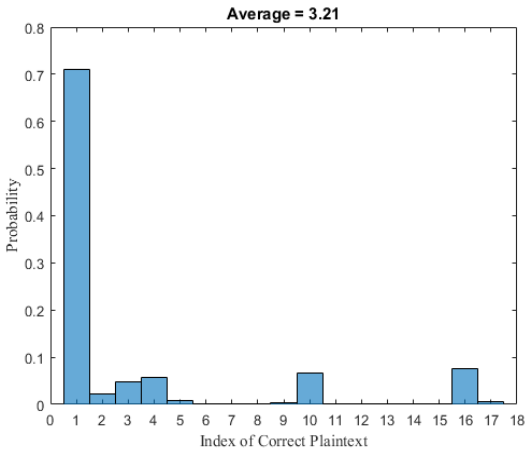
شکل ۹. بلوک دیاگرام روش پیشنهادی.

حضور پیام رمزنشده درست در میان پیش‌بینی‌ها کافی نیست. نکته با اهمیت دیگر این است که این پیام درست، چندمین حدس در میان تمام پیش‌بینی‌های ممکن است. در حقیقت سرعت رمزشکنی رابطه مستقیم با این متغیر دارد. به عنوان مثال اگر در همه نشست‌ها، تمام تخمین‌های درست، دهمین تخمین درست در میان تمام پیش‌بینی‌ها باشند، زمان لازم برای رمزشکنی نسبت به حالتی که اولین تخمین صحیح باشد، ده برابر می‌شود.

از آنجا که در مجموعه داده مورد بررسی، برای تمامی نشست‌ها کلید رمزنگاری معلوم است، می‌توان پس از تخمین پیام رمز نشده، بررسی نمود که آیا این پیام در میان پیام‌های رمز شده بوده است یا خیر؟ همچنین در صورت مثبت بودن پاسخ، محل این پیام مشخص می‌گردد. مجدداً باید تأکید شود که در زمان پیش‌بینی پیام رمز نشده صحیح، صرفاً از پیام‌های پیش از ارسال فرمان رمزگذاری استفاده می‌گردد تا شرایط واقعی به درستی شبیه‌سازی گردد. در شکل (۱۱)، توزیع موقعیت پیام رمزنشده صحیح در میان تمام پیش‌بینی‌ها برای BTS مورد آزمایش نمایش داده شده است. همان‌طور که ملاحظه می‌شود برای این BTS، متوسط موقعیت صحیح برابر ۳/۲۱ است که باعث می‌شود، سرعت رمزشکنی حدود یک‌سوم سرعت رمزشکنی در حالت ایده‌آل باشد. منظور از حالت ایده‌آل، روشی فرضی است که بتواند برای هر نشست پیام رمز نشده را در اولین حدس خود به درستی پیش‌بینی نماید.



شکل ۱۰. الگوی زنجیره مارکوف به‌دست‌آمده برای BTS مورد آزمایش.



شکل ۱۱. توزیع موقعیت پیام رمزنشده صحیح در میان تمام پیش‌بینی‌ها برای BTS مورد آزمایش.

۵- نتیجه‌گیری

در این مقاله برای اولین بار روشی جهت پیش‌بینی پیام رمز نشده در کانال منطقی SACCH شبکه سلولی GSM پیشنهاد شده است. برای این منظور از الگوسازی توالی ارسال پیام در مسیر فروسوی کانال SACCH توسط یک زنجیره مارکوف مرتبه اول استفاده شده است. با استفاده از این روش می‌توان برای هر نشست چهار بلوک ۱۱۴ بیتی رمزنشده را پیش‌بینی نمود. با XOR کردن پیام رمزشده و پیام رمزنشده، می‌توان به چهار بلوک ۱۱۴ بیتی خروجی الگوریتم A۵ دست یافت. این بلوک‌های ۱۱۴ بیتی حاصل می‌توانند برای اجرای حمله بر روی الگوریتم رمزگذاری مورد استفاده قرار گیرند.

با آزمایش روش پیشنهادی بر روی داده‌های یک شبکه واقعی، برای حدود ۹۹٪ نشست‌ها، پیام رمزنشده به‌صورت صحیح تخمین زده شده است. همچنین متوسط موقعیت پیام رمزنشده صحیح در میان تخمین‌ها برابر ۳/۲۱ است که باعث می‌شود، سرعت رمزشکنی حدود یک‌سوم سرعت رمزشکنی در حالت ایده‌آل باشد.

بسته‌های دریافتی SACCH در نشست‌های مورد استفاده در آزمایش‌های این مقاله، همگی دارای نویز بسیار پایینی بودند. لذا مشکلی در کدگشایی آن‌ها به‌وجود نیامد. اما باید توجه داشت که در عمل ممکن است، نویز بالا باشد. در چنین شرایطی می‌توان با توجه به الگوی تکرارشونده ارسال اطلاعات در لینک فروسوی کانال SACCH، از روش ارائه شده در [۱۸] استفاده شود.

با توجه به نتایج به‌دست‌آمده، پیشنهاد می‌شود برای امن‌تر کردن شبکه GSM، از تنوع بیشتری از پیام‌های ارسالی در کانال SACCH استفاده شود. همچنین احتمال وقوع تمامی پیام‌ها در هر لحظه با هم برابر باشد.

۶- مرجع‌ها

[1] Yousef, P. “A Survey and Evaluation of the Current Situation. Institutionen för Systemteknik”; GSM-Security, 2004.

[2] ETSI “05.02: Multiplexing and Multiple Access on the Radio Path”; Digital Cellular Telecommunications System, 1999.

[3] ETSI “04.08: Mobile Radio Interface Layer 3 Specification”; Digital Cellular Telecomsmunication Systems 1999.

[4] Pourebrahim, Y. “Design and Analysis of a New Secure Stream Cipher Algorithm”; Adv. Defence Sci. & Technol. 2014, 5, 81-91.

[5] Buckley, M. E.; Vutukuri, E. K. “Method and System for Security Enhancement for Mobile Communications”; Google Patents, 2016.

[6] Biryukov, A.; Shamir, A. “Real Time Cryptanalysis of the Alleged A5/1 on a PC”; Preliminary Draft, http://cryptome.org/a51-bs.htm 1999.

[7] Biryukov, A.; Shamir, A.; Wagner, D. “Real Time Cryptanalysis of A5/1 on a PC”; Proc. International Workshop on Fast Software Encryption 2000, 1-18.

[8] Ekdahl, P.; Johansson, T. “Another Attack on A5/1”; IEEE Trans. Inform. Theor. 2003, 49, 284-289.

[9] Nohl, K. “Attacking Phone Privacy”; Black Hat USA, 2010, 1-6.

[10] Bulavintsev, V.; Semenov, A.; Zaikin, O.; Kochemazov, S. “A Bitslice Implementation of Anderson’s Attack on A5/1”; Open Engineering 2018, 8, 7-16.

[11] Olawski, M. “Security in the GSM Network”; IPSec. PL. Stream ciphers 2011.

[12] Zhang, B. “Cryptanalysis of GSM Encryption in 2G/3G Networks Without Rainbow Tables”; Proc. Int. Conf. Theory and Application of Cryptology and Information Security, 2019, 428-456.

[13] ETSI. “04.07: Mobile Radio Interface Signalling Layer 3 General Aspects”; Digital Cellular Telecommunication Systems, 1995.

[14] ETSI. “04.06: Mobile Station - Base Station System (MS - BSS) Interface Data Link (DL) Layer Specification”; Digital Cellular Telecommunication Systems, 1994.

[15] ETSI. “04.04: Layer 1 General requirements”; Digital Cellular Telecommunication Systems, 1994.

[16] ETSI. “05.03: Channel Coding”; Digital Cellular Telecommunications System, 1997.

[17] Rakhshanfar, M.; Teimouri, M.; HassanShahi, Z. “Implementation of Software Radio Based on PC and FPGA”; Proc. 2008 4th IEEE Int. Conf. Circuits and Systems for Communications 2008, 633-637.

[18] Heiman, A. “Method and System for Decoding SACCH Control Channels in GSM-Based Systems with Partial Combining”; Google Patents, US20100189201A1, 2012.