Journal of Electronical & Cyber Defence
Vol. 9, No. 3, 2021, Serial No. 35

Prediction of Plaintext in GSM Networks Using the SDCCH Logical Channel

M. Teimouri*

* University of Tehran

(Received: 20/10/2020, Accepted: 30/12/2020)

ABSTRACT

GSM cellular standard is still widely used worldwide. In this standard, 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 SDCCH logical channel. Four possible downlink SDCCH packets, which are RR, UA, SABM, and UI Fill frames, are considered. The matrices of the occurrence positions and probabilities of these packets are learned by observing the network traffic. Four matrices are considered corresponding to four different types of sessions. Experiments on a real-world network show that we can correctly predict on average 2.94 plaintexts for each session. Moreover, the average position of the first correct plaintext in all predicted plaintexts is equal to 1.24. So, the required time for cipher cracking is around 25% more than the time required by an ideal plaintext prediction system.

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

* Corresponding Author Email: mehditeimouri@ut.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۳، پاییز ۱۴۰۰، ص ۴۷- ۳۹

علمی- پژوهشی

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

مهدی تیموری
دانشیار دانشگاه تهران، ایران
(دریافت: ۱۳۹۹/۰۷/۲۹، پذیرش: ۱۳۹۹/۱۰/۱۰)

چکیده

استاندارد GSM یک استاندارد تلفن همراه سلولی کماکان پرکاربرد در جهان است. در این استاندارد از خانواده رمزهای A5 جهت محافظت از داده‌های ارسالی و دریافتی کاربران استفاده می‌شود. تقریباً تمام الگوریتم‌های حمله کاربردی به رمزهای قوی A5/1 و A5/3 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 SDCCH ارائه می‌شود. روش پیشنهادی مبتنی بر یادگیری ماتریس احتمال و محل وقوع هر یک از پیام‌های محتمل RR، UA، SABM و UI Fill Frame در مسیر فروسوی کانال SDCCH است. این ماتریس‌های احتمال برای چهار نوع نشست مختلف تعریف و به‌روزرسانی می‌شوند. با آزمایش روش پیشنهادی بر روی داده‌های یک شبکه واقعی، برای هر نشست به‌طور متوسط ۲/۹۴ پیام رمز نشده به‌طور صحیح تخمین زده شده‌اند. همچنین، متوسط موقعیت پیام رمز نشده صحیح در میان تخمین‌ها برابر ۱/۲۴ است که باعث می‌شود، زمان رمزشکنی به‌طور متوسط حداکثر ۲۵٪ بیشتر از زمان رمزشکنی در حالت ایده‌آل باشد.

کلید واژه‌ها: شبکه GSM؛ رمزگذاری خانواده A5، پیش‌بینی پیام رمز نشده؛ کانال منطقی SDCCH

۱- مقدمه

استاندارد GSM 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 کانال‌هایی فرکانسی با پهنای باند ۲۰۰ کیلوهرتز در باندهای فرکانسی ۹۰۰ و ۱۸۰۰ مگاهرتز 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 FDMA/TDMA است. هر کانال فرکانسی در این استاندارد به ۸ شیار زمانی تقسیم می‌شود. این ۸ شیار زمانی با یک شماره فریم مشخص می‌گردند.

کانال‌های فیزیکی مطابق با قواعد مشخصی به کانال‌های منطقی اختصاص داده می‌شوند. کانال‌های منطقی به سه دسته کلی کانال‌های ترافیکی (TCH)، کانال‌های کنترلی (CCH) و کانال پخش سلول (CBCH) تقسیم می‌شوند. دو نوع کانال TCH وجود دارد که توسط نرخ بیت از یکدیگر مجزا می‌شوند: TCH تمام‌نرخ TCH/F و TCH نیم‌نرخ TCH/H. 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 [۱].

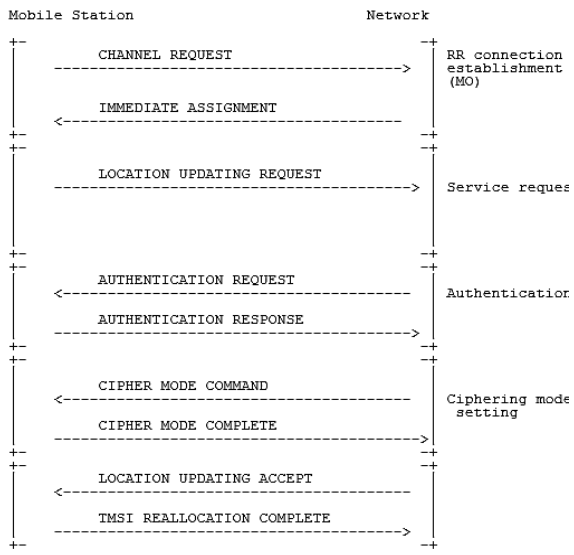
کانال‌های کنترلی برای ارسال داده سیگنالینگ و یا هم‌زمانی به‌کار می‌روند. این کانال‌ها به سه دسته کلی تقسیم می‌شوند. کانال پخش BCH برای ارسال اطلاعات هم‌زمانی (در قالب کانال‌های منطقی FCCH، SCH و BCCH) استفاده می‌شود. کانال کنترلی مشترک CCCH برای فراخوانی موبایل (در قالب PCH)، اختصاص کانال کنترلی یا ترافیکی اختصاصی (در قالب AGCH) و یا ارسال درخواست اولیه برای سرویس توسط موبایل (در قالب RACH) استفاده می‌شود. کانال کنترلی اختصاصی DCCH نیز برای سیگنالینگ اختصاصی (در قالب کانال SDCCH)، سیگنالینگ کمکی (یا همراه) آهسته مانند کنترل توان (در قالب SACCH) و سیگنالینگ کمکی سریع در حالت برقراری کانال ترافیکی (در قالب FACCH) 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 [۱].

در عمل، پس از احراز هویت کاربر، کانال‌های ترافیکی و کانال کنترلی اختصاصی توسط الگوریتم‌های خانواده A5 (به‌خصوص رمزگذاری‌های A5/1 و A5/3) رمزگذاری می‌شوند.

*رایانامه نویسنده مسئول: mehditeimouri@ut.ac.ir

ناشر: دانشگاه جامع امام حسین (ع)

به‌عنوان مثال، در شکل (۱)، فرایند به‌روزرسانی موقعیت نمایش داده شده است. همانطور که ملاحظه می‌شود، در این فرایند، بعد از ورود به کانال اختصاصی و در فاز تبادل، شبکه و موبایل به‌ترتیب با ارسال پیام‌های LOCATION UPDATING ACCEPT و TMSI REALLOCATION COMPLETE فرایند به‌روزرسانی موقعیت را تکمیل می‌کنند. 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 رد و بدل می‌گردند.



شکل (۱): مثالی از یک نشست به‌همراه فرایند احراز هویت و رمزگذاری [۲] .

یکی از مسائل مهم در ارزیابی یک سیستم مخابراتی، میزان مقاومت در برابر نفوذ و دسترسی به اطلاعات کاربران در آن است [۳] . برای یک سیستم مراقبت یا شنود غیرفعال[1] که دسترسی به مؤلفه‌های الگوریتم رمزگذاری ندارد، اولین قدم اجرای یک حمله و دستیابی به کلید مورد استفاده است. بسیاری از الگوریتم‌های عملی حمله به رمزهای A5/1 و A5/3 یک فرض بسیار مهم دارند. آن‌ها فرض می‌کنند که برای بخشی از پیام رمزشده دریافتی، پیام رمز نشده[2] متناظر نیز در دسترس است. با استفاده از این موضوع که رمزهای خانواده A5 از نوع رمزهای جریانی[3] هستند و با توجه به شکل (۲)، با XOR کردن پیام رمز نشده و پیام رمز نشده، می‌توان به بلوک‌های ۱۱۴ بیتی خروجی الگوریتم A5 یا همان جریان کلید[4] دست یافت. برای یافتن کلید Kc نیز با استفاده از این بلوک‌های ۱۱۴ بیتی معلوم حمله انجام می‌شود [۴] .

در اولین حمله به الگوریتم A5/1 توسط بیریوکوف و شامیر در سال ۱۹۹۹ طراحی شد [۵] . این حمله نیاز به معلوم بودن دو دقیقه از جریان کلید دارد. واگنر و همکارانش این دو دقیقه را به دو ثانیه کاهش دادند [۶] . 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 [۷] .

از آنجا که معلوم بودن جریان کلید مستلزم معلوم بودن اطلاعات رمز نشده است، طرح‌هایی برای حمله به A5/1 بدون معلوم بودن جریان کلید و صرفاً با در دسترس بودن داده رمز نشده ارائه شده است. برای مثال در یکی از این طرح‌ها با داشتن هشت ثانیه از اطلاعات رمز نشده می‌توان با استفاده از ۲۰۰ کامپیوتر و ۷۰ ترابایت حافظه در زمان واقعی 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 رمز نشده دارد [۸] . مشابه این طرح در سال ۲۰۱۸ با استفاده از GPU پیاده‌سازی شده است [۹] .

همانطور که نول اشاره کرده است، پیش‌بینی پیام رمز نشده می‌تواند به روش‌های مختلف انجام شود [۹]. ساده‌ترین راه استفاده از فریم‌های زائد ارسالی توسط شبکه است. مشکل این روش این است که با گذر زمان و معلوم شدن 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 رمز نشده ارائه نشده است؛ هرچند اولاسکی در سال ۲۰۱۱ [۱۰] و همچنین اخیراً ژنگ در سال ۲۰۱۹ [۱۱] 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 رمز نشده در کانال منطقی SDCCH ارائه می‌شود. نوآوری‌های این کار را می‌توان به این صورت خلاصه نمود:

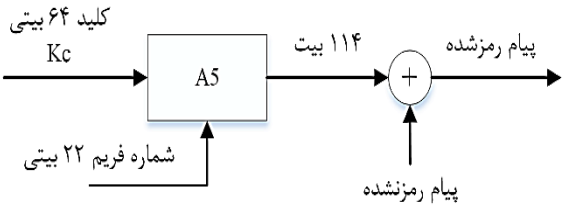
- برای اولین بار روشی آماری برای پیش‌بینی پیام رمز نشده در کانال SDCCH ارائه می‌گردد که با احتمال بالا می‌تواند

[1] Passive
[2] Plaintext
[3] Stream
[4] Keystream

دست‌کم چهار بلوک ۱۱۴ بیتی رمز نشده را پیش‌بینی نماید. لازم به‌ذکر است که چندین سیستم رمزشکنی عملی در دنیا وجود دارد که به احتمال بسیار بالا مبتنی بر پیش‌بینی پیام رمز نشده عمل می‌کنند؛ اما هیچ‌کدام از آنها داده‌ها و روش‌های مرتبط با خود را منتشر نکرده‌اند؛ لذا با جستجو در منابع علمی، هرچند مراجعی مانند مرجع شماره [۱۱] ، به روش کلی کار اشاره می‌کنند؛ ولی هیچ یک روشی منسجم برای این منظور پیشنهاد نداده‌اند.

- 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 SDCCH مورد بررسی قرار می‌گیرد. در بخش سوم، روش پیشنهادی برای پیش‌بینی پیام رمز نشده 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.

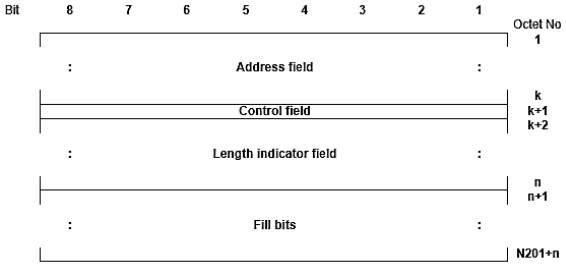


شکل (۲): فرایند رمزگذاری در GSM

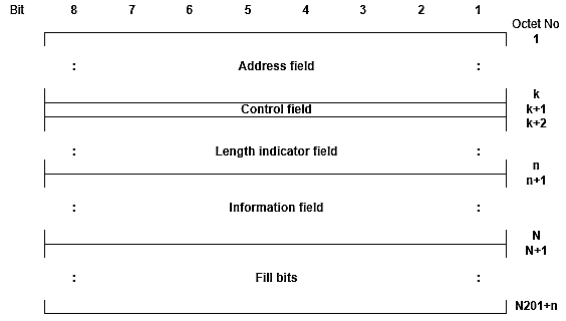
۲- نحوه تولید و ارسال اطلاعات در کانال SDCCH

همانطور که در مثال شکل (۱) مشاهده می‌شود، 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[1] و فروسوی[2] کانال‌های SDCCH و SACCH ارسال می‌گردند. این پیام‌ها، اصطلاحاً پیام‌های لایه ۳ نام دارند. هر پیام لایه ۳ شامل یک یا چند عنصر اطلاعاتی می‌باشد. هر یک از این عنصرهای اطلاعاتی می‌تواند شامل یک یا چند مؤلفه باشد [۱۲] . 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 [۱۳] . 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 لایه ۲ به نام‌های A، B، B4 و Bter استفاده می‌شود. مطابق با شکل‌های (۳ و ۴)، 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 [۱۳] ، ممکن است از بیت‌های تصادفی برای بیت‌های پُرکننده نیز استفاده شود.



شکل (۳): قالب پیام A در لایه ۲ [۱۳].



شکل (۴): قالب پیام B در لایه ۲ [۱۳].

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. قالب آخر برای پیام لایه ۲، B4 نام دارد. این قالب برای ارسال پیام‌های UI[3] در لینک فروسوی SACCH استفاده می‌شود.

[1] Uplink
[2] Downlink
[3] Unnumbered Information

در دو قالب A و B، قبل از اطلاعات لایه ۳، سه بایت (سه هشت‌تایی) قرار دارند که بایت‌های آدرس، کنترل و مشخص‌کننده طول می‌باشند. مطابق شکل (۵)، بایت آدرس شامل بخش‌های زیر است:

۱. بیت اول که برابر یک است.
۲. بیت دوم که بیت فرمان و پاسخ (C/R) است و مطابق با جدول (۱) مقادیر صفر و یک می‌گیرد.
۳. سه بیت بعد، بیت‌های تعیین‌کننده نقطه دسترسی سرویس (SAPI) است که مطابق جدول (۲) صرفاً دو مقدار متفاوت می‌گیرند.
۴. سه بیت پایانی نیز صفر هستند.

بخش کنترل در اطلاعات لایه ۲ قالب A و B، مطابق با شکل (۶)، سه حالت مختلف دارد. این سه حالت، شامل حالت‌های I، S و U است که به ترتیب برای انتقال اطلاعات در حالت عادی (ارسال بسته‌های اطلاعات در حالت عادی)، انتقال اطلاعات در وضعیت مدیریتی و انتقال اطلاعات بدون شماره‌گذاری (وضعیت ارسال بدون تأیید[1]) استفاده می‌شوند. در جدول (۳)، N(S) شماره فریم لایه ۲ ارسال شده است که از صفر تا هفت تغییر می‌کند. همچنین N(R) شماره فریم بعدی است که انتظار می‌رود ارسال‌کننده پیام استفاده نماید. این عدد نیز از صفر تا هفت تغییر می‌کند.

Bit	8	7	6	5	4	3	2	1
	Spare	LPD		SAPI			C/R	EA =1

شکل (۵): ساختار قسمت آدرس لایه ۲ [۱۳].

جدول (۱): معانی مختلف بیت C/R در قسمت آدرس [۱۳].

Type	Direction	C/R value
Command	BS side to MS side	1
	MS side to BS side	0
Response	BS side to MS side	0
	MS side to BS side	1

جدول (۲): معانی مختلف فیلد SAPI در قسمت آدرس [۱۳].

SAPI value	Related entity
0	Call control signalling, mobility management signalling and radio resource management signalling (see 3GPP TS 04.08 and 04.10)
3	Short message service
All others	Reserved for future standardization

Control field bits	8	7	6	5	4	3	2	1
I format	N(R)			P	N(S)			0
S format	N(R)			P/F	S	S	0	1
U format	U	U	U	P/F	U	U	1	1

شکل (۶): ساختار قسمت کنترل لایه ۲ [۱۳].

[1] Unacknowledged

جدول (۳): حالت‌های مختلف قسمت کنترل لایه ۲ [۱۳]

Format	Commands	Responses	8 7	6	5 4 3 2	1
Information transfer	I (information)		N(R)	P	N(S)	0
Supervisory	RR (receive ready)	RR (receive ready)	N(R)	P/F	0 0	0 1
	RNR (receive not ready)	RNR (receive not ready)	N(R)	P/F	0 1	0 1
	REJ (reject)	REJ (reject)	N(R)	P/F	1 0	0 1
Unnumbered	SABM (set asyn-chronous balanced mode)		0 0 1	P	1 1	1 1
		DM (disconnect mode)	0 0 0	F	1 1	1 1
	UI (un-numbered information)		0 0 0	P	0 0	1 1
	DISC (disconnect)		0 1 0	P	0 0	1 1
		UA (un-numbered acknow-ledge)	0 1 1	F	0 0	1 1

مطابق با اطلاعات جدول (۳)، با استفاده از بایت دوم پیام لایه ۲، می‌توان حالت‌های I، S و U را از یکدیگر تفکیک نمود:

۱. اگر بیت اول برابر صفر باشد (بیت ۱ هشت‌تایی دوم پیام لایه ۲)، پیام از نوع I است. این نوع پیام همیشه به عنوان دستور[2] (اطلاعات[3]) ارسال می‌شود؛ یعنی بیت ۲ در هشت‌تایی اول مطابق در حالت دستور تنظیم می‌گردد (مقدار ۱ برای فروسو و مقدار ۰ برای فراسو). هر پیام از نوع I باید حتماً توسط گیرنده و به وسیله یک پیام نوع I و یا S پاسخ داده شود. اگر بیت P در قسمت کنترل پیام I برابر ۱ باشد، حتماً باید پیام S از نوع RR[4] و یا PNR[5] در پاسخ ارسال شود که در آن بیت P/F[6] (که در این حالت در حقیقت بیت F است) برابر ۱ قرار داده شود. در حالتی که بیت P در قسمت کنترل پیام I برابر ۰ باشد و گیرنده پیام نوع I‌ای برای ارسال نداشته باشد، باید پیام S از نوع RR و یا PNR در پاسخ ارسال شود که در آن بیت F برابر ۰ است.

۲. اگر چهار بیت اول برابر ۰۰۰۱ باشد، پیام لایه ۲ از نوع RR است. این پیام برای اعلام آمادگی جهت دریافت داده استفاده می‌شود. بیت پنجم نیز بیت P/F است. در حالتی که فریم از نوع فرمان باشد، این بیت بیت P است و در حالتی که فریم لایه ۲ از نوع پاسخ باشد، این بیت بیت F است. وقتی فرستنده بیت P را برابر ۱ قرار دهد، گیرنده باید یک فریم پاسخ لایه ۲ ارسال نماید. در چنین حالتی، گیرنده در پاسخ یک فریم پاسخ با بیت F برابر ۱ ارسال می‌کند. در این نوع پیام لایه ۲ قسمت اطلاعات وجود ندارد.

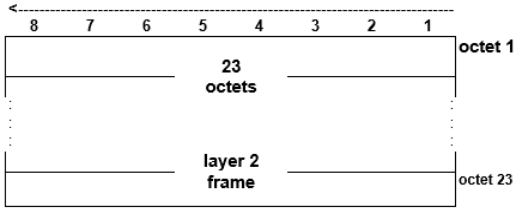
۳. اگر چهار بیت اول برابر ۰۱۰۱ باشد، پیام لایه ۲ از نوع PNR است. این پیام برای SAPI برابر ۰ و ۳ استفاده نمی‌شود. در این نوع پیام لایه ۲ قسمت اطلاعات وجود ندارد.

[2] Command
[3] Information
[4] Receive Ready
[5] Receive Not Ready
[6] Polling/Final

۴. اگر چهار بیت اول برابر ۱۰۰۱ باشد، پیام لایه ۲ از نوع REJ[1] است. این پیام برای درخواست ارسال مجدد فریم شماره N(R) است. در این نوع پیام لایه ۲ قسمت اطلاعات وجود ندارد.

۵. اگر دو بیت اول دارای مقدار ۱۱ باشد، به معنی پیام‌هایی است که شماره‌گذاری ندارند. این نوع پیام‌ها چند دسته هستند که توسط بیت ۶ تا ۸ بایت دوم از یکدیگر تفکیک می‌گردند. دو نوع از این پیام‌ها، پیام SABM (پیام از نوع فرمان) و UA (پیام از نوع پاسخ) است که در درخواست سرویس و رفع ابهام به‌کار می‌رود (این نوع پیام‌ها نمی‌توانند پیام لایه ۳ قطعه‌بندی‌شده ارسال نمایند). پیام دیگر پیام از نوع فرمان DISC است که برای قطع ارتباط مورد استفاده قرار می‌گیرد. پیام دیگر پیام از نوع پاسخ DM است که نشان می‌دهد که امکان دریافت پیام لایه ۲ وجود ندارد. در پیام‌های لایه ۲ نوع DISC و DM قسمت اطلاعات وجود ندارد. پیام مهمی که در این دسته وجود دارد، پیام نوع UI[2] است. این نوع پیام برای انتقال اطلاعات بدون نیاز به تأیید گیرنده است. همچنین این نوع پیام می‌تواند برای ارسال بسته خالی (در زمانی که اطلاعاتی برای ارسال وجود ندارد) مورد استفاده قرار گیرد.

هر پیام لایه ۲ توسط یک پیام لایه ۱ منتقل می‌شود [۱۴] . 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 [۱۵] . مطابق با شکل (۷)، در کانال‌های منطقی BCCH، CCCH، SDCCH و FACCH تمامی این ۲۳ بایت، همان پیام‌های لایه ۲ است.



شکل (۷): ساختار بسته‌های لایه ۱ در کانال‌های SDCCH، FACCH، BCCH و CCCH

۲-۱- امکان پیش‌بینی پیام رمز نشده در مسیر فراسوی کانال SDCCH

اولین پیام رمز نشده‌ای که در کانال SDCCH ارسال می‌شود، پیام CIPHERING MODE COMPLETE است که توسط کاربر ارسال می‌گردد. این پیام قاعدتاً با فرمت لایه ۲ از نوع I ارسال می‌گردد. اگر در پیام CIPHERING MODE COMMAND ارسالی از سمت BTS، از موبایل خواسته شده باشد که IMEISV خود را ارسال ننماید، CIPHERING MODE COMPLETE ساختاری بسیار ساده، مشخص و با اندازه دو بایت خواهد داشت. با این توصیف، یک پیام محتمل در مسیر فراسوی SDCCH در شکل (۸) نمایش داده شده است. مؤلفه‌های این پیام به‌صورت زیر تنظیم می‌شوند:

- SAPI: با توجه به این‌که پیش از شروع نشست ارسال و یا دریافت پیامک فرایند تنظیم وضعیت رمزگذاری اجرا می‌شود، مقدار SAPI در این پیام برابر ۰ است.
- N(R): شماره فریم پیام بعدی که قرار است از سمت شبکه ارسال گردد.
- N(S): شماره فریم فعلی ارسالی توسط موبایل است.

Bit	8	7	6	5	4	3	2	1	
	0	0	0	SAPI (000)			0	1	1
	0	0	0	0	0	0	1	0	2
	N(R)			P		N(S)		1	3
	0	0	0	0	0	1	1	0	4
	0	0	1	1	0	1	0	1	5
	Fill Bits								6
									23

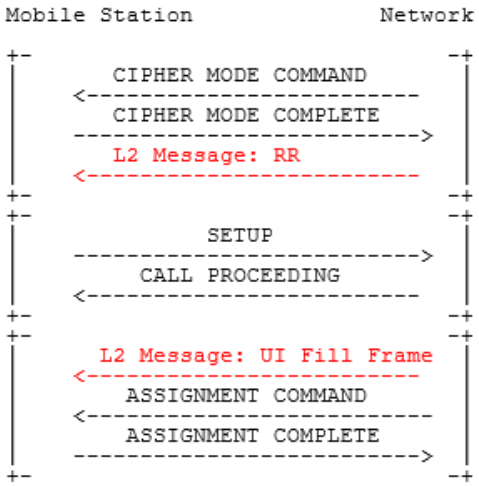
شکل (۸): پیام محتمل ارسالی در مسیر فراسوی SDCCH (پیام CIPHERING MODE COMPLETE)

۲-۲- امکان پیش‌بینی پیام رمز نشده در مسیر فروسوی کانال SDCCH برای نشست‌های صوتی از مبدأ موبایل و نشست‌های پیامکی

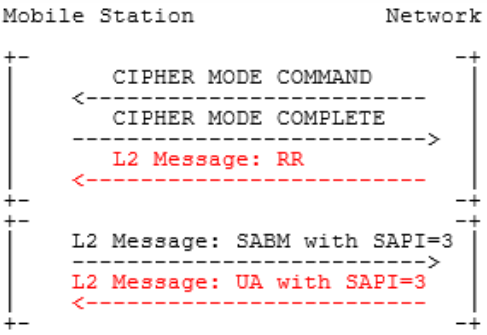
در این نشست‌ها، بعد از ارسال پیام CIPHERING MODE COMPLETE از سمت موبایل، از آنجا که شبکه پیام لایه ۲ از نوع I برای ارسال ندارد، باید دریافت صحیح پیام دریافتی از موبایل را با ارسال یک پیام S از نوع RR اعلام نماید؛ (شکل‌های (۹، ۱۰و ۱۱) مشاهده شود). در شکل (۱۲) این پیام نمایش داده شده است. مؤلفه‌های این پیام به‌صورت زیر تنظیم می‌شوند:

- N(R): شماره فریم پیام بعدی که قرار است از سمت موبایل ارسال گردد (به عنوان مثال اگر بعد از درخواست سرویس، تنها احراز هویت و فرمان رمزگذاری اجرا شده باشد، این عدد برابر ۲ است).
- SAPI: با توجه به اینکه پیش از شروع نشست ارسال و یا دریافت فرایند تنظیم وضعیت رمزگذاری اجرا می‌شود، مقدار SAPI در این پیام برابر ۰ است.
- F: برابر مقدار بیت P در پیام لایه ۲ حاوی CIPHERING MODE COMPLETE است.

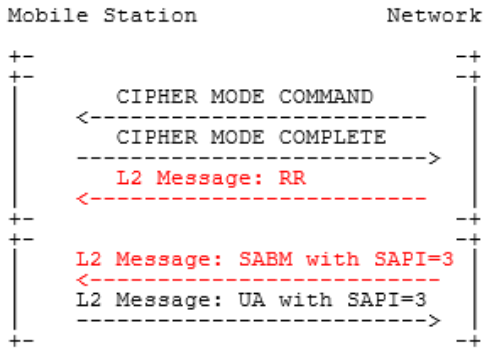
[1] Reject
[2] Unnumbered Information



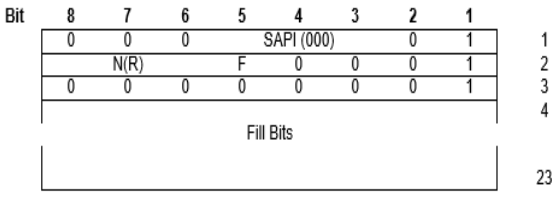
شکل (۹): امکان پیش‌بینی پیام رمزنشده در مسیر فراسوی کانال SDCCH طی فرایند برقراری تماس از سمت موبایل [۲]



شکل (۱۰): امکان پیش‌بینی پیام رمزنشده در مسیر فراسوی کانال SDCCH طی فرایند ارسال پیامک از سمت موبایل [۲]



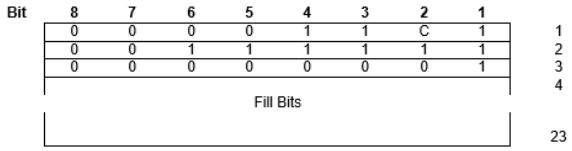
شکل (۱۱): امکان پیش‌بینی پیام رمزنشده در مسیر فراسوی کانال SDCCH طی فرایند ارسال پیامک از سمت شبکه [۲]



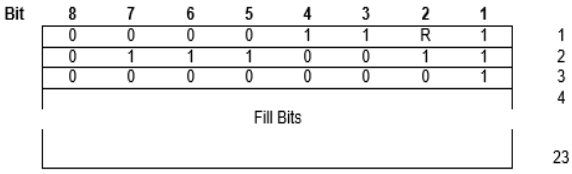
شکل (۱۲). پیام محتمل ارسالی در مسیر فراسوی SDCCH متناظر با تصدیق دریافت پیام CIPHERING MODE COMPLETE

۲-۳- امکان پیش‌بینی پیام رمز نشده در کانال SDCCH برای نشست‌های پیامکی

طبق استاندارد [۱۶] ، در نشست‌هایی که برای تبادل پیامک برقرار می‌شوند، بعد از تنظیم وضعیت رمزگذاری، پیام‌های SABM و UA بین موبایل و شبکه تبادل می‌شود؛ (شکل‌های (۱۰ و ۱۱) مشاهده شود). از آنجا که نیازی به ارسال پیام لایه ۳ در این حالت وجود ندارد، ساختار این پیام‌ها بسیار ساده و به‌صورت آنچه در شکل‌های (۱۳ و ۱۴) نشان داده شده است خواهد بود. در شکل (۱۳) اگر پیام از سمت شبکه ارسال شده باشد مقدار C= ۱ استفاده می‌شود و در غیر این صورت مقدار C= ۰ مورد استفاده قرار خواهد گرفت. در شکل (۱۴) نیز اگر پیام از سمت موبایل ارسال شده باشد مقدار R= ۱ استفاده می‌شود و در غیر این صورت مقدار R= ۰ مورد استفاده قرار خواهد گرفت.



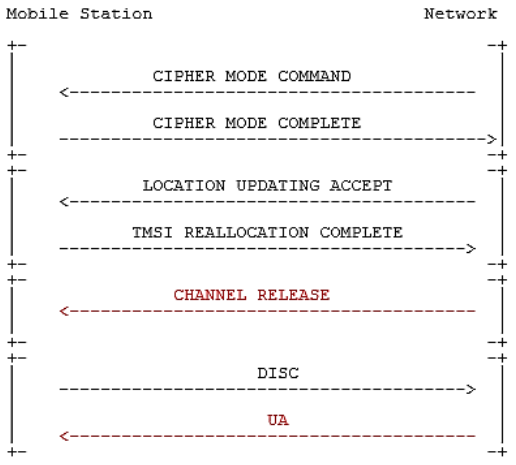
شکل (۱۳): ساختار پیام SABM ارسالی پس از تنظیم وضعیت رمزگذاری در نشست‌های پیامکی



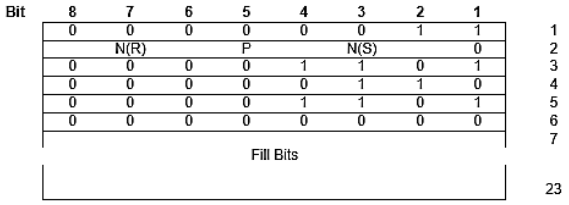
شکل (۱۴): ساختار پیام UA ارسالی پس از تنظیم وضعیت رمزگذاری در نشست‌های پیامکی.

۲-۴- امکان پیش‌بینی پیام رمز نشده در مسیر فروسوی کانال SDCCH برای نشست‌های به‌روزرسانی موقعیت

زمانی که نشستی برای به‌روزرسانی موقعیت اجرا می‌شود، همانطور که در شکل (۱۵) ملاحظه می‌شود، بعد از تنظیم وضعیت رمزگذاری، بعد از پیام‌های LOCATION UPDATING ACCEPT و TMSI REALLOCATION COMPLETE، پیام CHANNEL RELEASE از سمت شبکه ارسال می‌شود. در صورتی که بخش‌های اختیاری این پیام توسط شبکه مورد استفاده قرار نگیرد، ساختار این پیام آن چیزی است که در شکل (۱۶) نشان داده شده است. با توجه به ساختار پیچیده این پیام (وجود دو فیلد متغیر N(R) و N(S))، پیشنهاد می‌شود که از پیام UA ارسالی در تأیید فرمان DISC به عنوان پیش‌بینی استفاده شود.



شکل (۱۵): امکان پیش‌بینی پیام رمزنشده در مسیر فراسوی کانال SDCCH طی فرایند به‌روزرسانی موقعیت [۲]



شکل (۱۶): ساختار پیام محتوی CHANNEL RELEASE

۲-۵- ارسال Fill Frames در نشست‌های صوتی

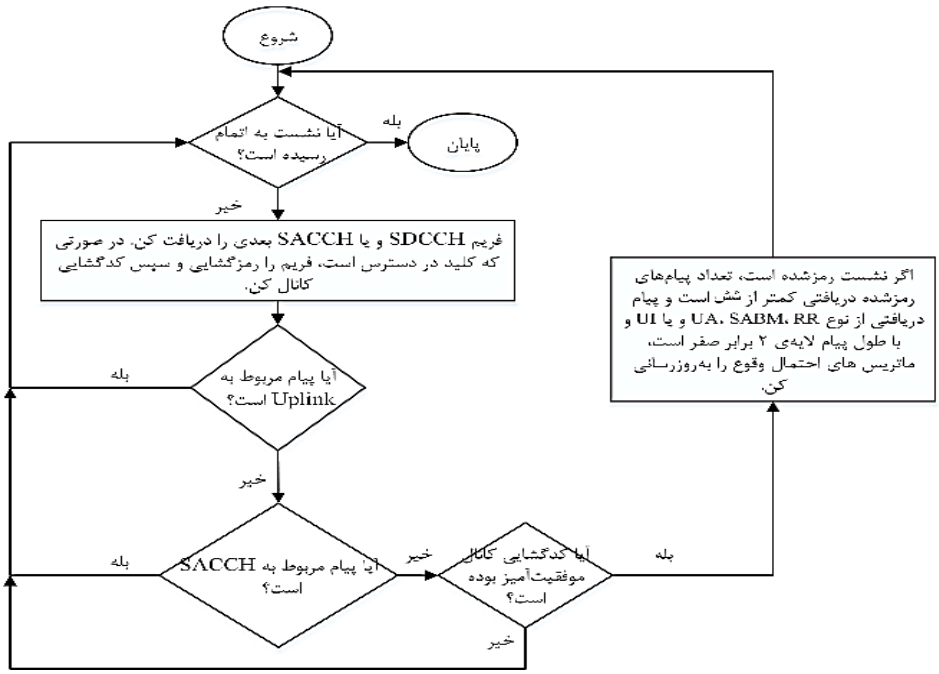
در زمان‌هایی که شبکه در حال تصمیم‌گیری در طی نشست است و پیامی برای ارسال ندارد، ممکن است بسته‌های خالی در قالب UI (با SAPI= ۰ و P= ۰) ارسال نماید. ارسال چنین بسته‌هایی بستگی به پیاده‌سازی شبکه دارد و تنها با مشاهده نشست‌های مختلف می‌توان احتمال رخداد و همچنین محل رخداد آن را تعیین نمود.

۳- روش پیشنهادی برای پیش‌بینی پیام رمز نشده در کانال SDCCH

با جمع‌بندی نتایج بخش قبل و همچنین مشاهدات انجام‌شده بر روی داده‌های واقعی، روش پیشنهادی برای پیش‌بینی پیام رمز نشده در کانال SDCCH به‌طور خلاصه به‌صورت زیر قابل بیان است:

- با توجه به اینکه در بسیاری از نشست‌ها احتمال رسیدن به اطلاعات بدون خطا در مسیر فراسو بسیار پایین است، از مسیر فروسو برای پیش‌بینی پیام رمز نشده استفاده می‌کنیم.
- مطمئن‌ترین گزینه‌ها در مسیر فروسوی SDCCH پیام‌های لایه ۲ شامل RR، UA، SABM و UI Fill Frame هستند.
- در فرایند برقراری تماس و یا ارسال پیامک از سمت شبکه پیام‌های RR و SABM محتمل‌تر هستند.
- در فرایند برقراری تماس از سمت موبایل پیام RR محتمل‌تر است.
- در فرایند ارسال پیامک از سمت موبایل پیام‌های UA و RR محتمل‌تر هستند.
- در فرایند به‌روزرسانی موقعیت پیام UA محتمل‌تر است.
- بسته به پیاده‌سازی شبکه و همچنین شرایط نشست، ارسال پیام UI Fill Frame نیز در هر یک از انواع نشست‌های فوق محتمل است.
- محل ارسال این پیام‌ها قطعی نیست؛ اما با یادگیری ترافیک شبکه می‌توان با احتمال بالا محل دقیق را پیش‌بینی نمود.
- نشست‌ها را به چهار دسته ۱- برقراری تماس و یا ارسال پیامک از سمت شبکه، ۲- برقراری تماس از سمت موبایل، ۳- ارسال پیامک از سمت موبایل و ۴- به‌روزرسانی موقعیت تقسیم می‌کنیم.
- برای هر دسته از نشست‌ها، با مشاهده تدریجی ترافیک شبکه، احتمال وقوع هر یک از پیام‌های محتمل را به همراه فاصله آن از پیام CIPHERING MODE COMMAND در یک ماتریس احتمال ذخیره می‌کنیم. به‌دلیل محدودیت در پردازش و همچنین فرصت محدود برای رمزشکنی، باید سقفی برای حداکثر تعداد پیام‌های مورد بررسی بعد از پیام CIPHERING MODE COMMAND در نظر بگیریم. این سقف به‌صورت تجربی برابر شش در نظر گرفته می‌شود.
- با توجه به اینکه باید هر نشست رمزگشایی شود تا بتوان از محتوای آن برای به‌روزرسانی ماتریس‌های احتمال استفاده نمود؛ باید مقادیر اولیه مناسبی برای ماتریس‌های احتمال در نظر بگیریم.
- در ماتریس‌های احتمال وقوع اولیه، تمام محل‌های وقوع به همراه پیام مورد انتظار برای وقوع را با احتمال یکسان تعریف می‌کنیم. انتظار داریم که با گذر زمان، این ماتریس‌های احتمال به‌روزرسانی‌شده به‌خوبی رفتار شبکه را پیش‌بینی کنند.

در شکل (۱۷) بلوک دیاگرام روش پیشنهادی آورده شده است.



شکل (۱۷): بلوک دیاگرام روش پیشنهادی.

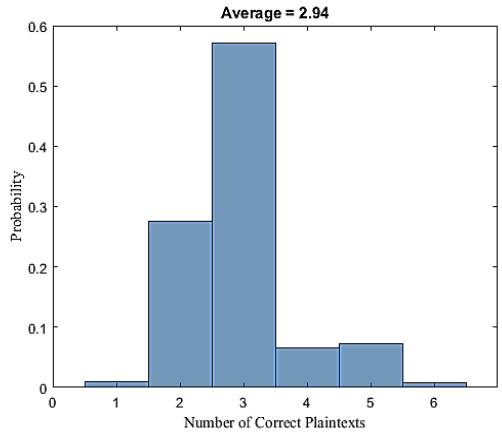
۴- ارزیابی روش پیشنهادی

در این بخش عملکرد روش پیشنهادی بر روی یک نمونه داده واقعی، مورد بررسی و ارزیابی قرار می‌گیرد. این نمونه داده، شامل ۶۶۴ نشست مختلف می‌باشد که توسط پژوهشگاه مخابرات و الکترونیک نصر فراهم شده است. این نمونه‌ها توسط رادیوی نرم‌افزاری تشریح شده در [۱۷] دریافت شده‌اند. مؤلفه‌های رمزگذاری تمامی این نشست‌ها معلوم است. با این حال، از این اطلاعات صرفاً برای ارزیابی صحت عملکرد روش پیشنهادی استفاده می‌شود.

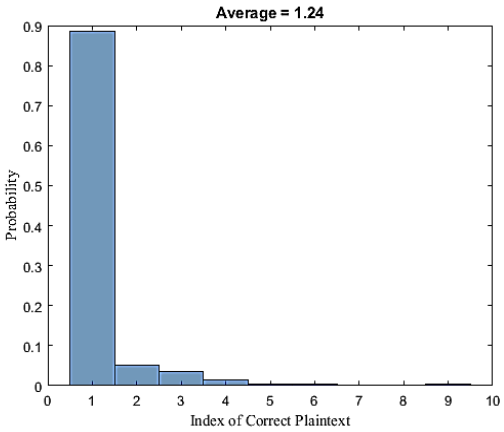
از آنجا که در مجموعه داده مورد بررسی، برای تمامی نشست‌ها کلید رمزنگاری معلوم است، می‌توان پس از تخمین پیام رمز نشده، بررسی نمود که آیا این پیام در میان پیام‌های رمز نشده بوده است یا خیر؟ همچنین در صورت مثبت بودن پاسخ، محل این پیام مشخص می‌گردد. مجدداً باید تأکید شود که در زمان پیش‌بینی پیام رمز نشده صحیح، صرفاً از پیام‌های پیش از ارسال فرمان رمزگذاری استفاده می‌گردد تا شرایط واقعی به درستی شبیه‌سازی گردد.

در شکل (۱۸) توزیع تعداد پیام رمز نشده صحیح در میان تمام پیش‌بینی‌ها برای BTS مورد آزمایش نمایش داده شده است. همانطور که ملاحظه می‌شود، برای هر نشست به‌طور متوسط ۲/۹۴ پیام رمز نشده به‌طور صحیح تخمین زده شده‌اند.

حضور پیام رمز نشده درست در میان پیش‌بینی‌ها کافی نیست. نکته با اهمیت دیگر این است که اولین پیام درست، چندمین حدس در میان تمام پیش‌بینی‌های ممکن است. در حقیقت سرعت رمزشکنی رابطه مستقیم با این مؤلفه دارد. به‌عنوان 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. در شکل (۱۹)، توزیع موقعیت اولین پیام رمز نشده صحیح در میان تمام پیش‌بینی‌ها برای BTS مورد آزمایش نمایش داده شده است. همانطور که ملاحظه می‌شود برای این BTS، متوسط موقعیت صحیح برابر ۱/۲۴ است که باعث می‌شود، زمان رمزشکنی حدود ۲۵٪ بیشتر از زمان 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 (۱۸): توزیع تعداد پیام رمز نشده صحیح در میان تمام پیش‌بینی‌ها برای BTS مورد آزمایش.



شکل (۱۹): توزیع موقعیت اولین پیام رمز نشده 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 SDCCH شبکه سلولی GSM پیشنهاد شده است. برای این منظور، با مشاهده تدریجی ترافیک شبکه، احتمال وقوع هر یک از پیام‌های محتمل RR، UA، SABM وUI Fill Frame به‌همراه فاصله آن از پیام CIPHERING MODE COMMAND در یک ماتریس احتمال ذخیره می‌شود. این کار برای چهار نوع نشست به‌طور مجزا انجام می‌شود: ۱- برقراری تماس و یا ارسال پیامک از سمت شبکه، ۲- برقراری تماس از سمت موبایل، ۳- ارسال پیامک از سمت موبایل و ۴- به‌روزرسانی موقعیت. در ماتریس‌های احتمال وقوع اولیه، تمام محل‌های وقوع به‌همراه پیام مورد انتظار برای وقوع، با احتمال یکسان تعریف می‌شود. با گذر زمان، ماتریس‌های احتمال به‌روزرسانی شده به خوبی رفتار شبکه را پیش‌بینی خواهند کرد.

با استفاده از این روش، می‌توان برای هر نشست دسته‌کم یک پیام را که شامل چهار بلوک ۱۱۴ بیتی رمز نشده است، پیش‌بینی نمود. با XOR کردن پیام رمز نشده و پیام رمز نشده، می‌توان به چهار بلوک ۱۱۴ بیتی خروجی الگوریتم A5 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 هر نشست به‌طور متوسط ۲/۹۴ پیام رمز نشده به‌طور صحیح تخمین زده شده‌اند. همچنین، متوسط موقعیت پیام رمز نشده صحیح در میان تخمین‌ها برابر ۱/۲۴ است که باعث می‌شود، زمان رمزشکنی حدود ۲۵٪ بیشتر از زمان رمزشکنی در حالت ایده‌آل باشد.

۶- مراجع

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

[2] ETSI. “04.08: Mobile Radio Interface Layer 3 Specification,” Digital Cellular Telecommunication Systems 1999.

[3] S. Ahmadiyan and M. Teimouri. “Blind Estimation of Number of Users in TDMA Networks Using Redundancy of Adaptive Channel Coding,” Electronic and Cyber Defense. vol. 6, pp. 11-20, 2018.

[4] E. P. Barkan, E.Biham. “Cryptanalysis of ciphers and protocols,” Computer Science Department, Technion, 2006.

[5] A. Biryukov, A. Shamir. “Real time cryptanalysis of the alleged A5/1 on a PC ,” preliminary draft"; URL: http://cryptome.org/a51-bs.htm 1999.

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

[7] P. Ekdahl, T. Johansson, “Another attack on A5/1,” IEEE transactions on information theory. vol. 49, pp. 284-289,2003.

[8] K. Nohl, “Attacking phone privacy,” Black Hat USA, pp.1-6,2010.

[9] V. Bulavintsev, A. Semenov, O. Zaikin, S. Kochemazov, “A bitslice implementation of Anderson’s attack on A5/1,” Open Engineering, vol.23 8, pp. 7-16,2018.

[10] M. Olawski, “Security in the GSM network"; IPSec. pl. Stream ciphers 2011.

[11] B. Zhang, “Cryptanalysis of GSM Encryption in 2G/3G Networks Without Rainbow Tables,” Proc. International Conference on the Theory and Application of Cryptology and Information Security. pp. 428-456, 2019.

[12] ETSI. “04.07: Mobile radio interface signalling layer 3 General aspects,” Digital Cellular Telecommunication Systems 1995.

[13] ETSI. “04.06: Mobile Station - Base Station System (MS - BSS) interface Data Link (DL) layer specification,” Digital Cellular Telecommunication Systems 1994.

[14] ETSI. “04.04: Layer 1 General requirements"; Digital Cellular Telecommunication Systems 1994.

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

[16] ETSI. “04.11: Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface"; Digital Cellular Telecommunication Systems 1996.

[17] Rakhshanfar, M.; Teimouri, M.; HassanShahi, Z. “Implementation of software radio based on PC and FPGA,” Proc. 2008 4th IEEE International Conference on Circuits and Systems for Communications. pp.633-637,2008.

Prediction of Plaintext in GSM Network using SDCCH Logical Channel

Mehdi Teimouri

University of Tehran

(Received: ……..; Accepted: ……)

Abstract

GSM cellular standard is still widely used worldwide. In this standard, 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 SDCCH logical channel. Four possible downlink SDCCH packets, which are RR, UA, SABM, and UI Fill frames, are considered. The matrices of the occurrence positions and probabilities of these packets are learned by observing the network traffic. Four matrices are considered corresponding to four different types of sessions. Experiments on a real-world network show that we can correctly predict on average 2.94 plaintexts for each session. Moreover, the average position of the first correct plaintext in all predicted plaintexts is equal to 1.24. So, the required time for cipher cracking is around 25% more than the time required by an ideal plaintext prediction system.

Keywords: GSM network, A5 ciphering algorithms, plaintext prediction; SDCCH logical channel