نشریه علمی "پدافند الکترونیکی و سایبری"

سال هفتم، شماره ۲، تابستان ۱۳۹۸، ص ۱۳۲-۱۲۱

تحلیل چالش‌های امنیتی شبکه LTE، و موانع و فرصت‌های بومی‌سازی شبکه در بستر استاندارد

محسن شهریاری[۱]، بهمن مددی[۲*]، محمد صابری[۳]

۱- کارشناس ارشد الکترونیک، ۲- کارشناس ارشد مخابرات رمز ۳- کارشناس ارشد مخابرات سیستم، مرکز تحقیقات صدر

(دریافت: ۹۷/۰۶/۱۸، پذیرش: ۹۷/۱۲/۱۴)

چکیده

فناوری‌های LTE و LTE-A با هدف دست‌یابی به مخابرات نسل چهار و دسترسی به اینترنت سرعت بالای پهن باند طراحی شده‌اند، اگرچه در نهایت LTE-A بود که نیازمندی‌های نسل چهارم مخابرات را پشتیبانی نمود و می‌توان آن را به‌عنوان 4G پـذیرفت. مشخصـات آن‌هـا توسـط 3GPP در طول سال‌های مختلف منتشر شد. هدف اصلی 4G این است که با یکی کردن شبکه‌های تلفن همراه موجود و ایجاد شبکه مرکـزی جهانی که مبتنی بر IP باشد، امکاناتی مثل سرعت بالا، ظرفیت بالا، پشتیبانی از صوت و داده که همگی برمبنـای IP هسـتند را فـراهم کنـد. شبکه LTE یا همان به دلیل ویژگی‌های منحصر به فرد شبکه‌های LTE، چالش‌هـای جدیـدی در مکانیسـم طراحـی آن وجـود دارد. همـین موضوع نیز منجر به آسیب‌پذیری امنیتی این شبکه شده است. این مقاله نتیجه بیش از چندین سال تحقیـق در مـورد شـبکه LTE و تحلیـل امنیت و آسیب‌پذیری‌های امنیتی آن و امکان بومی‌سازی امنیت شبکه در بستر استاندارد است. این مقاله ابتدا نمایی کلی از سـاختار سـامانه LTE/SEA را ارائه و بخش‌های درگیر با امنیت شبکه را ترسیم خواهد کـرد. شـبکه LTE در در ادامـه بـه‌طـور ویـژه فرآینـد احـراز هویـت و راه‌اندازی پروتکل‌ها و توافق کلید بین بخش‌های مختلف شبکه تشریح و تحلیل می‌شود. پس از آن، بـا در نظـر گـرفتن اهمیـت نحـوه خـاص مدیریت کلید در این نوع شبکه، به بررسی مزایا و معایب آن پرداخته می‌شود. با نگاهی جامع، آسیب‌شناسی امنیتـی ایـن شـبکه مطـرح و در نهایت به بررسی امکان بومی‌سازی شبکه LTE در بستر استاندارد پرداخته می‌شود. نتایج مرتبط با بومی‌سازی که به‌صورت جدولی در انتهـای مقاله ارائه می‌گردد، به روش تحلیل استانداردهای3GPP، تحلیل تمام پروتکل‌های مشـترک در بخـش‌هـای مختلـف شـبکه و امکـان‌سـنجی ظرفیت بومی‌سازی با حفظ پایبندی به استاندارد صورت گرفته است. این جدول از جنبه امنیت شبکه بسیار حائز اهمیت است و ظرفیت‌هـای موجود در ساختار شبکه برای بومی‌سازی را به‌طور دقیق به تصویر می‌کشد.

کلید واژه‌ها: نسل چهار تلفن همراه، شبکه LTE، فرآیند AKA، مدیریت کلید، بومی‌سازی

۱- مقدمه

صنعت مخابرات بی‌سیم برای ارتقاء سطح مخابراتی و افزایش باند و به‌منظور افزایش سرعت و همچنین توسعه شـبکه، کمیتـه‌ای را برای طراحی نسل جدیدی از موبایل یعنـی 4G گـردآوری نمـود. هدف اصلی 4G این بود که بـا یکـی کـردن شـبکه‌هـای موبایـل موجود و ایجاد یک شبکه مرکزی جهانی که مبتنی‌بـر IP باشـد، امکاناتی مثل سرعت بالا، ظرفیت بالا، پشتیبانی از صوت و دیتا بر مبنای IP را هم فراهم کند. در پاییز سال ۲۰۰۴، برای اولین بـار کارگاهی برای معرفی یک استاندارد جدید به نام LTE[۱] برپا شـد. در واقع نام کامل سامانه LTE/SAE است که اصطلاح فنی بـرای این سامانه، EPS[۲] است [۱].

همان‌طور که بیان شد LTE دسترسی مبتنی‌بـر IP را فـراهم می‌کند و همچنین پهنای بانـد وسـیعی ارائـه مـی‌کنـد. 3GPP[۳] تصمیم گرفت به مطالعه ساختاری بپردازد که از ویژگی‌های ذکـر شده پشتیبانی کند؛ این تحقیقات SAE[۴] نامیده شدند. نتیجه این تحقیقات EPC[۵] اسـت کـه یـک معمـاری تمامـا IP اسـت. EPC همچنین راه‌حل‌هایی را برای امنیت، QOS[۶]، تحرک و اتصـال بـه

* رایانامه نویسنده مسئول: ieeecombit@chmail.ir

1- Long term evolution

2- Evolved packet system

3- 3rd Generation Partnership Project

4- System Architecture Evolution

5- Evolved Packet Core

6- Quality of service

خدمات مبتنی بر IP همانند IMS[1] را ارائه می‌کند.

با توجه به اهمیت این موضوع و استفاده‌ی روز افزون از این فناوری، در این مقاله سعی بر آن شد تا با نگاه اجمالی به مبحث معماری LTE، به طور دقیق چالش‌های امنیتی و نقاط آسیب‌پذیر این شبکه تحلیل شود [۲]. به دنبال آن با بررسی استانداردهای 3GPP، تحلیل پروتکل‌های ارتباطی و امنیتی و گره‌های درگیر در شبکه به استخراج ظرفیت‌های موجود جهت بومی‌سازی شبکه با هدف بالابردن امنیت شبکه پرداخته می‌شود. تشخیص و کشف موارد و ظرفیت‌های انتخابی موجود در شبکه با رعایت استانداردها، امکان ایجاد تغییرات در شبکه را با هدف بالا بردن امنیت شبکه را فراهم می‌کند.

در مورد بومی‌سازی باید اشاره کرد که در معماری امنیتی یک سامانه، یک سری از اجزا وجود دارد که شاکله اساسی امنیت در آن سامانه را تشکیل می‌دهند. در مواردی به‌صورت انتخابی، قابلیت تغییر و بومی‌سازی توسط کارشناسان امنیتی یک کشور امکان‌پذیر است. همان‌طور که ذکر شد، کشف این موارد در سامانه و استاندارد، بازطراحی و تولید این اجزا در این مقاله، بومی‌سازی نامیده می‌شود.

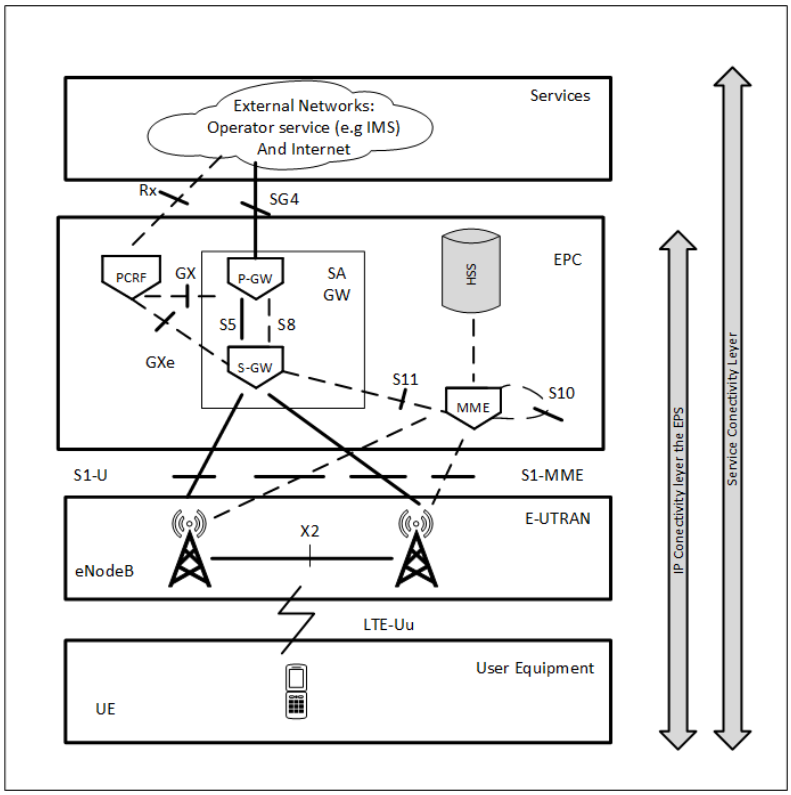
ادامه مقاله به شرح زیر است. بخش دو ارائه یک نمای کلی از معماری شبکه LTE خواهد بود. در بخش سه توصیف احراز هویت و سلسله مراتب کلید و در بخش چهار مدیریت کلید تشریح می‌گردد. در بخش پنج، آسیب‌پذیری احراز هویت و مدیریت کلید در شبکه LTE مورد بررسی قرار خواهد گرفت. در نهایت در بخش شش به فرآیند بومی‌سازی شبکه و ارائه ظرفیت‌های شبکه در این بحث خواهیم پرداخت.

۲- معماری شبکه LTE

به‌طور کلی معماری شبکه LTE شبیه به GSM[2] و UMTS[3] است. در اصل، شبکه به دو بخش شبکه رادیویی و شبکه هسته تقسیم می‌شود. معماری شبکه LTE به چهار زیر بخش اصلی تقسیم می‌شود که در شکل (۱) قابل مشاهده است [۳].

۲-۱- E-UTRAN[4]

تنها گره فیزیکی موجود در E-UTRAN و پیچیده‌ترین بخش شبکه LTE، ایستگاه پایه آن است که در متون eNodeB[5] نامیده می‌شود. eNodeB شامل سه المان مهم زیر است: آنتن‌ها، ماژول‌های رادیویی و ماژول‌های دیجیتالی.



شکل (۱): معماری شبکه LTE

1- IP Multimedia Subsystem

2- Global System for Mobile communications
3- Universal Mobile Telecommunications System
4- Evolved Universal Terrestrial Radio Access Networ
5- Evolved Node B

۲-۲- تجهیزات کاربر[1]

در مشخصات LTE مانند UMTS، دستگاه موبایل با UE نام‌گذاری می‌شود.

۲-۳- هسته بسته تکامل‌یافته [2]

نقش EPC در ساختار LTE، معادل شبکه هسته در سامانه‌های GSM/UMTS است. این بخش شامل تمام نهادهای عملکردی شبکه از جمله MME[3]، S-GW[4]، P-GW[5]، HSS[6] و PCRF[7] می‌باشد. EPC مسئول مدیریت تماس‌های صوتی، مدیریت اطلاعات تماس، صدور صورت‌حساب و دیگر عملکردهایی از این قبیل است.

۲-۳-۱- مرکز مدیریت جابه‌جایی

در واقع MME قلب EPC است. MME گره مسئول شبکه، برای همه مبادلات سیگنالینگ بین ایستگاه‌های پایه و شبکه هسته و نیز بین کاربران و شبکه‌های اصلی است. در شبکه‌های بزرگ، تعداد زیادی MME به دلیل وجود سیگنال‌های زیاد و افزونگی، وجود دارد. در حالت کلی MME وظایفی مانند تصدیق هویت، ایجاد کردن حامل‌ها، مدیریت تحرک NAS[8]، پشتیبانی از دست‌به‌دست شدن، تعامل با دیگر شبکه‌های رادیویی و پشتیبانی از صوت و SMS را بر عهده دارد.

۲-۳-۲- Serving Gateway

بخش S-GW مسئول مدیریت کانال‌های اطلاعاتی کاربر بین eNodeBها در شبکه رادیویی و P-GW که روتر درگاه اتصال به اینترنت است، است.

۲-۳-۳- Packet Data Network Gateway

سومین گره از هسته شبکه PDN-GW نام دارد که نقش یک درگاه برای دسترسی به شبکه خارجی را برعهده دارد. همچنین مسولیت اختصاص IP به دستگاه‌های موبایل نیز بر عهده این گره است.

۲-۳-۴- Home Subscription Server

واحد HSS محلی است که تمام اطلاعات دائمی کاربران نگهداری می‌شود. به علاوه، در این قسمت یک کپی از مشخصات سرویس‌هایی که قابل بهره‌برداری توسط مشترک است نیز ذخیره می‌شود. یک کلید دائمی برای انجام فرآیند احراز هویت توسط AuC[9] تولید شده و بعد از آن کلیدهای دیگر برای پشتیبانی از محرمانگی و یکپارچگی، از آن مشتق می‌شوند. AuC بخشی از HSS است. واحد HSS باید به‌طور مداوم نه تنها با MME، بلکه با دیگر MMEهای موجود در شبکه‌های دیگر نیز، در تعامل باشد.

۲-۴- خدمات حوزه اینترنتی[10]

این قسمت مانند بقیه بخش‌های EPC ثابت نیست و ممکن است شامل چندین زیرسامانه باشد که آن‌ها نیز شامل چندین گره‌ی منطقی هستند. از جمله خدمات فراهم شده به EPC می‌توان به IMS و شبکه اینترنت اشاره کرد.

۳- احراز هویت و سلسله مراتب کلید

این بخش چگونگی شناسایی و احراز هویت کاربر و توافق کلید در سامانه‌های EPS را توضیح می‌دهد. هر زمانی که UE و شبکه بخواهند به هم متصل شوند و مفاد امنیتی را به اشتراک بگذارند، برای احراز هویت دو طرفه و توافق کلید از فرآیند AKA[11] استفاده می‌کنند. این فرآیند به سه بخش عمده تقسیم شده است که عبارتند از [۴]:

احراز هویت: این مرحله به منظور احراز هویت کاربر به شبکه صورت می‌گیرد که در طی آن، به طور ضمنی شبکه نیز به کاربر احراز هویت خواهد شد. بعد از اتمام این مرحله، طرفین به یکدیگر معرفی شده و به کلید مشترک میانی برای ادامه گام‌های بعدی دست می‌یابند.

راه‌اندازی پروتکل NAS: بعد از مرحله‌ی احراز هویت، پروتکل NAS راه‌اندازی می‌شود که با برقراری این پروتکل، حفاظت از یکپارچگی و محرمانگی اطلاعات سیگنالینگ ایجاد خواهد شد. بعد از اتمام این مرحله، کلیدهای حفاظت از یکپارچگی و رمزنگاری برای اطلاعات سیگنالینگ و نیز الگوریتم‌های مورد نیاز برای آن‌ها، بین کاربر و شبکه به اشتراک می‌رسند.

راه‌اندازی پروتکل AS: در نهایت بعد از برقراری دو مرحله احراز هویت و پروتکل NAS، پروتکل AS راه‌اندازی می‌شود. با برقراری این پروتکل، رمزنگاری سطح کاربر و حفاظت از محرمانگی و یکپارچگی سیگنالینگ RRC ایجاد می‌شود و طرفین ارتباط به کلیدهای مشترک لازم، دست پیدا می‌کنند.

1- User Equipment
2 -Evolved Packet Core (EPC)
3- Mobility Management Entity
4- Serving Gateway
5- Packet Data Network Gateway
6- Home Subscriber Server
7- Policy and Charging Rules Function
8- Non-access stratum
9- Authentication Center
10-Services Domain
11- Authentication and Key Agreement

فرآیند AKA که در سامانه EPS استفاده می‌شود در سامانه UMTS نیز مورد استفاده قرار گرفته است. برای درک بهتر تفاوت‌های EPS AKA و UMTS AKA بهتر است که نقش هر یک از بخش‌های درگیر را با هم مقایسه کنیم. MME نقش VLR[1] را برای CS[2] و همچنین نقش SGSN[3] را برای PS[4] در UMTS AKA در شبکه‌های 3G بر عهده دارند. توجه شود که عملکرد MME نسبت به فعالیت‌های صورت گرفته در UMTS AKA، بسیار بیشتر است. ME و همچنین HSS، در هر دو پروتکل وظایف مشابه و نه دقیقا یکسانی را بر عهده دارند. USIM[5] مورد استفاده UMTS AKA در EPS AKA نیز قابل استفاده است؛ به صورت اختیاری امکان قرار دادن ویژگی‌های بیشتر برای آن در EPS AKA نیز وجود دارد [۵].

در ادامه هر کدام از این بخش‌ها به صورت جزیی تحلیل می‌شوند.

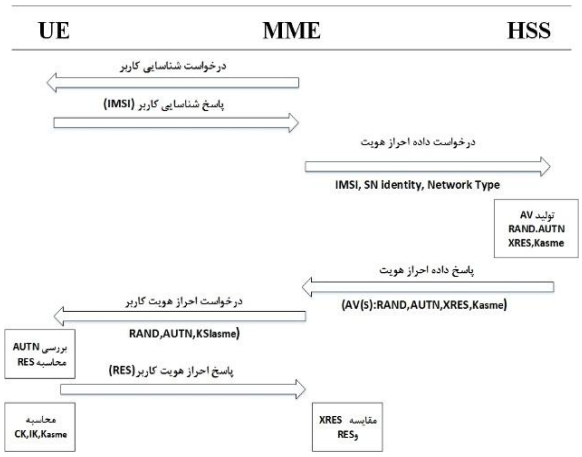
۳-۱- احراز هویت

در یک فرآیند AKA، همان‌طوری که در شکل (۲) مشاهده می‌شود، به محض درخواست از سمت MME، یک فرآیند برای تولید بردار احراز هویت[6](AV) در HSS و سپس توزیع به آن صورت می‌گیرد. MME با انتخاب یک EPS AV استفاده نشده موجود در بانک اطلاعاتی خودش، یک فرآیند احراز هویت را شروع می‌کند. اگر MME، EPS AV را موجود نداشته باشد، آن را از HSS درخواست خواهد کرد. هر EPS AV تنها برای راه‌اندازی یک فرآیند AKA بین MME و USIM قابل استفاده است. اطلاعات احراز هویت درخواستی باید شامل SNid[7] و IMSI[8] مربوط به MME درخواست‌کننده بوده و بیانگر اطلاعات احراز هویت سامانه EPS باشد. از SNid برای محاسبه کلید K_{ASME} در HSS استفاده می‌شود.

AV در سامانه UMTS شامل یک شماره تصادفی RAND، یک پاسخ قابل انتظار XRES، یک کلید رمزنگاری CK، یک کلید IK برای افزایش پیچیدگی سامانه و یک توکن تصدیق هویت AUTN است. این در حالی است که AV سامانه EPS شامل یک عدد تصادفی RAND، یک پاسخ قابل انتظار XRES، و یک کلید نشت محلی K_{ASME} و یک نشانه تصدیق هویت AUTN است.

AuC با تولید یک رشته عددی جدید SQN و یک RAND چالشی غیرقابل پیش‌بینی شروع به کار می‌کند. HSS برای هر کاربر، شمارنده SQN_{HE} را دنبال می‌کند.

به دنبال درخواست HSS، AuC مطابق توضیحاتی که در ادامه داده می‌شوند، مقادیری به شرح ذیل محاسبه می‌کند:



شکل (۲): فرآیند AKA

$$MAC = f1_k(SQN \,||\, RAND \,||\, AMF) \quad (۱)$$

$$XRES = f2_K(RAND) \quad (۲)$$

$$CK = f3_K(RAND) \quad (۳)$$

$$IK = f4_K(RAND) \quad (۴)$$

$$AK = f5_K(RAND) \quad (۵)$$

رابطه (۱) بیانگر یک کد احراز هویت است که f1 یک تابع تصدیق پیغام است. AuC باید بیت جداسازی را برای حالت AMF برابر "یک" و در سایر حالات برابر "صفر" EPS استفاده در سامانه یک تابع تصدیق f2قرار دهد. رابطه (۲) یک پاسخ قابل انتظار و یک تابع تولید f3پیغام می‌باشد. رابطه (۳) یک کلید رمزنگاری و یک تابع تولید f4کلید است. رابطه (۴) یک کلیدیکپارچگی و یک تابع تولید f5کلید می‌باشد. رابطه (۵) یک کلید گمنامی و کلید است و برابر با صفر نیز می‌تواند باشد. در نهایت رابطه (۶) که توکن تصدیق است، محاسبه می‌شود.

اگر اپراتور تصمیم بگیرد که برای SQN پوششی نیاز نیست، f5=0 قرار داده خواهد شد (AK=0).

بعد از فراهم شدن بردار AV، MME یک RAND چالشی

1- Visitors Location Register
2- circuit switched
3- Serving GPRS Support Node
4- packet switched
5- Universal Subscriber Identity Module
6- Authentication Vector
7- Serving Network Identity
8- International Mobile Subscriber Identity

تصادفی و یک توکن احراز هویت برای احراز هویت شبکه –AUTN– به ME ارسال می‌کند، که ME آن را برای USIM نیز می‌فرستد. هم‌چنین MME یک شناسه تنظیم کلید در EPS[1] نیز تولید می‌کند، که درخواست احراز هویت شامل آن نیز می‌باشد.

در سمت کاربر، USIM پس از دریافت RAND و AUTN با همان روند قبل شروع به کار می‌کند. USIM ابتدا $AK = f5_K(RAND)$ را محاسبه می‌کند. سپس $AUTN=(SQN \text{ xor } AK)$ را بازیابی کرده و بعد از آن $XMAC=f1_k(SQN \| RAND \| AMF)$ را محاسبه می‌کند و آن را با MAC موجود در AUTN مطابقت می‌دهد. در نهایت، USIM صحیح و مجاز بودن رنج SQN را مورد تایید قرار می‌دهد. اگر SQN در رنج درست قرار داشته باشد، USIM، $RES = f2_K(RAND)$ را محاسبه کرده و برای ME ارسال می‌کند، RES در پیغام پاسخ احراز هویت ارسالی به MME قرار می‌گیرد. همچنین USIM، کلید رمز CK و کلید یکپارچگی IK را محاسبه کرده و آن ها را برای ME ارسال می‌کند.

پس از دریافت پیغام پاسخ احراز هویت، MME، RES دریافتی را با XRES که از AV جدا شده است، تطابق می‌دهد. اگر هم‌خوانی داشته باشد، احراز هویت کاربر موفقیت‌آمیز بوده است [۴].

با توجه به مطالب ذکر شده، می‌توان این‌طور بیان کرد که EPS AKA تعمیم داده شده UMTS AKA است. این امر بدین معناست که توافق کلید EPS و UMTS شبیه یکدیگر است و تفاوت اساسی در راه‌اندازی درخواست احراز هویت، تایید در USIM و پاسخ احراز هویت بین UMTS AKA و EPS AKA وجود ندارد. یکی از پیشرفت‌هایی که EPS AKA نسبت به UMTS AKA داشته است، تصدیق هویت ضمنی شبکه سرویس دهنده(SN)[2] توسط EPS AKA است که در UMTS AKA اتفاق نمی‌افتد. تصدیق هویت ضمنی SN، با بسته شدن یک کلید K_{ASME} مناسب، به شناسه شبکه سرویس‌دهنده و استفاده موفق از کلید با جابه‌جایی پیغام‌های بعد از احرازهویت، حاصل خواهد شد [۵].

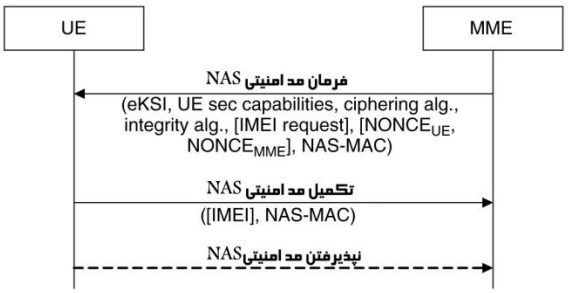
۳-۲- راه‌اندازی پروتکل NAS

در فرآیند فرمان مد امنیتی NAS همان‌طوری که در شکل (۳) مشخص شده است، MME پیام فرمان مد امنیتی NAS را به UE ارسال می‌کند و UE با پیام تکمیل فرمان مد امنیتی NAS یا پیام رد شدن آن، به MME پاسخ می‌دهد. یک پیغام NAS SMC از قابلیت‌های امنیتی UE و الگوریتم‌های انتخاب شده برای حفاظت از سیگنالینگ NAS تشکیل شده است. این پیغام هم‌چنین شامل یک شناسه تنظیم کلید است. این شناسه، سلسله مراتب کلید صحیحی را که برای مشتق شدن کلیدها از آن استفاده می‌شود، شناسایی می‌کند. علاوه‌بر این، کلیدی که برای حفاظت یکپارچگی پیغام استفاده می‌شود را نیز شناسایی می‌کند.

وقتی MME پیام مد امنیتی NAS را به UE ارسال می‌کند، UE با استفاده از ورودی‌هایی از قبیل K_{ASME} و الگوریتم‌های دریافتی توسط یک تابع KDF کلیدهای KNASenc و KNASint را می‌سازد. این تولید کلید در سمت MME نیز اجرا می‌شود.

NAS SMC به‌صورت یکپارچه-حفاظت شده است به‌طوری که UE می‌تواند یکپارچگی آن را بررسی کند ولی برای رمزنگاری قادر به بررسی نیست، چرا که هنوز نمی‌داند کدام الگوریتم و کلید برای رمزگشایی استفاده می‌شود.

از آنجا که شبکه از قبل می‌داند که کدام الگوریتم‌ها و کلیدها انتخاب شده‌اند، می‌تواند پیام‌های رمزشده را دریافت کند. بنابراین UE پیغام NAS SMC را به صورت رمز شده و یکپارچه حفاظت شده، ارسال می‌کند. MME بعد از بررسی کردن موفقیت‌آمیز NAS SMC، رمز کردن سیگنالینگ پایین سو را آغاز می‌کند. MME بعد از فرستادن پیام NAS SMC، رمزگشایی سیگنالینگ NAS بالاسو را آغاز می‌کند. در نتیجه بعد از برقراری موفقیت‌آمیز پروتکل NAS، رمزنگاری و یکپارچگی حفاظت شده برای سیگنالینگ فراهم می‌شود.



شکل (۳): فرمان مد امنیتی NAS

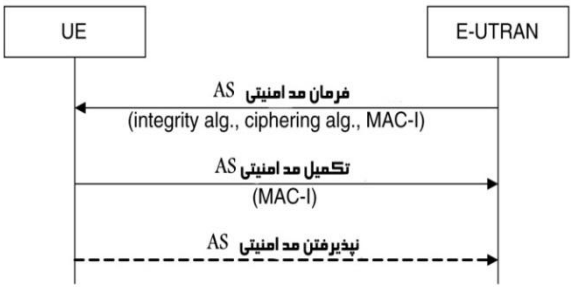
۳-۳- راه‌اندازی پروتکل AS

همان‌طوری که در شکل (۴) تصویر شده است، ایستگاه پایه یک فرمان مد امنیتی AS که شامل الگوریتم‌های رمزنگاری و یکپارچگی انتخاب شده و یک MAC-I است را به UE به‌صورت یکپارچه حفاظت شده ارسال می‌کند. UE با استفاده از ورودی‌هایی که از پیام دریافت می‌کند، کلیدهایی را تولید کرده و

1- Key Set Identifier
2- Serving Network

MAC دریافتی را رمز می‌کند و در نهایت به ایستگاه پایه ارسال می‌کند. ایستگاه پایه پیام را رمزگشایی می‌کند و MAC را با MAC خودش مقایسه کرده و آن را بررسی می‌کند. سپس اگر کد درست باشد، یکپارچگی سیگنالینگ سطح کنترل و حفاظت باز بخش آغاز می‌شود و آماده می‌شوند تا پیام‌های سطح کاربر و کنترل پایین سوی رمزشده را دریافت کنند.

لازم به ذکر است، پروتکل سیگنالینگ سطح AS، پروتکل کنترل منابع رادیویی (RRC) نامیده می‌شود. هر دو اطلاعات سطح کاربر و سیگنالینگ RRC روی پروتکل بسته همگرایی اطلاعات (PDCP) حمل می‌شوند. به‌علاوه امنیت روی لایه PDCP اجرا می‌شود. به این ترتیب، هر دو حفاظت سیگنالینگ و حفاظت اطلاعات سطح کاربر می‌توانند از یک ساختار مشابه روی سطح PDCP استفاده کنند [۴].



شکل (۴): فرمان مد امنیتی AS

۴- مدیریت کلید

طبق توضیحات قبل، EPS AKA تعمیم داده شده UMTS AKA است. برای UMTS کلیدهای CK و IK در طی اجرای UMTS AKA تولید می‌شود. تمام کلیدهای امنیتی که برای سازوکارهای امنیتی مختلف مورد نیاز است، از کلید میانی K_{ASME} استخراج می‌شوند که این می‌تواند به‌عنوان "کلید اصلی محلی" در مقابل کلید اصلی دائمی K برای مشترکین شناخته شود. از دید شبکه، کلید میانی محلی اصلی K_{ASME} در MME ذخیره می‌شود و کلید دائمی اصلی K در Auc ذخیره می‌شود. مزیت استفاده از کلید میانی به شرح زیر است [۴]:

این امکان را فراهم می‌کند که کلیدهای رمزنگاری تفکیک شوند، به این ترتیب که هر کلید تنها برای یک ویژگی مخصوص استفاده شود.

این امر سامانه را در حالتی قرار می‌دهد که کلیدهای تازه تولید کند. به عبارت دیگر این امکان فراهم می‌شود که کلیدهای باز تولیدشده بیشتری در سازوکارهای امنیتی به‌کار روند.

به‌طور واضح، استفاده از کلید میانی یک عیب دارد و آن هم افزایش پیچیدگی سامانه است. روی هم رفته یک داد و ستد بین پیچیدگی و خواسته‌ها وجود دارد. برای EPS، مزایای امنیتی استفاده از کلید میانی، خیلی بیشتر از معضل اضافه کردن پیچیدگی است.

به‌طور کلی سلسله مراتب کلید شامل یک کلید ریشه (K) چندین کلید میانی ($CK.IK,K_{ASME},K_{eNB},NH$) و چندین کلید دیگر مثل (K_{UPint}, K_{NASenc}, K_{NASint}, K_{RRCenc}, K_{RRCint}, K_{UPenc}) است. در ادامه اهداف کلیدها و سودمندی‌شان را به‌طور خلاصه بیان می‌کنیم.

K: کلید نشست ویژه مشترک است که در AuC و USIM ذخیره می‌شود. این کلید از هیچ کلید دیگری مشتق نمی‌شود و یک کلید ۱۲۸بیتی تصادفی است.

CK و IK: کلیدهای ۱۲۸ بیتی هستند که به کمک پارامترهای ورودی فرعی از K مشتق می‌شوند.

K_{ASME}: از دو کلید IK و CK به کمک دو پارامتر ورودی فرعی مشتق می‌شود. این دو پارامتر عبارتنداز:

۱- SNid که از MNC[1] و MCC[2] تشکیل شده است. برای اینکه کلید به شبکه ارتباط داده شود استفاده می‌شود.

۲- پارامتر حاصل از عملیات بیتی[3] دو پارامتر فرعی AK و SQN. توجه شود که AK خودش کلیدی است که در طی EPS AKA مشتق می‌شود و مقدار (SQN xor AK) بخشی از پارامتر AUTN است که در طی فرایند EPS AKA در متن خام ارسال می‌شود. بنابراین، فرض می‌شود که به‌صورت بالقوه مهاجم از آن آگاهی دارد. هدف از K_{ASME} این است که به عنوان کلید محلی در MME ذخیره شود.

K_{eNB}: از کلید K_{ASME} و یک پارامتر شمارنده NASUPLINK (COUNT) مشتق می‌شود. این پارامتر برای اطمینان از اینکه هر کلید K_{eNB} جدید که از K_{ASME} مشتق می‌شود با دیگر کلیدهایی که زودتر استخراج شده‌اند متفاوت است، ضروری است. هدف از این کلید، ایجاد یک کلید نشت محلی در eNB است.

NH: یک نوع دیگر کلید میانی است که در موقعیت دست‌به‌دست شدن[4] نیاز است. NH از K_{ASME} مشتق می‌شود. از کلید مشتق شده جدید K_{eNB} و NH قبلی به‌عنوان پارامتر ورودی برای به‌دست آوردن NH بعدی استفاده می‌کند. برای مرحله بعد

1- Mobile Network Code
2- Mobile Country Code
3- BIT-WISE
4- Handover

استفاده می‌کند. به جز موارد ذکر شده، کلید میانی دیگری نیز وجود دارد که برای به‌دست آمدن K_{eNB} باید مشتق شود. این کلید K_{eNB}^{*} نامیده می‌شوند که از K_{eNB} یا NH که به‌صورت پارامتر وجود داشته باشند، استخراج می‌شود. پارامترهای فرعی ID سلول فیزیکی و فرکانس پایین سو برای ارتباط دادن کلید به بستر محلی استفاده می‌شوند. در دست‌به‌دست شدن کلید K_{eNB}^{*} درایستگاه پایه هدف به K_{eNB} جدید تبدیل می‌شود.

K_{NASenc}: کلیدی است که ترافیک سیگنالینگ NAC را رمز می‌کند. این کلید ازکلید K_{ASME} و دو پارامتر فرعی استخراج می‌شود. اولین پارامتر، متمایزکننده مدل الگوریتم[1] نامیده می‌شود که در مورد کلید K_{NASenc} مقداری دارد که برای رمزنگاری NAS استفاده می‌شود. دومین پارامتر، شناسه الگوریتم رمزنگاری است.

K_{NASint}: این کلید برای حفاظت از یکپارچگی ترافیک سیگنالینگ NAS مورد استفاده قرار می‌گیرد. این کلید نیز از K_{ASME} و دو پارامتر فرعی تولید می‌شود. اولی که همان متمایزکننده مدل الگوریتم است، اشاره دارد به این که کلید برای یکپارچگی NAS استفاده می‌شود و دومی شناسه الگوریتم یکپارچگی است.

K_{RRCenc}: کلیدی است که برای رمزنگاری ترافیک سیگنالینگ RRC استفاده می‌شود. این کلید از کلید K_{eNB} و دو پارامتر فرعی مشتق می‌شود. اولین پارامتر فرعی متمایزکننده مدل الگوریتم است. این پارامتر اشاره به این دارد که کلید برای رمزنگاری RRC استفاده می‌شود و دومی شناسه الگوریتم رمزنگاری است.

K_{RRCint}: این کلید برای حفاظت از یکپارچگی ترافیک سیگنالینگ RRC استفاده می‌شود. مشابه کلید قبلی این کلید از کلید K_{eNB} و دو پارامتر فرعی مشتق می‌شود. اولین پارامتر فرعی اشاره دارد به این که کلید برای یکپارچگی RRC استفاده می‌شود و دومی شناسه الگوریتم یکپارچگی است.

K_{UPenc}: این کلید برای رمزنگاری ترافیک UP استفاده می‌شود که از K_{eNB} و دو پارامتر فرعی مشتق می‌شود. اولین پارامتر فرعی اشاره دارد به این که کلید برای رمزنگاری UP استفاده می‌شود و دومی شناسه الگوریتم رمزنگاری است.

K_{UPint}: این کلید برای حفاظت از یکپارچگی نوع خاصی از ترافیک UP استفاده می‌شود. این کلید فقط روی واسط Un بین relay node و Donor eNB استفاده می‌شود، و روی واسط بین UE و ایستگاه پایه استفاده نمی‌شود. به همین دلیل روی شکل جعبه‌ای با نقطه‌چین کشیده شده است. این کلید از کلید K_{eNB} و دو پارامتر فرعی مشتق می‌شود. اولین پارامتر فرعی اشاره دارد به این که کلید برای یکپارچگی UP استفاده می‌شود و دومی شناسه الگوریتم یکپارچگی است.

کلیدهای بیشتری وجود دارند که برای تعاملات EPS با دیگر سامانه‌ها مورد نیاز هستند برای مثال کلید 'CK کلیدی است که از K_{ASME} مشتق شده و بعد از دست به‌دست شدن از EPS به 3G، برای رمزنگاری استفاده می‌شود [۴].

۵- آسیب‌پذیری EPS AKA و معماری LTE

همان‌طوری که ذکر شد، 3GPP الزامات امنیتی، ویژگی‌ها، تهدیدها و راه‌حل‌هایی را برای مشکلات امنیتی مربوطه مشخص کرده است. با این حال هنوز هم برخی از آسیب‌پذیری‌ها و مشکلات امنیتی در معماری امنیتی LTE وجود دارند. در این بخش نقاط ضعف موجود را با جزئیات دقیق، در چهارچوب امنیتی LTE بررسی می‌کنیم.

۵-۱- آسیب‌پذیری معماری LTE

شبکه LTE برای معماری تماما IP و نیز پشتیبانی کامل از تعامل با شبکه‌های دسترسی رادیویی ناهمگون، طراحی شده است. این ویژگی منحصربه‌فرد شبکه LTE موجب چالش‌های جدید در مکانیسم طراحی می‌شود [۵].

۱) معماری بر مبنای IP در شبکه‌های LTE منتج به خطرپذیری مانند حملات تزریق اطلاعات جعلی، اصلاح اطلاعات و یا استراق سمع می‌شود. همچنین منتج به احتمال خطر بیشتری هم نسبت GSM و UMTS در حفظ حریم خصوصی خواهد شد [۷] و [۶] این مساله نشان می‌دهد که معماری LTE نسبت به حمله‌های مخرب سنتی که در اینترنت وجود دارد مانند حمله‌های IP SPOOFING، DOS، ویروس‌ها، هرزنامه‌ها، هرزتماس‌ها و ... آسیب‌پذیرتر است [۸].

۲) بعضی از نقاط ضعف بالقوه دیگر، ناشی از ایستگاه‌های پایه موجود در سامانه‌های LTE است. شبکه تماما IP یک مسیر مستقیم برای حمله مخرب به ایستگاه پایه فراهم می‌کند. از آن جا که در معماری تخت LTE، MME چندین eNB را مدیریت می‌کند، ایستگاه‌های مرکزی در مقایسه با معماری UMTS، خیلی بیشتر مستعد حمله می‌باشند. هنگامی که یک مهاجم یک ایستگاه پایه را به خطر می‌اندازد، به دلیل ماهیت تمام IP شبکه

1- Algorithm Type Distinguisher

LTE، احتمال این که کل شبکه به خطر بیافتد بیشتر است [۹].

۳) در معماری شبکه‌های LTE، ممکن است مشکلات جدیدی در فرآیند احراز هویت در زمان دست‌به‌دست شدن روی دهد. سناریوهای مختلفی برای جابه‌جایی در شبکه LTE در حالتی که UE از یک eNB/HeNB به یک HeNB/eNB جدید جابه‌جا می‌شود وجود دارد. به هر حال، فرآیندهای مجزای دست‌به‌دست شدن به سناریوهای مختلفی نیاز دارند، مانند دست‌به‌دست شدن بین eNBها بین HeNBها، بین HeNB و eNB و دست‌به‌دست شدن‌های داخلی MME که همه این‌ها پیچیدگی سامانه را افزایش می‌دهند. علاوه بر این ممکن است چندین شبکه دسترسی ناهمگون در شبکه LTE موجود باشند که این مساله تهدیدها علیه امنیت شبکه را بیشتر می‌کند. علی‌الخصوص زمانی که جابه‌جایی در این شبکه‌های ناهمگون پشتیبانی شود. کمیته 3GPP چندین روش مختلف برای دست‌به‌دست شدن امن و بدون نفوذ E_UTRAN و شبکه‌های دسترسی Non-3GPP ارائه کرده است. اما در آن‌ها باید به طریقی تمام فرآیند احراز هویت دسترسی بین UE و شبکه دسترسی جدید، قبل از اینکه UE به شبکه دسترسی جدید دست‌به‌دست شود، انجام شود؛ که این مساله یک فرآیند دست‌به‌دست شدن با تاخیر بیشتر را ایجاد می کند. دلیل آن این است که باید چندین بار پیغام‌های احراز هویت، اجازه اتصال و حسابرسی سرور AAA جابه‌جا شود. علاوه‌بر این، سناریوهای مختلف جابجایی برای فرآیند احراز هویت در دست‌به‌دست شدن وجود دارد که این پیچیدگی کلی سامانه را افزایش می‌دهد. این آسیب‌پذیری‌ها نه تنها باعث ناپیوستگی در اتصال به شبکه LTE می‌شود، هم چنین باعث سوءاستفاده مهاجمان برای حمله به سایر شبکه‌های دسترسی از این طریق و یا از طریق شبکه اصلی به منابع شبکه، حتی تا مرز فلج کردن شبکه، می‌شوند [۱۰].

۵-۲- آسیب‌پذیری فرآیند AKA

فرآیند EPS AKA نسبت به UMTS AKA در برخی شرایط بهبود پیدا کرده است. مانند حملات تغییر مسیر[1]، حملات ایستگاه پایه جعلی، و حملات MitM. علی‌رغم همه این‌ها هنوز هم در سازوکار دسترسی به LTE نقاط ضعف وجود دارد که به شرح زیر هستند [۵]:

۱) طرح EPS AKA فاقد حفاظت از حریم خصوصی است. در بسیاری از موارد امکان افشای IMSI وجود دارد. به‌عنوان مثال وقتی UE برای اولین بار ثبت می‌شود و یا این‌که تماس نمی‌تواند با MME برقرار شود. بنابراین، UE برای ارسال IMSI باید آن را به شکل یک پیغام رمزی ارسال کند. افشای IMSI ممکن است باعث ایجاد مشکل شدید امنیتی شود. اگر IMSI فاش شود، مهاجم می‌تواند اطلاعات کاربر، اطلاعات مربوط به مکان و حتی اطلاعات مکالمه را به‌دست بیاورد. سپس UE واقعی را پنهان کند و حملات دیگری مانند DOS را راه اندازی کند تا در نهایت منجر به تخریب شبکه شود. در مقاله [۱۰] مدل حمله فعال برای سرقت IMSI ارائه شده است که از طریق آن، IMSI به راحتی توسط یک مهاجم فعال قابل افشا شدن است. بنابراین، سازوکارهای امنیتی حال حاضر، نمی‌تواند جلوی حملات فعال این چنینی را بگیرد.

۲) طرح EPS AKA نمی‌تواند از حملات DOS جلوگیری کند. [۱۳-۱۱]. MME باید پیام درخواست UE را به HSS/AuC، حتی قبل از این‌که UE توسط او احراز هویت شده باشد ارسال کند. به‌علاوه MME تنها زمانی می‌تواند UE را احراز هویت کند که RES دریافت شده باشد. بر اساس شرایط ذکر شده، یک مهاجم می‌تواند حملات DOS را روی HSS/AuC و MME راه‌اندازی کند. ضمنا مهاجم می‌تواند با یک UE قانونی پنهانی به‌طور مداوم IMSIهای جعلی را برای مختل کردن HSS/AuC ارسال کند. در این حالت HSS/AuC باید توان زیادی را صرف محاسبات تولید بردار احراز هویت برای UE کند. از طرف دیگر، MME نیز باید حافظه بافر خود را به مدت طولانی برای پاسخ قانونی بودن UE یا عدم آن، اشغال نگه دارد. علاوه بر موارد ذکر شده، در مقاله [۱۴] نشان داده شده است که فرآیند امنیتی NAS، در برابر حملات DOS آسیب‌پذیر است و در فرآیند NAS چندین DOS پیدا شده که باعث اشباع شدن در E-UTRAN می‌شوند.

۳) پروتکل EPS AKA همانند پروتکل GSM AKA و UMTS AKA، یک پروتکل محول شده[2] است. تقریبا تمام مسولیت احراز هویت از شبکه خانگی به شبکه ملاقات شده محول شده است که این مساله نیازمند اعتماد زیاد به مفروضات بین اپراتورها است. به علاوه، EPS AKA فاقد قابلیت احراز هویت آنلاین است، به این دلیل که HN با توجه به فرآیند احرازهویت بین UE و SN، بیرون‌خط است [۱۵].

۶- بررسی امکان بومی‌سازی امنیتی شبکه LTE

در این بخش به بررسی بخش‌هایی از معماری امنیتی شبکه LTE که امکان بومی‌سازی آن‌ها وجود دارد می‌پردازیم. همان‌طوری که

1- Redirection

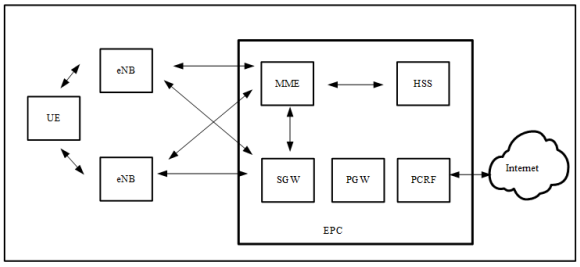
2- Delegated Protocol

قبل از این ذکر گردید، بخشی از امنیت اساسی هر کشوری با امن بودن شبکه‌های مخابراتی عمومی و خصوصی آن تامین می‌گردد. در سامانه‌های مخابراتی تا آن‌جایی که ممکن است و در چارچوب استانداردها، باید سخت‌افزارها، پروتکل‌ها و توابع مرتبط با آن‌ها باز طراحی و تولید گردد. در این مقاله در چارچوب استانداردهای 3GPP، ظرفیت‌های ممکن بومی‌سازی در شبکه LTE مورد بررسی قرار می‌گیرد.

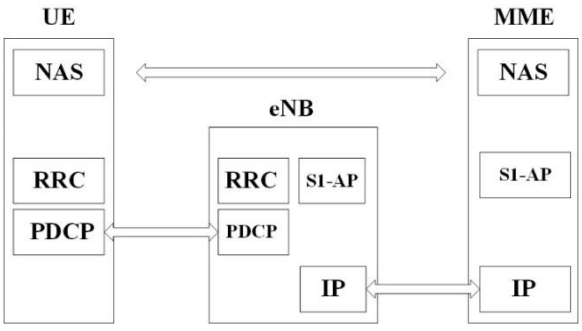
۶-۱- بومی سازی معماری امنیتی EPC

تمامی ارتباط‌های میان اجزای شبکه EPC، مستقل از این‌که تغییری در سمت تلفن همراه کاربر و یا سیم‌کارت کاربر ایجاد شود را می‌توان به صورت بومی طراحی کرد. با توجه به شکل (۵) این ارتباط‌ها شامل ارتباط میان MME با HSS و SGw و eNBها و یا ارتباط میان PGw و PCRF و یا ارتباط میان SGW با eNBها می‌باشد. با توجه به شکل (۶) و شکل (۷) این بومی‌سازی احتمالاً می‌تواند در پروتکل‌های S1-AP و GTP-U و ارتباط IPSec بین eNBها و MME یا SGw انجام شود.

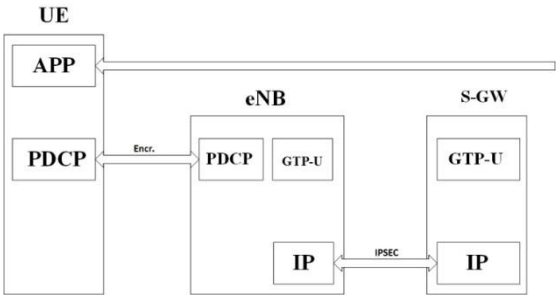
بنابراین به طور خلاصه با توجه به شکل (۱) نحوه ارتباط و پروتکل‌های ارتباطی در لایه‌های S1-U، S1-MME، S6a، S11 می‌توانند به صورت بومی طراحی شوند.



شکل (۵): معماری شبکه LTE



شکل (۶): حفاظت سطح سیگنالینگ EPS



شکل (۷): حفاظت سطح دیتای کاربر در EPS

۶-۲- بومی سازی معماری امنیتی HSS

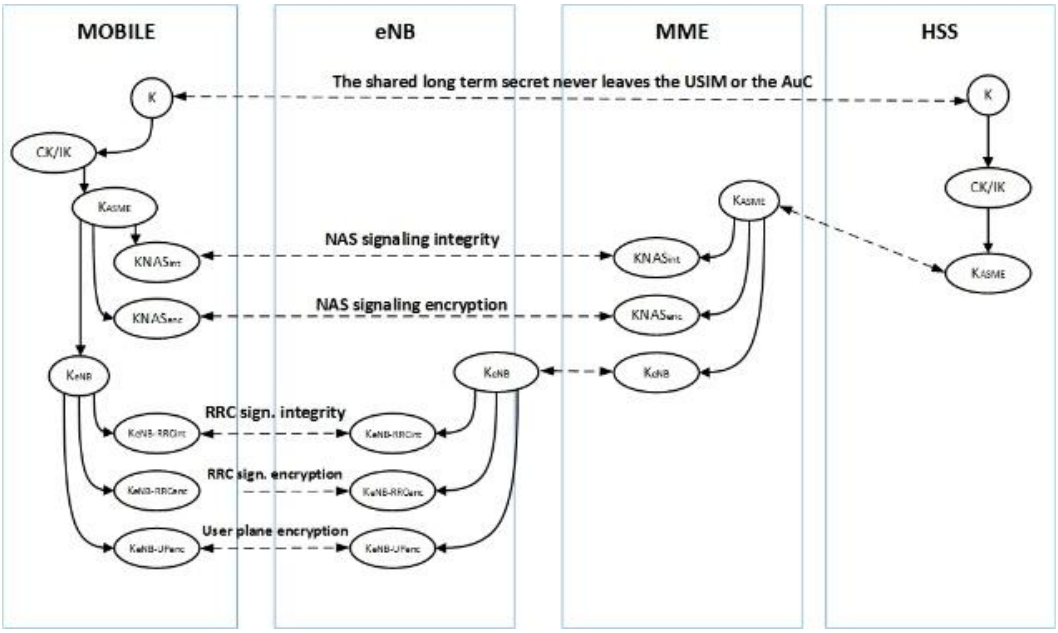
با توجه به شکل (۸) کلیدهای CK/IK در سمت کاربر توسط USIM کاربر و در سمت شبکه توسط HSS و یا AuC محاسبه و تولید می‌شود، بنابراین، اگر قرار باشد تا HSS و یا AuC به‌صورت بومی طراحی گردد نیازمند این هستیم که USIM را هم در سمت کاربر به صورت بومی طراحی کنیم و یا نحوه تولید کلیدهای CK/IK را در سمت شبکه (HSS و یا AuC) و در سمت کاربر (سیم‌کارت کاربر USIM) استاندارد کنیم.

همچنین با توجه به شکل (۸) از آن‌جایی که کلید $\mathbf{K_{ASME}}$ در سمت شبکه در HSS تولید می‌شود و در سمت کاربر در ME (گوشی تلفن همراه کاربر) بنابراین، جهت بومی‌سازی HSS باید تلفن همراه کاربر هم بتواند فرآیند تولید کلید $\mathbf{K_{ASME}}$ را از روی کلید CK/IK انجام دهد یعنی یا باید تلفن همراه هم بومی شود و یا نحوه تولید کلید $\mathbf{K_{ASME}}$ از روی کلیدهای CK/IK کاملاً مطابق استانداردهای 3GPP انجام شود.

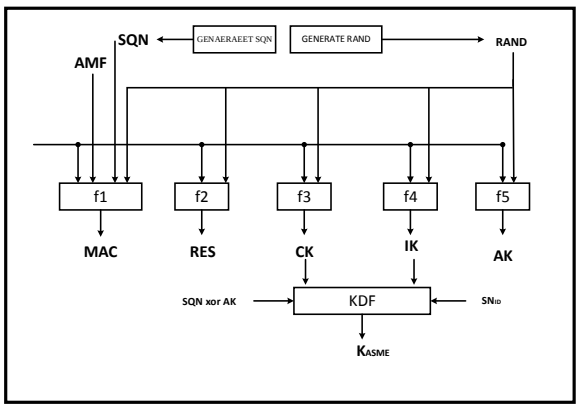
بنابراین، به‌طور خلاصه برای بومی‌سازی HSS باید سیم‌کارت و گوشی تلفن همراه هم در سمت کاربر بومی شود. با توجه به این‌که پروتکل احراز اصالت و توافق کلید AKA در سمت شبکه در HSS و در سمت کاربر در USIM اجرا می‌شود بنابراین، برای بومی‌سازی آن باید این تغییرات هم در سمت شبکه یعنی در HSS و هم در سمت کاربر یعنی در USIM پشتیبانی شود.

قبل از آن‌که حفاظت مخابراتی بتواند انجام شود، UE و شبکه نیاز دارند تا برای الگوریتم امنیتی که استفاده می‌کنند به توافق برسند. EPS الگوریتم‌های امنیتی زیادی را پشتیبانی می‌کند و شامل دو دسته الگوریتم اجباری 128-EEA1, 128-EIA1 بر مبنای SNOW 3G و 128-EEA2 و 128-EIA2 بر مبنای AES است که تمامی پیاده‌سازی‌های UEها، eNBها و MMEها باید آن‌ها را پشتیبانی کنند به علاوه دسته سومی از الگوریتم‌های امنیتی که اختیاری هستند نیز پیاده‌سازی می‌شود

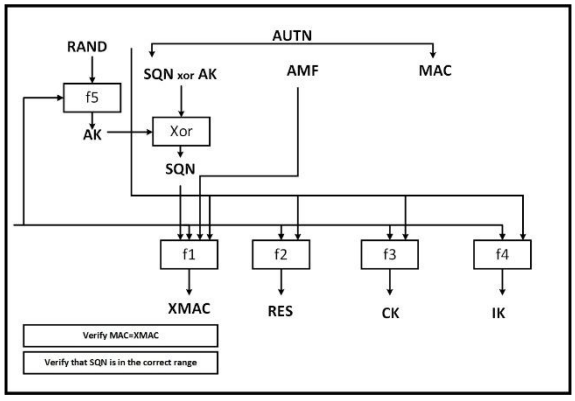
مانند 128-EEA3 و 128-EIA3 که بر مبنای ZUC هستند. شبکه، الگوریتم‌ها را بر اساس توانایی‌های UE و لیست الگوریتم‌هایی که برای شبکه مجاز است، آن‌ها را انتخاب می‌کند. UE توانایی‌های امنیتی خود را هنگامی که به شبکه متصل می‌شود و زمانی که در حال ارسال پیام درخواست Tracking Area Update (TAU) است و بعد از Handover به Evolved Universal Terrestrial Radio Access Network (E-UTRAN) اعلام می‌کند. توانایی‌های سطح سیگنالینگ AS، سیگنالینگ NAS و دیتای کاربر مشابه است فقط UE در دیتای کاربر نیازی به حفاظت یکپارچگی ندارد. باید توجه کرد که طبق استاندارد [TS33.401] اعمال فرآیندهای رمزگذاری و یکپارچگی در سطح NAS و AS بر عهده اپراتور گذاشته شده است و توسط شبکه EPC در پروتکل PDCP تعیین می‌گردد. بنابراین، برای بومی‌سازی پروتکل AKA باید امکان پیاده‌سازی و اجرای آن در سمت تلفن همراه کاربر هم فراهم باشد. با توجه به شکل‌های (۱۰-۹) از آن‌جایی که توابع f1 تا f5 و تابع KDF هم در سمت کاربر و هم در سمت شبکه مورد استفاده قرار می‌گیرند. بنابراین، برای تغییر و بومی‌سازی آن‌ها باید این تغییرات هم در سمت دستگاه تلفن همراه کاربر و هم در سمت شبکه در بخش‌های HSS و MME صورت پذیرد.



شکل (۸): توافق کلید در سامانه EPS



شکل (۹): تولید بردارهای احراز اصالت در EPS



شکل (۱۰): فرایند احراز اصالت در USIM

۶-۳- بومی‌سازی معماری امنیتی MME

برای بومی‌سازی MME، در آن بخش‌هایی که مربوط به ارتباط‌های میان MME و سایر بخش‌های EPC می‌شود، نیازمند تغییر در سمت UE نیست. برای تغییرات و بومی‌سازی روتکل‌های

داخلی آن، با توجه به این‌که کلیدهای K_{NASenc}، K_{NASint} و K_{eNB} در آن تولید می‌شود نیازمند تغییرات در سمت UE است.

۶-۴- بومی‌سازی معماری امنیتی eNB

با توجه به این‌که کلیدهای K_{RRCenc} ، K_{RRCint} و K_{UPenc} که برای رمزگذاری و یکپارچگی ارتباط سیگنالینگ و رمزگذاری دیتای کاربر استفاده می‌شوند در سمت eNB و سمت UE به طور جداگانه محاسبه و تولید می‌شوند بنابراین، برای تغییر و بومی‌سازی eNBها باید این تغییرات در سمت UE نیز قابل اعمال باشد. پروتکل مورد استفاده در محرمانگی بین کاربر و eNB پروتکل PDCP می‌باشد.

اما نحوه ارتباط eNBها با یکدیگر و ارسال و دریافت اطلاعات بین آن‌ها و با بخش‌های مختلف EPC نیازمند تغییراتی در سطح گوشی تلفن همراه کاربر نمی‌باشد. این تغییرات در واسط X2، S1-U و S1-MME انجام می‌شود.

همچنین استفاده و یا عدم استفاده از گواهی برای شناسایی eNBها و شبکه EPC طبق استاندارد [TS33.401] بر عهده اپراتور گذاشته شده است.

۷-۴- جدول نهایی بومی‌سازی

همان‌طور که در جدول (۱) مشخص شده است، اجزا شبکه و محتواهای مشترک (به‌طور خاص در این جدول به کلیدها اشاره شده است) بین آن اجزا مشخص شده است.

جدول (۱): توزیع کلید در گره‌های شبکه با رویکرد بومی‌سازی

	USIM	UE	eNB	MME	HSS
AKA					
KDF_{NAS}		■		■	
KDF_{AS}		■	■		
HSS					
CK/IK	■				■
K_{ASME}		■		■	
MME					
K_{NASenc}		■		■	
K_{NASint}		■		■	
K_{enb}		■		■	
eNB					
K_{RRCenc}		■	■		
K_{RRCint}		■	■		
K_{UPenc}		■	■		

برای مثال کلید KDF_{NAS} بین UE و MME مشترک است. این اشتراک همان‌طور که قبل از این ذکر گردید امکان بومی‌سازی توابع، پروتکل‌های و محتواهای بین این دو بخش را ممکن می‌سازد. در جدول (۱) خلاصه‌ای از مواردی که در بالا توضیح داده شده است.

۷- نتیجه‌گیری

به‌طور خلاصه بسیاری از تغییرات در توابع تولید کلید و پروتکل‌های ارتباطی در بخش‌های مختلف، نیازمند امکان اعمال همان تغییرات در سمت گوشی تلفن همراه کاربر نیز می‌باشد و گوشی تلفن همراه کاربر باید بتواند این تغییرات و فرآیندهای جدید را پشتیبانی کند. اما تغییرات در نحوه ارسال و دریافت اطلاعات در بخش‌های مختلف شبکه ارتباطی و بین اجزای داخلی شبکه نیازمند تغییراتی در سطح گوشی تلفن همراه کاربر نمی‌باشد.

با توجه به شکل (۸) برای بومی‌سازی پروتکل AKA که شامل توابع f1 تا f5 می‌باشد باید امکان پیاده‌سازی این تغییرات هم در سمت HSS و هم در سمت USIM وجود داشته باشد. اصولاً HSS و USIM همواره در اختیار اپراتور می‌باشد و هر تغییری اپراتور در HSS اعمال کند باید در USIM نیز منظور گردد.

همچنین برای بومی‌سازی تابع استخراج کلید KDF در سطح امنیتی NAS (که شامل کلیدهای K_{NASenc}، K_{NASint} و K_{eNB} است) باید امکان پیاده‌سازی این تغییرات هم در سمت MME و هم در سمت UE وجود داشته باشد.

همچنین برای بومی‌سازی تابع استخراج کلید KDF در سطح امنیتی AS (که شامل کلیدهای K_{RRCenc} ، K_{RRCint} و K_{UPenc} است) باید امکان پیاده‌سازی این تغییرات هم در سمت eNBها و هم در سمت UE وجود داشته باشد.

در جدول (۱) تاثیر هر تغییری در بخش‌ها و پروتکل‌های مختلف سامانه EPS که در ستون سمت چپ جدول آمده است بر سایر بخش‌های سامانه با رنگ سیاه نشان داده شده است.

۸- منابع

[1] M. Saberi, B. Madadi, and S. M. Pournaghi, "LTE NETWORK SECURITY," ISBN 978-600-124-474-2, 2015.

[2] K. Farooq, "LTE for 4G Mobile Broadband, Air Interface Technologies and Performance," Cambridge University Press, 2009.

[3] S. S. Dhruv, "A tutorial on lte evolved utran (eutran) an lte self organizing networks," the university of texas at arlington, December 2010.

[4] F. Dan, H. Gunther, M. Wolf-Dietrich, and N. Valtteri, "LTE SECURITY", John Wiley and Sons Ltd, ISBN 978-1-118-35558-9 © 2013, 2013.

[5] C. Jin, M. H. L. Maode, and Z. Yueyu, "A Survey on Security Aspects for LTE and LTE-A Networks," IEEE Communications Surveys & tutorials, accepted for publication.

[6] M. Al-Humaigani, D. Dunn, and D. Brown, "Security Transition Roadmap to 4G and Future Generations Wireless Networks," Proc. 41st.

[7] "Southeastern Symposium on System Theory," (SSST 2009), March 2009, pp. 94-97, 2009.

[8] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing Securityin 4G Systems: Unveiling the Challenges," Proc. Sixth Advanced International Conference on Telecommunications (AICT), pp. 439-444, May 2010.

[9] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," Proc. IEEE Globecom Workshops, pp. 1-6, Nov. 2007.

[10] "3rd Generation Partnership Project," Technical Specification Group Services and System Aspects, Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution, (SAE), (Rel 9), 3GPP TR 33.821 V9.0.0, June 2009.

[11] D. Forsberg, "LTE Key Management Analysis with Session Keys Context," Computer Communications, vol. 33, no. 16, pp. 1907-1915, Octomber 2010.

[12] D. Forsberg, L. Huang, K. Tsuyoshi, and S. Alanara, "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface," Proc. Personal, Indoor and Mobile Radio Communications (PIMRC), pp. 1-5, Septmber 2007.

[13] T. Ahmed, D. Barankanira, S. Antoine, X. Huang, and H. Duvocelle, "Inter-system Mobility in Evolved Packet System (EPS): Connecting Non-3GPP Accesses," Proc. Intelligence in Next Generation Networks (ICIN), pp. 1-6, Oct. 2010.

[14] D. Yu and W. Wen, "Non-access-stratum Request Attack in E-UTRAN," Proc. Computing, Communications and Applications Conference (Com-ComAp), pp. 48-53, January 2012.

[15] M. Purkhiabani and A. Salahi, "Enhanced Authentication and Key Agreement Procedure of Next Generation Evolved Mobile Networks," Proc IEEE 3rd International Conference on Communication Software and Networks (ICCSN), pp. 557-563, May 2011.

[16] G. M. Koien, "Mutual Entity Authentication for LTE," Proc 7th International Wireless Communications and Mobile, Computing Conference (IWCMC), p. 689, July 2011.