چهارمین کنفرانس انجمن رمز ایران
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران
انجمن رمز ایران
Iranian Society of Cryptology

پروتکل احراز اصالت تکامل‌یافته برای شبکه GSM

هانی صالحی سیچانی
دانشگاه صنعتی اصفهان
hni_salehi@hotmail.com

مهدی برنجکوب
دانشگاه صنعتی اصفهان
brnjkb@cc.iut.ac.ir

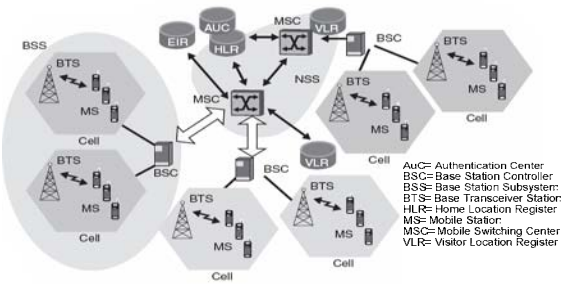
علی فانیان
دانشگاه صنعتی اصفهان
alifanian@gmail.com

چکیده: با گسترش استفاده از شبکه‌های بی‌سیم سلولی، برقراری امنیت در این شبکه‌ها به یک ضرورت اجتناب ناپذیر تبدیل شده است. شبکه *GSM* که نمونه‌ای پر کاربرد از شبکه‌های بی‌سیم سلولی است، دارای نقاط ضعف زیادی در مسائل امنیتی می‌باشد. از جمله این مشکلات امنیتی می‌توان به احراز اصالت یکطرفه در این شبکه اشاره نمود که در روند احراز اصالت، تنها دستگاه موبایل برای شبکه احراز اصالت می‌شود. همچنین در این پروتکل، پهنای باند شبکه بر اثر ترافیک پیامهای کنترلی مربوط به احراز اصالت، به هدر رفته و باعث افزایش زمان برقراری تماس می‌گردد. در این مقاله ابتدا امنیت شبکه *GSM* به طور اجمال بررسی شده است و پس از آن راه‌کاری ارائه خواهد شد که در آن نه تنها احراز اصالت دوطرفه امکان پذیر می‌شود، بلکه زمان برقراری تماس و پهنای باند مصرفی شبکه هم کاهش می‌یابد.

واژه های کلیدی: ارتباطات بی‌سیم، *GSM*، امنیت شبکه، احراز اصالت، احراز اصالت دوطرفه، ترافیک تبادلات کنترلی، تسلا.

۱- مقدمه

GSM[1] که در دهه ۱۹۸۰میلادی در اروپا به منصه ظهور رسید، امروزه در بیشتر نقاط جهان پیاده‌سازی شده است و مشترکان بسیاری از این شبکه استفاده می‌کنند[1]. در ساختار *GSM*، دستگاه موبایل (*MS*) از طریق اتصال رادیویی با ایستگاه پایه (*BS*) در ارتباط است [1,2]. *BS* تنها ارسال‌کننده و دریافت‌کننده امواج رادیویی است و عملیات کنترلی چند *BS* را یک کنترل کننده ایستگاه پایه (*BSC*) انجام می‌دهد. *BSC* از طریق مرکز رهیابی موبایل (*MSC*) به دو پایگاه داده در شبکه، ثبات محل اقامت (*HLR*) و ثبات محل ملاقات (*VLR*)، متصل می‌شود. *HLR* محل ذخیره اطلاعات مشترکان محلی و *VLR* محل ذخیره اطلاعات کاربرانی است که فعلا در ناحیه تحت پوشش *VLR* قرار دارند. مرکزاحراز اصالت (*AuC*) کلیدهای مخفی کاربران (*Ki*) را برای تولید پارامترهای احراز اصالت درخواستی *HLR*، نگهداری می‌کند. در شکل ۱ ساختار شبکه مشاهده می‌شود:



شکل ۱: ساختار شبکه *GSM*

[1] *Global System for Mobile communication*

در شبکه *GSM*، پروتکل احراز اصالت به صورت درخواست/پاسخ است که در این روش، شبکه درخواستی را برای موبایل ارسال می‌کند و موبایل با ارسال پاسخ صحیح، می‌تواند خود را به شبکه احراز اصالت نماید. مشکل اصلی این پروتکل عدم احراز اصالت شبکه نزد موبایل است و بنابراین یک خرابکار به سادگی می‌تواند از طریق حمله ایفای نقش، خود را به جای شبکه اصیل جا بزند. با استفاده از این حمله، دشمن می‌تواند شناسه *IMSI* کاربر را بدست آورد و با ارسال درخواست‌های متعدد و برقراری حمله تصادم [3]، به کلید مخفی کاربر، *Ki*، دست پیدا کند.

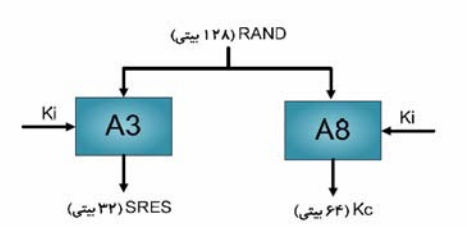
در این مقاله، پروتکلی برای احراز اصالت در شبکه *GSM* با استفاده از پروتکل تسلا[2] ارائه می‌شود که در آن، شبکه بی‌سیم نیز برای موبایل احرازاصالت می‌گردد. از سوی دیگر روش پیشنهادی تعداد پیامهای کنترلی احراز اصالت را کاهش می‌دهد و بدین طریق علاوه بر کاهش استفاده از پهنای باند شبکه، تأخیر ناشی از احراز اصالت و زمان برقراری تماس نیز کاهش می‌یابد.

۲- پروتکل احراز اصالت GSM

در این بخش، ابتدا پروتکل احراز اصالت *GSM* و چگونگی احراز اصالت کاربر به شبکه مورد بررسی قرار می‌گیرد. سپس به معایب و مشکلات موجود در پروتکل احراز اصالت پرداخته و در ادامه، کارهای اصلاحی صورت گرفته برای برطرف نمودن مشکلات امنیتی این پروتکل شرح داده می‌شود.

۲-۱ معرفی پروتکل

همانطور که بیان شد، احراز اصالت در شبکه *GSM* از طریق ارسال یک درخواست از سوی شبکه برای موبایل و وارسی پاسخ دریافتی از موبایل صورت می‌گیرد. درخواست ارسال شده از سوی شبکه برای سیم‌کارت، عدد تصادفی ۱۲۸ بیتی *RAND* است که در سیم‌کارت با اعمال تابع *A3* بر روی آن و کلید خصوصی *Ki*، پاسخ ۳۲ بیتی *SRES* تولید می‌شود و برای شبکه (*VLR*) ارسال می‌گردد. همین ورودی‌ها نیز به الگوریتم *A8* وارد شده و کلید جلسه *Kc* تولید می‌شود. از این کلید در الگوریتم *A5* برای رمزنگاری داده‌های اتصال مستقیم و معکوس استفاده می‌شود. در شکل ۲ فرایند تولید *SRES* و K_C نشان داده شده است:



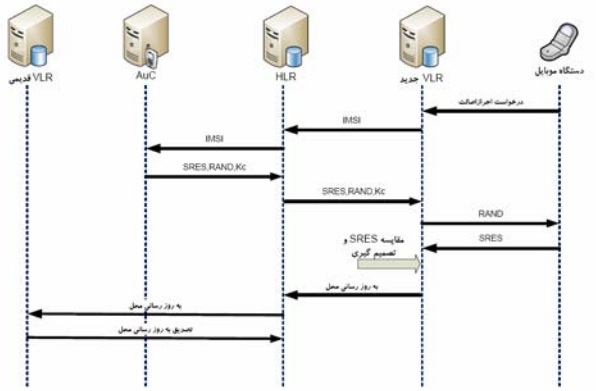
شکل ۲: تولید *SRES* و *Kc* در سیم‌کارت و مرکز *AuC*

روند احراز اصالت در شبکه، مطابق شکل ۳، به این صورت است که دستگاه موبایل ناحیه جاری (*LA*[3]) خود را درون سیم‌کارت ذخیره می‌کند. ناحیه هر *BS* از طریق کانال همه‌پخشی در آن سلول ارسال می‌شود. بنابراین در صورتی که *LA* یک موبایل عوض شود او این موضوع را متوجه شده و بلافاصله درخواست احراز اصالت را از طریق کانال *SDCCH*[4] برای *BS* ارسال می‌کند. این درخواست شامل شماره شناسه *LA* قدیمی کاربر و شناسه موقت (*TMSI*) کاربر می‌باشد. شناسه موقت کاربر در *VLR* به شناسه دائم کاربر (*IMSI*) نگاشت می‌شود و برای *HLR* ارسال می‌شود. او هم با استفاده از این شناسه، از *AuC* تقاضای سه‌تایی‌های احراز اصالت را برای این کاربر خاص می‌کند و مرکز *AuC* در پاسخ، تعداد *n* (به صورت پیش‌فرض ۵ تا) سه‌تایی *{SRES,RAND,Kc}* را برای *HLR* ارسال می‌کند و او هم این پارامترها را برای *VLR* می‌فرستد[4].

VLR در هر مرحله احراز اصالت از یکی از این سه‌تایی ها استفاده می‌کند و با ارسال *RAND* آن برای موبایل، منتظر پاسخ *SRES* سیم‌کارت می‌ماند تا با دریافت پاسخ موبایل و مقایسه آن با *SRES*ی که از *HLR* دریافت کرده بود، در صورت یکسان بودن دو پارامتر، موبایل را احراز اصالت کند. از سوی دیگر در صورتی که *LA* موبایل عوض شده باشد، بایستی پیام "به روز رسانی محل" به *VLR* قدیمی هم ارسال شود. توجه کنید که احراز اصالت نه تنها در هنگام تغییر *LA*، بلکه در هنگام برقراری تماس یا پاسخ به تماس رسیده هم صورت می‌گیرد که در این شرایط بعد از عملیات احراز اصالت، به موبایل یک کانال ترافیکی[5] برای برقراری مکالمه تخصیص داده می‌شود.

[2] *Tesla (Time Efficient Stream Loss tolerant Auth.)*

[3] *Location Area*
[4] *Standalone Dedicated Control Channel*
[5] *Traffic Channle (TCH)*



شکل ۳ : پیامهای کنترلی مربوط به احراز اصالت کاربر در شبکه *GSM*

۲-۲- نارسایی‌های پروتکل و مرور کارهای صورت گرفته

پروتکل احراز اصالت *GSM* دارای نقاط ضعف زیادی است که برخی از اهم آنها عبارتند از:

- عدم احراز اصالت ایستگاه‌پایه یا به عبارت دیگر *VLR* برای دستگاه موبایل
- زیادبودن پهنای باند مصرفی میان *VLR* و *HLR*
- فضای حافظه بالای مورد نیاز در *VLR*
- تحمیل سرباره پردازشی بر روی *HLR* در هنگام احرازهویت موبایل

برای رفع این مشکلات، تاکنون پروتکل‌های احراز اصالت زیادی ارائه شده است. در [5] پروتکلی جهت احراز اصالت کاربران با استفاده از کلمه عبور آنها ارائه شده است. در این روش کاربران ناچارند برای هر بار استفاده از موبایل، کلمه عبور خود را وارد کنند. از سوی دیگر این پروتکل از الگوریتمهای رمزکلیدعمومی استفاده می‌کند که برای استفاده در موبایل بهینه نیست. در [6] برای جلوگیری از حمله ازکاراندازی‌سرویس[6] و از دست رفتن تمامی کانالهای ترافیکی موجود روشی پیشنهاد شده است. این روش هر چند از این حمله بر روی کانالهای شبکه جلوگیری می‌کند اما حجم محاسبات و حافظه زیادی را بر روی شبکه تحمیل می‌نماید و شبکه ناچار است که به صورت پیوسته پیامهایی را در هر ناحیه، همه‌پخشی نماید و منتظر درخواستهای رسیده از موبایلها بماند. در [7] پروتکلی برای احراز اصالت دوسویه ارائه شده است که در آن کاربران بعد از تهیه بلیط، به صورت گمنام به شبکه احراز اصالت می‌شوند و از خدمات شبکه استفاده می‌کنند. روش پیشنهادی بر مبنای رمز کلیدعمومی است اما سعی شده است تا حد امکان پردازشهای تحمیلی بر روی موبایل کاهش یابد. در [8] پروتکلی ارائه شده است که احراز اصالت دو طرفه در شبکه و کاهش پهنای باند مصرفی میان *VLR* و *HLR* و کاهش حافظه مورد نیاز در *VLR* را در بر دارد. اما روش ارائه شده هنوز دارای پیامهای کنترلی زیادی می‌باشد و چندان بهینه نیست. در [9] روش *KAY* پیشنهاد شده است که در آن تعداد پیامهای کنترلی شبکه کاهش چشمگیری یافته است. اما در این روش، اولاً دستگاه موبایل ناچار است که همواره عددی را به صورت تصادفی تولید و برای شبکه ارسال کند که این امر ممکن است باعث پایین آمدن کارایی دستگاه موبایل شود و ثانیاً شبکه برای موبایل احراز اصالت نمی‌شود. در نهایت هم تحلیل‌هایی که در این مقاله ارائه شده است، بر این مبنا است که در شبکه *GSM* برای هر بار احراز اصالت موبایل، *VLR* با *HRL* تماس برقرار می‌کند؛ در حالی که این فرض درست نیست. چرا که بعد از بار اولی که *VLR* با *HLR* برای احراز اصالت موبایل، تماس برقرار نمود، *HLR* به *VLR* ۵ تا از سه‌تایی‌های امنیتی را برای احراز اصالت‌های بعدی موبایل می‌دهد و *VLR* تا ۴ بار دیگر با *HLR* تماس برقرار نمی‌کند. بنابراین بهبودهای ۵۰٪ که در این مقاله در نرخ پیامهای کنترلی مربوط به احراز اصالت در *VLR* و *HLR* داده شده است، صحیح نمی‌باشد.

۳- پروتکل پیشنهادی بر مبنای تسلا

در [8] پروتکلی جهت احراز اصالت در شبکه *GSM* ارائه شده است که در آن *HLR* برای مدت زمانی به *VLR* مجوز احراز اصالت دستگاه موبایل را با استفاده از بلیط TK_i می‌دهد. در این مقاله سعی می‌شود از آن ایده با تغییرات عمده‌ای استفاده گردد؛ بدین صورت که برای بار اول احراز اصالت، *VLR* مجوز احراز اصالت موبایل را برای مدت زمان T از *HLR* می‌گیرد و از آن به بعد تا T واحدزمان بعد، *VLR* بدون مراجعه به *HLR* موبایل را احراز اصالت می‌کند. در ضمن در پروتکل پیشنهادی، احراز اصالت شبکه به دستگاه موبایل از طریق پروتکل تسلا صورت می‌گیرد. بنابراین در ابتدا پروتکل تسلا شرح داده می‌شود و سپس پروتکل احراز اصالت پیشنهادی مورد بررسی قرار می‌گیرد.

[6] *Denial of Service (DoS)*

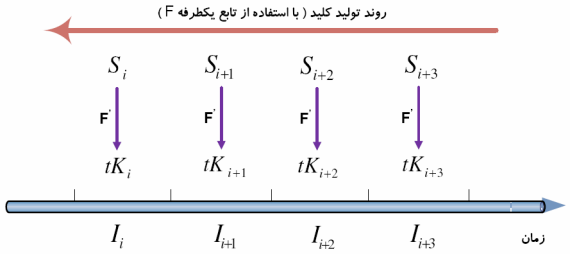
۳-۱ پروتکل احراز اصالت تسلا

در ارسال داده به صورت همه‌پخشی، در صورت نیاز به احراز اصالت مبدا ارسال داده، مناسب است از رمزنگاری کلیدعمومی استفاده شود. واضح است که استفاده از اینگونه رمزنگاری هزینه محاسباتی و پردازشی بالایی را هم بر روی گره ارسال کننده و هم بر روی گره‌های دریافت کننده داده تحمیل می‌کند. در شبکه‌های PCN[7] کلیدعمومی شبکه در دست همه کاربران قرار گرفته است و اطلاعات ارسالی برای شبکه با این کلید رمز و برای شبکه ارسال می‌گردد [10]. اما این روش هزینه زیادی را بر روی شبکه و دستگاه موبایل تحمیل می‌کند.

پروتکل تسلا [11,12] پروتکلی جهت احراز اصالت مبدأ ارسال داده و مبتنی بر رمزنگاری متقارن است که به طور وسیعی از توابع درهم‌ساز یکطرفه استفاده می‌کند. این پروتکل با استفاده از تأخیر زمانی، خاصیت نامتقارنی را که در رمزنگاری کلید عمومی وجود دارد، بدست می‌آورد. با استفاده از این روش، گره‌های دارای توان پردازشی پایین هم می‌توانند مبدا ارسال داده را احراز اصالت کنند. لازمه پروتکل تسلا این است که گیرنده‌ها با فرستنده به طور تقریبی همزمانسازی[8] شوند. تسلا زمان را به بازه‌هایی با طول مساوی تقسیم می‌نماید و به هر بازه یک کلید اختصاص می‌دهد. به عنوان نمونه، به بازه‌زمانی n ام کلید tK_n اختصاص می‌یابد. برای هر بسته‌ای که در بازه n ام تولید و ارسال شود، فرستنده تابع درهمساز کلیددار (MAC) آن بسته را با استفاده از کلید tK_n محاسبه می‌کند و در کنار بسته ارسال می‌نماید. گیرنده‌ها بعد از دریافت بسته‌ها آنها را تا زمان آشکارسازی کلید MAC مربوطه، بافر می‌کنند و بعد از آشکار شدن هسته[9] کلید tK_n (یعنی s_n)، هر گیرنده می‌تواند بسته‌های ذخیره شده را احراز اصالت کند. البته به دنبال اعلان کلید tK_n، هر موجود می‌تواند بسته‌ای با MAC صحیح تولید کند و خود را به جای فرستنده جا بزند؛ اما تولید بسته‌هایی با کلید tK_n، تنها در بازه زمانی n ام معتبر است و بازه‌های بعدی دارای کلیدهای تسلای مخصوص به خود هستند. در پروتکل تسلا هر کلید بعد از مدت زمان d که تحت عنوان "تأخیر آشکارسازی" شناخته می‌شود، اعلان می‌شود. در [11] مقدار کمینه d به صورت $d<(RTT/T_{\text{int}})+1$ بدست آمده است که در آن RTT بیشینه تأخیر ناشی ارسال بسته برای تمامی گیرنده‌ها و T_{int} طول هر بازه زمانی است. کلید tK_n با استفاده از تابع یکطرفه F' از هسته s_n بدست می‌آید و s_nها با استفاده از یک زنجیره تابع درهم یکطرفه به یکدیگر مربوط هستند. برای تولید این زنجیره، فرستنده ابتدا یک هسته اولیه s_l انتخاب می‌کند و سپس با استفاده از تابع یکطرفه F، l بار از آن تابع درهم می‌گیرد. با هر بار تابع درهم گرفتن، هسته بعدی زنجیره بدست می‌آید. به عبارت دیگر داریم:

$$s_{k-1}=F(s_k) \qquad k=l,\ l-1,...,1$$

بدین صورت زنجیره $\{s_0,s_1,...,s_l\}$ مطابق با شکل ۴ بدست می‌آید. فرستنده از مولفه‌های زنجیره فوق به صورت عکس روند تولید آنها یعنی از S_0 به سمت S_l استفاده می‌کند.



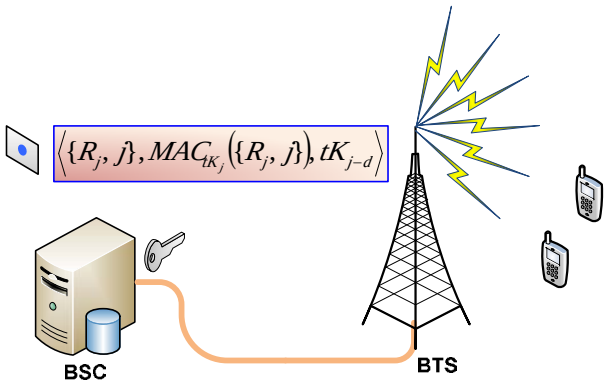
شکل ٤: زنجیره هسته‌های کلید تسلا و کلیدهای مشتق شده از آنها

از آنجا که گیرنده و فرستنده باید با هم تقریباً همزمان باشند، دوطرف با استفاده از روشی بیشینه اختلاف زمانی خود، Δ، را بدست می‌آورند. با استفاده از این زمان، گیرنده می‌تواند بعد از دریافت هر بسته، تازه بودن (یعنی اینکه بسته قبل از آشکار شدن کلید مربوط به بازه ارسال، توسط فرستنده ارسال شده است) آنرا وارسی کند و در صورت تازه بودن بسته را بافر و در غیر این صورت، بسته را دور بیندازد. بعد از آشکار شدن هر هسته s_n، گیرنده با استفاده از تابع F و رسیدن به هسته قبلی احراز اصالت شده، ($F(s_n)=s_{n-1}$)، به صحت هسته s_n پی می‌برد. سپس او کلید tK_n را از روی هسته s_n می‌سازد و بسته ارسالی در بازه n ام را احراز اصالت می‌کند. نکته مهم در اجرای این پروتکل آن است که لازم است در ابتدا، فرستنده به صورتی یکی از هسته‌ها (s_{i0}) را برای گیرنده احراز اصالت کند که جزئیات آن در [11,12] آمده است.

[7] *Personal Communication Networks*
[8] *loosly time synchronized*
[9] *Seed*

۳-۲ معرفی پروتکل پیشنهادی

همانطور که بیان شد، هدف ارائه پروتکلی است که در آن شبکه نیز برای کاربر احراز اصالت شود. برای این منظور، پیشنهاد می‌شود که شبکه به طور پیوسته از طریق "کانال کنترل همه‌پخشی"[10]، پیام تسلا را مطابق شکل ۵ برای تمامی دستگاههای موبایل ارسال کند. توجه شود که در ساختار کانالهای کنترلی مستقیم *GSM*، تعدادی کانال بی‌استفاده وجود دارند [13] که می‌توان آنها را برای ارسال پیام تسلا به *BCCH* تبدیل کرد.



شکل ۵: ارسال پیامهای احراز اصالت شبکه

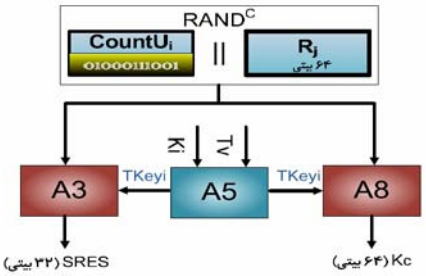
در این پیام، j شماره بازه‌زمانی تسلا، R_j عدد تصادفی ۶۴ بیتی مربوط به آن بازه و tK_j کلید *MAC* آن بازه (معادل هسته S_j) و tK_{j-d} کلید اعلان شده مربوط به d بازه قبل می‌باشد. موبایل این پیام را دریافت می‌کند و بعد از مدت d بازه زمانی که حدوداً به اندازه تأخیر *RTT* یک سلول (ماکزیمم ۳۰ μs [13]) است، می‌تواند شبکه را احراز اصالت کند. بعد از احراز اصالت شبکه، موبایل می‌تواند از همان عدد تصادفی R_j ارسال شده شبکه، چنانچه در ادامه شرح داده می‌شود، برای احراز اصالت خود به شبکه استفاده کند. چگونگی احراز اصالت هسته اولیه در بخشهای بعدی پیشنهاد می‌شود. علت انتخاب ۶۴ بیتی R_j، جلوگیری از هدر رفتن پهنای باند شبکه است.

از آنجا که در این پروتکل برای کاهش تعداد پیامهای کنترلی، از ساختار "بلیط احراز اصالت" استفاده می‌شود، کلید *Ki* مستقیماً برای تولید *SRES* و *Kc* به الگوریتمهای *A3* و *A8* داده نمی‌شود. بلکه ابتدا با استفاده از الگوریتم *A5*، "کلید بلیط" (*TKEY*) به صورت زیر ساخته می‌شود:

$$TKey_i = A5(K_i, Tv)$$

که در آن، *Tv* مقداری ۱۲۸ بیتی و زمان انقضاء بلیط می‌باشد. این زمان را *HLR* و در اولین روند احراز اصالت موبایل بعد از ورود کاربر به یک ناحیه جدید، تعیین می‌کند. توجه شود که ۸۶ بیت از K_i بعنوان کلید ورودی *A5* ($K_c||F_n$) به این الگوریتم داده می‌شود و *Tv* با رشته کلید تولیدی *A5* رمز شده و $TKey_i$ را تشکیل می‌دهد. بنابراین چون *Tv* ۱۲۸ بیتی است، $TKey_i$ هم ۱۲۸ بیتی خواهد بود. کاربر از این بلیط به عنوان کلید در الگوریتمهای *A3* و *A8* استفاده می‌کند.

پارامتر ورودی دیگر الگوریتمهای فوق، $RAND^C$ می‌باشد که از به هم پیوستن عدد تصادفی همه‌پخشی شده شبکه، R_j، و شمارنده *CountU* مربوط به کاربر ساخته می‌شود. *CountU* در درون سیم‌کارت کاربر و همچنین درون *HLR* ذخیره می‌شود و با هر فعالیت کاربر همانند ثبت کاربر در ناحیه جدید، برقراری تماس با کاربر، برقراری تماس از سوی کاربر و خلاصه هر فعالیتی که نیاز به احراز اصالت کاربر داشته باشد، به مقدار آن یکی اضافه می‌گردد. این شمارنده عددی ۶۴ بیتی است و از آن برای جلوگیری از حمله تکرار در شبکه استفاده می‌شود (توجه شود که در یک بازه زمانی، تمامی کاربران درون ناحیه تحت پوشش یک *BSC*، از عدد تصادفی یکسان R_j استفاده می‌کنند). شبیه این شمارنده در شبکه‌های بی‌سیم نسل سوم (*UMTS*) هم وجود دارد که در آنجا شماره ترتیب (*SQN*) نامیده می‌شود [14]. در شکل ۶ فلوچارت تولید کلیدرمز *Kc* و پاسخ‌امنیتی *SRES* با استفاده از پارامترهای ورودی شبکه، کلید *Ki* و شمارنده $CountU_i$ مشاهده می‌شود:



شکل ٦: چگونگی تولید *SRES* و *Kc* در پروتکل ارائه شده

توجه شود که در بار اولی که یک کاربر در یک *LA* خود را احرازاصالت می‌کند، *Tv* را در اختیار ندارد (چرا که اصلا بلیطی برای احراز اصالت او صادر نشده است) و بنابراین به صورت پیش‌فرض، کاربر به جای آن از مقدار صفر استفاده می‌کند.

[10] *Broadcast Control Channel (BCCH)*

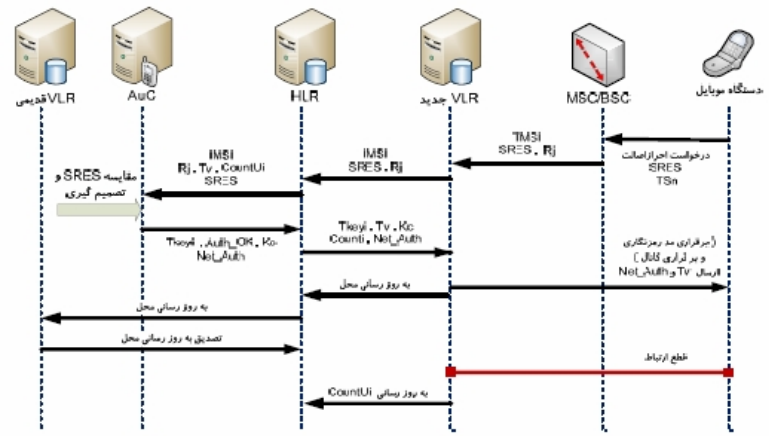
۳-۳- روند پیامهای احراز اصالت و تحلیل امنیتی پروتکل

برای تحلیل پروتکل ارائه شده، ابتدا فرض می‌شود موبایل به یک *LA* جدید وارد می‌شود. او ابتدا از طریق کانال دسترسی تصادفی، تقاضای خود را به شبکه اعلام می‌کند. *BS* با دریافت تقاضای موبایل و در صورت امکان به او یک کانال *SDCCH* را برای ارتباط با شبکه و عبور پیامهای احرازهویت، تخصیص می‌دهد[13]. کاربر تا زمان دریافت یک کانال ترافیکی، از این کانال برای ارتباط با شبکه و احراز اصالت خود استفاده می‌کند.

در شکل ۷، پیامهای احراز اصالت نشان داده شده است. در پیام اول، کاربر درخواست احراز اصالت خود (به همراه شناسه *TMSI* خود)، پاسخ *SRES* تولیدی الگوریتم، شماره بازه زمانی پروتکل تسلا (*TSn*) که از عدد تصادفی R_j درون پیام تسلای آن بازه برای تولید *SRES* استفاده کرده است را برای شبکه و *BSC* ارسال می‌کند. *VLR* با توجه به شناسه *TMSI* کاربر درمی‌یابد که او نخستین مرتبه‌ای است که در این ناحیه تقاضای احراز اصالت می‌کند. در این صورت، *VLR* هنوز بلیطی را برای احراز اصالت کاربر از *HLR* دریافت نکرده است و بنابراین روند پیامهای احراز اصالت تا *HLR* و *AuC* ادامه می‌یابد. از سوی دیگر در این شرایط *HLR* می‌داند که کاربر در این روند احراز اصالت، *Tv* را در اختیار نداشته و به جای آن از مقدار صفر استفاده کرده است. در پیام بعدی، *BSC* با استفاده از شماره *TSn*، R_j را تعیین می‌کند و آنرا به همراه سایر پارامترهای دریافتی برای *VLR* ارسال می‌کند. *VLR* با درخواستهای مناسب، *TMSI* کاربر را به *IMSI* او نگاشت می‌کند و پیام رسیده را برای *HLR* می‌فرستد.

در *HLR* با استفاده از شناسه *IMSI* دریافت شده، *CountUi* از پایگاه داده استخراج می‌شود و به همراه R_j و *SRES* و *IMSI* برای *AuC* ارسال می‌گردد. در ضمن *AuC* بایستی بلیطی را برای *VLR* تولید کند؛ بنابراین، *HLR* زمان انقضاء بلیط را هم برای *AuC* ارسال می‌کند تا او بتواند بلیط $TKey_i$ را تولید کند.

با رسیدن پیام به *AuC*، او با استفاده از پارامترهای رسیده و *Tv=0*، *SRES* و *Kc* را محاسبه می‌کند. در صورتی که *SRES* محاسبه شده و *SRES* رسیده یکسان بودند، موبایل برای شبکه احراز اصالت می‌شود. *AuC* همچنین برای احراز اصالت‌های بعدی موبایل در این *LA*، با استفاده از *Tv* و *Ki*، بلیط $TKey_i$ را تولید و آنرا به همراه *Kc* برای *HLR* و *VLR* مربوطه می‌فرستد. از سوی دیگر *Tv* باید برای موبایل هم ارسال شود؛ بنابراین *HLR* آنرا برای *VLR* ارسال می‌کند تا او بعد از برقراری کانال، آنرا برای موبایل ارسال کند. در ضمن برای احراز اصالت شبکه به موبایل در مرتبه اول، از پارامتر *Net_Auth* استفاده می‌شود. این پارامتر به صورت $Net\_Auth = A8(Ki, R_j)$ تولید می‌گردد. چون تنها موبایل و شبکه اصیل، *Ki* را در اختیار دارند، موبایل با دریافت این پارامتر، به اصالت شبکه پی می‌برد. از کلید tK_j به عنوان کلید اصیل احراز اصالت پروتکل تسلا، برای احراز اصالت شبکه در مراحل بعدی که هنوز کاربر در این ناحیه قرار دارد، استفاده می‌شود (روند این کار به این صورت است که موبایل با آشکار شدن کلید tK_m از طرف شبکه و با در اختیار داشتن کلید احراز اصالت شده tK_n، می‌تواند با گرفتن $(m\text{-}n)$ بار تابع یکطرفه از tK_m و رسیدن به tK_n، tK_m را احراز اصالت کند).

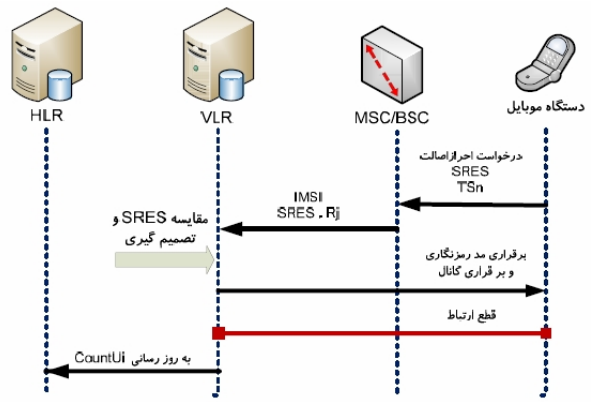


شکل ۷: احراز اصالت اولیه موبایل بعد از ورود به یک *LA* جدید

توجه شود در صورتی که موبایل در حالت *handoff* به ناحیه جدید وارد نشده باشد، نیازی به برقراری کانال ترافیکی نیست و *Tv* و *Net_Auth* از طریق کانال *SDCCH* برای موبایل ارسال می‌شوند. بعد از قطع ارتباط، *VLR* مقدار *CountUi* را یکی اضافه می‌کند و (به صورت گزینشی) آنرا برای *HLR* ارسال می‌کند تا *HLR* بتواند پایگاه خود را برای استفاده‌های بعدی به روز کند (برای کاهش بار ترافیکی شبکه، به روز رسانی *CountUi*، می‌تواند بعد از هر چند بار احراز اصالت موبایل صورت بگیرد).

در بخش تحلیل پروتکل مشاهده می‌شود که تعداد پیامهای کنترلی مربوط به احراز اصالت شبکه در پروتکل ارائه شده بسیار کمتر از پروتکل *GSM* است.

در شرایطی که موبایل برای مدت زمان زیادی در یک *LA* باقی بماند (و تا زمان اعتبار بلیط $TKey_i$ که برابر *Tv* است)، شرایط بسیار مطلوب‌تر است. پیامهای احراز اصالت این حالت در شکل ۸ مشاهده می‌شوند. پیامهای اول و دوم، همانند حالت قبل است به جز آنکه *MS* در تولید *SRES* و *Kc* از *Tv* مربوط به بلیط $TKey_i$ استفاده می‌کند. بعد از رسیدن پیامها به *VLR*، او با استفاده از پارامترهای موجود از این کاربر و همچنین پارامترهای دریافتی، موبایل را احراز اصالت می‌کند. در پی مرحله احراز اصالت، کانال ترافیکی امنی برای برقراری مکالمات صوتی، میان *BS* و *MS* برقرار می‌شود. دقت کنید که بعد از قطع کانال ارتباطی، *VLR* باید *CountUi* به روز شده را برای *HLR* ارسال کند. البته این عمل ممکن است بعد از چند مرحله احراز اصالت موبایل (قبل از *handoff* موبایل به یک *LA* دیگر) و نه بعد از هر بار احراز اصالت موبایل، صورت بگیرد.



شکل ۸ : پیامهای احراز اصالت در وضعیت پایدار موبایل در یک *LA*

۴-تحلیل کارایی پروتکل احراز اصالت ارائه شده

کارایی پروتکل احراز اصالت ارائه شده را با در نظر گرفتن پارامترهای پهنای باند مصرفی از شبکه (تعداد پیامهای تبادل شده) و تأخیر احراز اصالت، تحلیل می‌کنیم. برای این منظور ابتدا به چارچوب مناسبی برای تحلیل اشاره می‌شود و سپس بر اساس آن چارچوب، پروتکل ارائه شده را با پروتکل *GSM* مقایسه می‌کنیم.

٤-١- ارائه یک چارچوب مناسب برای تحلیل کارایی

فرایند احراز اصالت ممکن است در هنگام ثبت کاربر در یک *LA* جدید (و حذف از *LA* قدیمی)، برقراری مکالمه (کاربر مبدا یا مقصد تماس باشد) و یا با تغییر پارامترهای سرویس صورت بگیرد. در تمامی این حالات، فرایند احراز اصالت باعث تبادل حجم زیادی از پیامهای کنترلی در شبکه می‌شود که تبادل این پیامها، زمان برقراری تماس را افزایش می‌دهد.

در [15] مدلی برای جابجایی جریان سیّال ارائه شده است که می‌توان از آن به عنوان مدل جابجایی موبایل‌ها در شبکه *GSM* استفاده نمود. در این مدل تصور می‌شود که ترمینالهای موبایل با سرعت متوسط v در شبکه در حال حرکت هستند و جهت حرکت آنها دارای توزیع یکنواخت روی بازه $[0,2\pi]$ می‌باشد. از سوی دیگر کاربران شبکه به صورت یکنواخت و با چگالی ρ در شبکه پراکنده شده‌اند و هر ناحیه ثبت[1] دارای محیطی برابر با L می‌باشد. با توجه اینگونه فرض‌ها، در [16] اثبات شده است که نرخ عبور از یک ناحیه ثبت به صورت زیر می‌باشد:

$$R = \frac{\rho \times L \times v}{\pi} \qquad (۱)$$

برای بررسی‌های بیشتر، ابتدا لازم است که مدلی از محیط کاربردی شبکه ارائه شود. برای این منظور در [16] فرض‌های زیر به عنوان پارامترها و ابعاد شبکه در نظر گرفته شده است: کل شبکه *GSM* دارای ۱۲۸ *VLR*، یا به عبارت دیگر ۱۲۸ ناحیه ثبت با مساحت ٥٧/٤ کیلومترمربع برای هر ناحیه می‌باشد. طول مرز هر ناحیه، L، ۳۰/۳ کیلومتر است و نرخ میانگین برقراری تماس هر کاربر ۱/٤ تماس بر ساعت می‌باشد. چگالی میانگین افراد، ρ، ۳۹۰ کاربر بر کیلومترمربع و سرعت میانگین

[1] *Registration Area*

افراد، ۷۰، ۵/۶ کیلومتر بر ساعت است. در ضمن تعداد کل کاربران شبکه، ۲/۸۶۵ میلیون نفر می‌باشد.

همانطور که اشاره شد، با ورود کاربر به یک ناحیه جدید، ترافیکی که ناشی از ثبت دستگاه موبایل در ناحیه جدید است، بر روی شبکه برقرار می شود. با توجه به معادله (۱)، نرخ ورود کاربر به یک ناحیه *LA* جدید، که همان نرخ ثبت کاربر در آن ناحیه است، در هر ثانیه به صورت زیر محاسبه می‌شود:

$$R_{Reg.,LA}=\frac{390*30.3*5.6}{3600\pi}=5.85$$

به منظور حفظ تعادل، برای عملیات حذف از یک ناحیه، نرخ خروج با نرخ ثبت یکسان و در هر ثانیه برابر با $R_{DeReg.,LA}=5.85$ می‌باشد. بنابراین تعداد کل پیامهایی که برای عملیات ثبت در هر ثانیه به یک *HLR* می‌رسند (تعداد درخواست‌های احراز اصالت)، در هر ثانیه به صورت زیر محاسبه می‌شود:

$$R_{Reg.,HLR}=R_{Reg.,VLR}\times 128=5.85\times 128=748.9$$

حال تعداد کل درخواست‌های احراز اصالتی که ناشی از برقراری تماس است محاسبه می‌شود. با توجه با اینکه نرخ متوسط برقراری تماس در هر ساعت ۱/۴ به ازاء هر کاربر است و ۲/۸۶۵ میلیون کاربر تلفن‌همراه در شبکه وجود دارند، نرخ برقراری تماس (کاربر آغازگر) در هر ثانیه عبارت می‌شود از:

$$R_{CallOrig./HLR}=1.4*2.865*10^6/3600=1114.2$$

به طور مشابه، نرخ برقراری مکالمه (کاربر مقصد تماس باشد)، نیز مشابه مقدار بالا بدست می‌آید و بنابراین نرخ برقراری تماس برای هر *LA* در هر ثانیه به صورت زیر می‌باشد:

$$R_{CallOrig./VLR}=R_{CallTerm./VLR}=1114.2/128=8.7$$

در جدول ۱ نرخ درخواست های احراز اصالت برای هر *VLR* و *HLR*، برای عملیاتهای مختلف، آورده شده است:

جدول ۱: نرخ درخواست‌های احراز اصالت وارده به *VLR* و *HLR*

	VLR بر ثانیه	*HLR* برثانیه
ثبت در یک ناحیه	۵/۸۵	۷۴۸/۹
کاربر آغازکننده‌تماس	۸/۷	۱۱۱۴/۲
کاربر مقصد تماس	۸/۷	۱۱۱۴/۲
مجموع برای شبکه	۲۳/۲۵	۲۹۷۷/۳

۴-۲- مقایسه پهنای باند مصرفی (تعداد پیامها)

ابتدا بر اساس چارچوب ارائه شده، کارایی پروتکل *GSM* مورد ارزیابی قرار می‌گیرد.

با توجه به شکل ۳ تعداد پیامهای کنترلی لازم برای عملیات احراز اصالت در هنگام ورود کاربر به یک ناحیه جدید محاسبه شده است. برای حالاتی که کاربر در همان ناحیه باشد اما با او تماس گرفته شود و یا او خود آغازگر تماس باشد، روند مشابهی برقرار است؛ به جز آنکه در آنها پیام ارسالی به *VLR* قدیمی مبتنی بر "به روز رسانی محل"، وجود ندارد. در جدول ۲ تعداد این پیامها برای هر مولفه شبکه مشاهده می‌شود:

جدول ۲ :تعداد پیامهای کنترلی مبادله شده در شبکه *GSM*

	Auc	*HLR*	*VLR*	*VLR* قدیمی
ثبت در یک ناحیه	۲	۴	۵	۱
آغاز کننده تماس	۲	۴	۵	-
مقصد تماس	۲	۴	۵	-

همانطور که نشان دادیم برای عملیات ثبت کاربر جدید در یک ناحیه، به هر *VLR*، تعداد ۵/۸۵ درخواست احراز اصالت در ثانیه می‌رسد و برای هر درخواست احراز اصالت، هر *VLR* بایستی تعداد ۵ پیام را پردازش کند. در نتیجه تعداد پیامهای کنترلی برای عملیات ثبت برای هر *VLR* و در هر ثانیه، برابر با ۵×۵/۸۵=۲۹/۲۵ پیام است.

برای سایر موجودیتهای شبکه و انواع درخواست احراز اصالت نیز به طور مشابه می‌توان نرخ پیامها را محاسبه کرد که نتیجه در جدول ۳ مشاهده می‌شود.

جدول ۳: نرخ پیامهای کنترلی در شبکه *GSM*

	VLR (بر ثانیه)	*HLR* (برثانیه)
ثبت در یک ناحیه	۲۹/۲۵	۲۹۹۵/۶
کاربر آغازکننده‌تماس	۴۳/۵	۴۴۵۶/۸
کاربر مقصد تماس	۴۳/۵	۴۴۵۶/۸
مجموع برای شبکه	۱۶۱/۲۵	۱۱۹۰۹/۲

البته از آنجا که *HLR* تعداد *n* (عموما *n* برابر ۵ انتخاب می‌گردد) سه‌تایی احراز اصالت را برای *VLR* ارسال می‌کند، در شرایطی که مقادیر پارامترهای شبکه‌ی ذکر شده در بخش ۴-۱ تغییر کنند و نرخ برقراری تماس کاربر از نرخ احرازاصالت ناشی از تغییر *LA* کاربر بالاتر باشد، شرایط از آنچه در جدول‌های ۲ و ۳ آمده است، مناسبتر خواهد بود (چرا که دیگر نیازی به ارتباط *VLR* با *HLR* نیست). در این شرایط از هر پنج بار احراز اصالت، تنها یک بار با *AuC* تماس گرفته می‌شود و در این یک بار، دو پیام کنترلی ردوبدل می‌گردد. در نتیجه تعداد پیامهای کنترلی به طور متوسط به صورت زیر بدست می‌آید:

$AuC \quad : \quad (2*1+0*4)/5 = 0.4$

و برای *VLR* هم درحالتی که موبایل آغازکننده یا مقصد تماس باشد، تعداد پیامهای کنترلی به صورت زیر خواهد بود:

$VLR \quad : \quad (5*1+3*4)/5 = 3.4$

و در نهایت در زمان طولانی حضور کاربر در یک ناحیه، تعداد پیامهای کنترلی مطابق جدول ۴ خواهد بود (از آنجایی که تعداد پیامهای ناشی از ثبت کاربر در یک ناحیه مربوط به نرخ گذر کاربر و معادله ۱ است، این مقادیر برای حضور طولانی مدت کاربر در یک ناحیه، تغییری نمی‌کنند).

جدول ٤ :تعداد پیامهای کنترلی برای حضور طولانی در یک ناحیه (*GSM*)

	VLR قدیمی	*VLR*	*HLR*	*Auc*
ثبت در یک ناحیه	۱	۵	۴	۲
آغاز کننده تماس	–	۳/۴	۰/۸	۰/۴
مقصد تماس	–	۳/۴	۰/۸	۰/۴

و جدول ۳ هم که نرخ پیامهای کنترلی را برای *VLR* و *HLR* نشان می‌داد، برای حضور طولانی کاربر در یک ناحیه، به صورت جدول ۵ در می‌آید:

جدول ۵: نرخ پیامهای کنترلی برای حضور طولانی در یک ناحیه (*GSM*)

	VLR (بر ثانیه)	*HLR* (برثانیه)
ثبت در یک ناحیه	۲۹/۲۵	۲۹۹۵/٦
کاربر آغازکننده‌تماس	۲۹/۵۸	۹۸۱/۳٦
کاربر مقصد تماس	۲۹/۵۸	۹۸۱/۳٦
مجموع برای شبکه	۸۸/۱٤	٤۷۷۸/۳۲

اکنون به ارزیابی کارایی پروتکل پیشنهادی پرداخته می‌شود. مشاهده شد که پروتکل ارائه شده دارای تعداد پیامهای کنترلی بسیار کمتری از پروتکل *GSM* است. در صورتی که یک کاربر برای مدت زمان طولانی در یک *LA* باقی بماند و تا زمانی که بلیط احراز اصالت کاربر دارای اعتبار زمانی باشد (*Tv*)، تنها دو پیام کنترلی برای احراز اصالت کاربر نیاز است (شکل ۸). این در حالی است که در پروتکل *GSM* نمی‌توان به سادگی برای افزایش کارایی پروتکل، *n* (*n* سه‌تایی احراز اصالت) را زیاد کرد چرا که با افزایش *n*، *VLR* ناچار است که حجم زیادی از سه‌تایی‌های امنیتی را برای هر کاربر، در پایگاه داده خود نگهداری نماید؛ حال آنکه در پروتکل ارائه شده، در *VLR* برای هر کاربر تنها یک بلیط احراز اصالت و یک شمارنده *CountUi* نگهداری می‌شود.

در جدول ۶ تعداد پیامهای کنترلی مبادله شده برای ثباتهای شبکه مشاهده می‌شود. در این حالت تصور شده است که زمان اعتبار بلیط به اندازه کافی طولانی باشد (به اندازه زمانی که کاربر در یک ناحیه باقی می‌ماند). در این شرایط در هنگام برقراری مکالمه دیگر لازم نیست با *HLR* و *AuC* تماس گرفته شود و *VLR* به هر تعداد می‌تواند کاربر را احراز اصالت کند. دقت شود که طولانی بودن *Tv* مشکل امنیتی خاصی را بوجود نمی‌آورد.

جدول ٦ :تعداد پیامهای کنترلی در صورت بکارگیری پروتکل پیشنهادی

	VLR قدیمی	*VLR*	*HLR*	*Auc*
ثبت در یک ناحیه	۱	۳	۴	۲
آغاز کننده تماس	–	۲	۰	۰
مقصد تماس	–	۲	۰	۰

بنابراین نرخ پیامهای کنترلی برای *VRL* و *HLR* در پروتکل پیشنهادی با توجه به مندرجات جدول ۱، مطابق با جدول ۷ خواهد بود.

جدول ۷: نرخ پیامهای کنترلی برای پروتکل پیشنهادی

	VLR (بر ثانیه)	*HLR* (برثانیه)
ثبت در یک ناحیه	۱۷/۵۵	۲۹۹۵/٦
کاربر آغازکننده‌تماس	۱۷/٤	۰
کاربر مقصد تماس	۱۷/٤	۰
مجموع برای شبکه	۵۲/۳۵	۲۹۹۵/٦

در نهایت در جدول ۸ بهبود حاصل شده در نرخ پیامهای کنترلی شبکه (پیام بر ثانیه)، در مقایسه با شبکه *GSM* مشاهده می‌شود:

جدول ۸: مقایسه نرخ پیامهای کنترلی در دو پروتکل

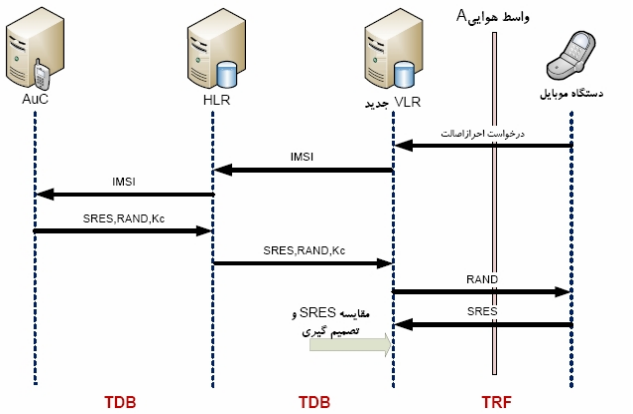
	درصد بهبود نسبت به		پروتکل پیشنهادی	*GSM*	
	حضور طولانی	حضور کوتاه		حضور طولانی	حضور کوتاه
VLR	٪٤۱	٪٦۸	۵۲/۳۵	۸۸/۱٤	۱٦۱/۲۵
HLR	٪۳۷	٪۷۵	۲۹۹۵/٦	٤۷۷۸/۳۲	۱۱۹۰۹/۲
کل	٪۳۷	٪۷۵	۳۰٤۷/۹۵	٤۸٦٦/٤٦	۱۲۰۷۰/٤۵

همانطور که مشاهده می‌شود، پروتکل ارائه شده، نرخ پیامهای کنترلی مربوط به احراز اصالت *GSM* را در حالت حضور طولانی کاربر در *LA* حدود ٪۳۷ و در حالت حضور کوتاه کاربر در *LA* حدود ٪۵۷ کم کرده و آنرا بهبود می‌دهد.

٤-۳- مقایسه تأخیر

تأخیر احراز اصالت در شبکه *GSM*، عبارت است از زمانی که کاربر فرایند احراز اصالت را آغاز می‌کند تا اینکه شبکه تصمیم خود مبنی بر پذیرش و یا رد کاربر را اتخاذ کند. پیامهای احراز اصالتی که بین کاربر و *BS* ردوبدل می‌شوند، از واسط هوایی

عبور می‌کنند و دارای تأخیر ناشی از عبور امواج رادیویی از هوا هستند. این تأخیر در [9]، *TRF* نامیده شده است (توجه شود که از تأخیر *BS* تا *VLR*، صرفنظر شده است). در داخل شبکه هسته، تأخیر زمانی ناشی از تبادل پیامها میان پایگاه‌داده‌های مختلف، *TDB* نامیده می‌شود. (شکل ۹)



شکل ۹: تأخیر پیامهای کنترلی مربوط به احراز اصالت در شبکه *GSM*

با توجه به این تعاریف، تأخیر احراز اصالت در شبکه *GSM* برابر با $Auth.Delay = 4*TDB + 3*TRF$ می‌باشد. در حالتی که کاربر برای مدت طولانی در یک *LA* بماند، تأخیر احراز اصالت برابر با $Auth.Delay = 0.8*TDB + 3*TRF$ می‌شود.

از سوی دیگر تأخیر احراز اصالت در پروتکل پیشنهادی با توجه به شکل ۸ به صورت زیر بدست می‌آید:

$Auth.Delay = TRF$

قابل مشاهده است که پروتکل پیشنهادی حداقل یک کاهش سه برابری در تأخیر ناشی از فرایند احراز اصالت ایجاد می‌نماید. البته هر چه تأخیرهای باند رادیویی و تأخیر ناشی از ارتباط میان پایگاههای داده مختلف بالاتر باشد، کارایی پروتکل پیشنهادی بالاتر می‌رود.

۵- نتیجه‌گیری

پروتکل احراز اصالت *GSM* دارای مشکلات فراوانی است. این پروتکل علاوه بر آنکه به صورت یکطرفه عمل می‌کند و در آن شبکه برای موبایل احراز اصالت نمی‌شود، حجم زیادی از مبادلات کنترلی شبکه را هم به خود اختصاص داده است. پروتکل پیشنهادی از جنبه‌های مختلف بر پروتکل احراز اصالت *GSM* برتری دارد. از لحاظ امنیتی پروتکل پیشنهادی نیازمندی احراز اصالت شبکه را برای موبایل برآورده می‌سازد که برای تحقق این سرویس از ایده‌ی پروتکل تسلا بهره‌برداری شد. از لحاظ کارایی نیز پروتکل پیشنهادی چه از لحاظ پهنای باند مصرفی، که آنرا حدود ۵۷٪ در حالت حضور کوتاه و ۳۷٪ در حالت حضور طولانی بهبود می‌داد، و چه از لحاظ تأخیر برقراری ارتباط، برتری قابل ملاحظه‌ای بر پروتکل احراز اصالت *GSM* دارد.

۶- مراجع

[1] M. Rahnema, "Overview of the GSM system and protocol architecture", IEEE Communicatio Magazine, pp. 92-100, April 1993
[2] MALLINDER, B.: 'An overview of the GSM system'. Proceedings of Third Nordic Seminar on Digital band mobile radio commun.,Copenhagen, Denmark, Sept. 1988, pp. 12-15
[3] Kai Schramm , "DES Sidechannel Collision Attacks On Smartcard Implementations" , Department of Electrical Engineering and Information Sciences Ruhr-Universit at Bochum , 2002
[4] J. Quirke, "Security in the GSM system" , AusMobile ,2004
[5] Ö. Aydemir, A. Aydın Selçuk, "A Strong User Authentication Protocol for GSM",in Proceedings of the 14th IEEE International Workshops on Enabling Technologies: 2005
[6] V. BOCAN and V. CRETU , "Mitigating Denial of Service Threats in GSM Networks" , Proceedings of the First International Conference on Availability, Reliability and Security (ARES'2006)
[7] W. Lin, J. Jan , "A Wireless-based Authentication and Anonymous Channels for Large Scale Area", IEEE, 2001
[8] c. Lee, M. Hwang, W. Yang, "Extension of authentication protocol for GSM", IEE Proc.-Cornmiin., Vol. 150. No. 2, April 2003
[9] K. Al-Tawil, A. Akrami, H. Youssef, "A new authentication protocol for gsm network", 1995
[10] D. Brown, "Techniques for privacy and authentication in personal communication systems", IEEE Personal Communications (August) (1995) 6–10.
[11] A. Perrig, R. Canetti, J.D. Tygar, D. Song,"The TESLA Broadcast Authentication Protocol",UC Berkeley and IBM Research, 2002
[12] A. Perrig, R. Canetti, J.D. Tygar, D. Song,"Timed Efficient Stream Loss-Tolerant Authentication (TESLA):Multicast Source Authentication Transform Introduction" , RFC 4082, 2005
[13] M. Schwartz, "Mobile wireless communications", First Edition, Cambridge University press, 2005
[14] C. Blanchard , "Security for the Third Generation (3G) Mobile System",Network Systems & Security Technologies , BTexaCT. MLB1 PP8
[15] R. Thomas, H. Gilbert, G. Mazziotto, "Influence of the mobile station on the performance of a radio mobile cellular network", Proceedings of the 3rd Nordic Seminar, Paper. 9.4, Copenhagen, Denmark, 1998.
[16] J.F. Stacha, E.K. Parka, K. Makkib ,"Performance of an enhanced GSM protocol supporting non-repudiation of service",Elsevier, 1999