مروری بر جنبه های امنیت برای شبکه‌های LTE و LTE-A

حمیدرضا دامغانی [۱] ، هلیا سادات حسینیان [۲]

[۱] دانشجوی دکتری مهندسی برق- مخابرات، دانشکده مهندسی برق و کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران

[۱] مرکز تحقیقات و مجموعه آزمایشگاه‌های همکار استاندارد شرکت صنایع گلدیران، تهران، ایران

H.damghani@goldiran.ir

[۲] کارشناس ارشد مهندسی برق قدرت - مدیریت انرژی، دانشکده مهندسی برق، دانشگاه صنعتی امیرکبیر، تهران، ایران

[۲] مرکز تحقیقات و مجموعه آزمایشگاه‌های همکار استاندارد شرکت صنایع گلدیران، تهران، ایران

H.hosseinian@goldiran.ir

چکیده

نیاز روز افزودن به مخابرات بی‌سیم موبایل پهن باند و ظهور کاربردهای بی‌سیم جدید، محرکی برای توسعه فن‌آوری‌های دسترسی بی‌سیم پهن باند، در سال‌های اخیر شده است. از آنجا که استفاده از محتوای تلویزیونی از جمله صدا و ویدئو، بر روی گیرنده‌های موبایل نظیر گوشی‌ها و تلویزیون‌های هوشمند و تبلت‌ها و نیز ترجیح به خصوصی‌سازی و قابل‌حمل‌شدن رسانه مشاهده می‌شود، لذا سیستم تکامل دراز مدت/تکامل معماری سیستم (LTE[۱]/SAE[۲]) توسط پروژهٔ همکاریِ نسل سوم (3GPP[۳]) برای حصول شبکه‌های موبایل نسل چهارم (4G[۴]) تعریف شده تا تضمین شود که 3GPP نفوذ و اهمیتِ فن‌آوری-های ارتباط سلولی را حفظ می‌کند. 3GPP، بواسطهٔ طراحی و بهینه سازیِ تکنیک‌های دسترسی رادیویی و تکاملِ سیستم-های LTE، شبکه‌های بی‌سیم و پیشرفته نسل آینده LTE (LTE-A[۵]) را به عنوان استانداردِ 4G ی 3GPP توسعه می دهد. از آنجایی که معماریِ 3GPP LTE و LTE-A، برای پشتیبانی از اتصال ساده با پروتکل اینترنت (IP[۶]) و شبکه‌بندی کامل با چندین شبکه دسترسی بی‌سیم، طراحی شده‌اند، این خصوصیات منحصربفرد جدید، چالش‌هایی جدید در طراحیِ مکانیزم های امنیت ایجاد می‌کنند. در گیرنده‌های تلویزیونی متصل به شبکه، تنها مشترکین و مخاطبین نیستند که درحال تماشای محتوا هستند، بلکه برای مثال تلویزیون هم در حال تماشای میلیون‌ها مخاطبی که در مقابلش قراردارند، است و این خود هزینه‌های گزاف افکارسنجی را کاهش می‌دهد. همین که هر مخاطب چه میزان زمان در حال مشاهده برنامه خاصی است تعین کننده میزان علاقه مخاطبان به آن برنامه است. این مقاله، جنبه‌های امنیتیِ شبکه LTE و LTE-A را ارائه می‌کند.

کلمات کلیدی: امنیت LTE، LTE-A، امنیت IMS[۷]، امنیت HeNB[۸]، امنیت MTC[۹]

۱- مقدمه

۱ Long-Term Evolution (LTE)
۲ System Architecture Evolution
۳ 3rd Generation Partnership Project
۴ Fourth generation of mobile telecommunications
۵ LTE Advanced
۶ Internet Protocol
۷ IP Multimedia Subsystem
۸ Home eNodeB
۹ Machine-Type Communications

با

توسعه سریعِ کاربردهای ارتباط بی‌سیم و چندرسانه‌ای همچون مرور وب، بازی‌های تعاملی، تلویزیون موبایل، و پخش مستقیم ویدئو و صدا، نیاز به رفع الزامات مختلف داده‌ها و عملکردهای چندرسانه‌ای موبایل دارند. با توجه به فراگیرترشدن روزافزون استفاده از تلفن‌های همراه با قابلیت پخش رسانه و این نکته که رسانه به سمت خصوصی‌شدن و قابل‌حمل‌شدن پیش می‌رود، و با افزایش توجه به دستگاه‌های همراه در استفاده از رسانه، سهمی که تلویزیون سنتی از مصرف رسانه داشته رو به کاهش است. از دلایل عمده‌ی این موضوع می‌توان به دو مورد عمومی بودن تلوزیون در مقابل فردی بودن دستگاه‌های همراه و همچنین قابلیت حمل و نقل و کاربرد این دستگاه‌ها در مکان‌های غیر ثابت و در حال حرکت مانند اتوبوس و مترو اشاره نمود. در نتیجه به طور کلی ارسال رسانه بر روی دستگاه تلفن همراه در دنیا از اهمیت خاصی برخوردار بوده و در تجارت توجه خاصی به خود جلب نموده است. به طوریکه همه‌ی تامین‌کنندگان بزرگ محتوا[۱۰] در دنیا به آن توجه نموده و توزیع‌کنندگان محتوا [۱۱] این موضوع را در برنامه‌ی اصلی خود قرار داده‌اند.در این راهکارهای مبتنی بر LTE و LTE-A،تلویزیون و رادیوی زنده با امکانات ساعت زمان و همچنین سرویس‌هایی از قبیل ویدیوی درخواستی (VOD[۱۲]) و موسیقی درخواستی (AOD[۱۳]) بر روی موبایل در اختیار اپراتورهای ۴G و LTE قرار می‌گیرد. کاربران این سیستم از تمامی امکانات یک سیستم تلویزیون تعاملی مانند سرتیتر اخبار، آب و هوا، خدمات ارزش‌افزوده مانند خرید خدمات خرد، رزرو تاکسی از طریق تلویزیون، یا خرید تلویزیونی، رستوران تلویزیونی و... استفاده می‌نمایند. با فراگیرشدن نسل‌های جدید فناوری‌هایی نظیر LTE و LTE-A در هر کجا و در هر زمانی مخاطب می‌تواند برنامه مورد نظر خود را دنبال نماید. موبایل‌های هوشمند و تبلت‌ها این امکان را بوجود آوردهحاند که افراد بتوانند از طریق این فناوری ها در هر کجا حتی اگر نتوانسته باشند برنامه مورد علاقه‌شان را در وقت مقرر خود ببینند، در یک حالتی که آمادگی برای دیدنش وجود داشته باشد، ببینند. این فناوری‌ها استانداردی جهت انتقال داده-هایی نظیر صدا و ویدئو در برودکست پرسرعت بی سیم برای تلویزیون‌ها و موبایل‌های هوشمند است.

برای تطبیق استفاده فزاینده از داده‌های موبایل و کاربردهای چندرسانه‌ایِ جدید، LTE و LTE-A توسط 3GPP به عنوان فن‌آوری‌های نوظهور برای ارتباط موبایل برای شبکه‌های بی سیم پهن باند نسل بعدی، تعریف شده‌اند. سیستم LTE طوری طراحی شده که مبتنی بر بسته و دارای عناصر کم شبکه باشد تا ظرفیت سیستم و پوشش آن بهبود یابد و عملکرد بهتری را از لحاظ نرخ داده بالا، نهفتگی پایین در دسترسی، عملکرد انعطاف‌پذیرِ پهنای باند و یکپارچگی کامل با دیگر سیستم-های ارتباطی بی سیم موجود فراهم کند. بدلیل مطرح شدن خصوصیات جدید، با چالش‌های امنیتی جدیدی در طراحی امنیتیِ سیستم‌های LTE و LTE-A روبرو هستیم.

از آنجایی که آسیب‌پذیری های امنیتی بسیاری در مکانیزم امنیتِ سیستم جهانی ارتباط از راه دور سیار (UMTS[۱۴])، همچون حملات مرد میانی(MitM[۱۵]) ، حمله به ایستگاه‌های مبنا و حملات رد سرویس (DoS[۱۶]) وجود دارد، سیستم‌های نسل بعدیِ ارتباطات موبایل، بایستی کاربردهای امنیتی بیشتری نسبت به سیستم‌های UMTS فراهم آورند. علاوه بر حفظ امنیت در سیستم‌های LTE، سیستم LTE-A چندین بخش و کاربرد جدید همچون ارتباط ماشینی (MTC)، HeNB، گره‌های واسط انتشاری را مطرح کرده است و آسیب‌پذیری های امنیتیِ مربوطه، الزامات و راهکارها را مشخص نموده است. در این مقاله، مروری برروی جنبه‌های امنیت در شبکه‌های LTE/LTE-A ارائه می‌کنیم. که شامل موارد ذیل است:

۱- مروری بر معماری‌ها و کارکردهای امنیت در شبکه‌های LTE/LTE-A،
۲- تجزیه و تحلیلِ آسیب‌پذیری‌های امنیتی در شبکه‌های LTE و امنیت در شبکه‌های LTE-A،
۳- بحث پیرامون راهکارهای موجود برای رفع آسیب‌پذیری‌ها و

۱۰ Content Provider
۱۱ Content Distributor
۱۲ Video on demand
۱۳ Audio on Demand
۱۰ Universal Mobile Telecommunications Service
۱۱ Man-in-the-middle
۱۲ Deny-of-service

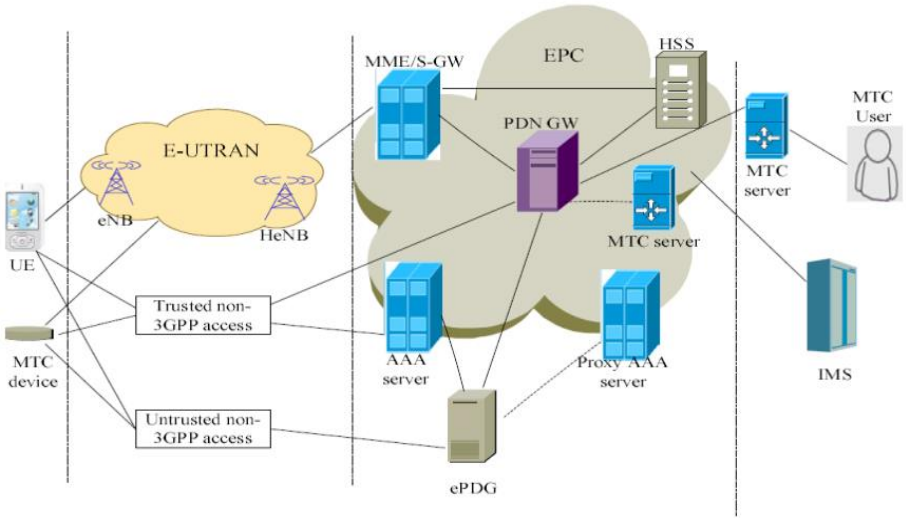
۴- نتیجه-

گیری و کشف حوزه‌ها و مسیرهای بالقوه پژوهشی برای تلاش‌های تحقیقاتی آینده [۱].

۲- مروری بر معماری امنیت

۲-۱- معماری شبکه LTE

همانطورکه در شکل (۱) آورده شده، یک شبکه LTE از هسته بسته تکامل یافته (EPC[۱۷]) و E-UTRAN[۱۸] تشکیل شده است. EPC، یک شبکه تماماً IP محور و یک شبکه چرخشی با بسته سوییچ شده (PS[۱۹]) در سیستم های LTE می‌باشد. سرویس صوتی، که یک سرویس شبکه با مدار سوییچ شده (CS[۲۰]) است، توسط شبکه زیر سیستم چندرسانه-ای IP (IP IMS) بکاربرده خواهد شد. EPC شامل یک MME[۲۱] و یک درگاه سروینگ (SGW[۲۲]) ، درگاه شبکه داده‌های بسته‌ای (PDN[۲۳] GW) همراه با سرور مشترک خانگی (HSS[۲۴]) می باشد. زمانیکه UE[۲۵] به EPC وصل می‌شود، MME به EPC می‌فهماند که باید اعتبارسنجی متقابل را با UE انجام دهد. E-UTRAN، شامل ایستگاه‌های مبنای شبکه جهانی دسترسی رادیویی زمینی به نام eNodeB ها می‌باشد که با UE ها ارتباط برقرار می‌کند[۱].



شکل ۱- معماری شبکه LTE [۱]

۲-۲- معماری امنیت LTE

پنج سطح امنیت وجود دارد که بصورت زیر تعریف می‌شوند:

۱- امنیت شبکه دسترسی: مجموعه مشخصه‌های امنیت همچون حفظ یکپارچگی و سری‌سازی میان USIM[۲۶]، تجهیزات کاربری (ME)، E-UTRAN، و اجزای EPC.

۲- امنیت حوزه شبکه: مجموعه مشخصه‌های امنیت که با حملات در شبکه‌های خط سیمی (wire line)، مقابله می-کند و گره‌ها را قادر به تبادل داده‌های سیگنال‌دهی و کاربری در حالتی امن می‌کند.

---

۱۳ Evolved Packet Core
۱۴ Evolved Universal Terrestrial Radio Access Network
۱۵ Packet switched
۱۶ Circuit switched
۱۷ Mobility Management Entity
۱۸ Serving gateway
۱۹ Packet Data Network
۲۰ Home Subscriber Server
۲۱ User equipment
۲۲ Universal subscriber identity module

۳- امنیت
حوزه کاربر: مجموعه مشخصه‌های امنیت که اعتبارسنجی متقابل میانِ USIM و ME را پیش از دسترسیِ USIM به ME فراهم می‌کند.
۴- امنیت حوزه کاربرد: مجموعه مشخصه‌های امنیت که کاربردها را در UE و در حوزه سرویس‌دهنده قادر به تبادل امن پیام‌ها می‌کند.
۵- امنیت در حوزه غیر 3GPP: مجموعه مشخصه‌های امنیت که UE ها را قادر به دسترسی امن به EPC توسط شبکه‌های دسترسیِ غیر 3GP می‌کند و حفاظت امنیتی را در لینک دسترسی رادیویی فراهم می‌کند [۲].

۳- خصوصیات و مکانیزم های امنیت LTE

براساس پیشرفت‌های پژوهشی دربارهٔ مشخصه‌های امنیت در LTE/LTE-A، برای امنیت در LTE، بر روی پنج جنبه زیر تمرکز خواهیم داشت:
۱- امنیت سلولی LTE؛
۲- امنیت در تعویض یا هندآور LTE؛
۳- امنیت IMS؛
۴- امنیت HeNB؛
۵- امنیت MTC [۳].

۳-۱- امنیت در سیستم سلولی LTE

اعتبارسنجی متقابل میان UE و EPC مهم‌ترین مشخصه امنیت در چهارچوب امنیتی LTE می باشد. سیستم LTE از روش AKA[۲۷] برای حصول اعتبارسنجی متقابل میان UE و EPC و ایجاد کلید سری‌سازی (CK[۲۸]) و یک کلید یکپارچه‌سازی (IK[۲۹])- که برای بدست‌آوردن کلیدهای مختلف اتصال برای رمزگذاری و حفظ هویت مورد استفاده قرار می-گیرند- استفاده می‌کند. بعلت پشتیبانی از دسترسی غیر 3GPP، چندین روش مختلف AKA در معماری امنیت LTE، زمان دسترسیِ UEها به EPC توسط شبکه‌های دسترسی مجزا، اجرا شده اند. شبکه‌های دسترسی معتبر غیر 3GPP، را می توان در UE از قبل پیکربندی نمود. اگر هیچ اطلاعاتِ از پیش پیکربندی نشده‌ای در UE وجود نداشته باشد، UE، باید شبکه دسترسی غیر 3GPP را نامعتبر (untrusted) فرض کند. برای یک شبکه دسترسی معتبر غیر 3GPP، UE و سرور AAA، پروتکل اعتبارسنجی تعمیم پذیر (EAP[۳۰]-AKA) یا EAP-AKA ی پیشرفته را برای انجام اعتبارسنجیِ دسترسی اجرا خواهد نمود [۳]،[۴]،[۵].

۳-۲- امنیت در فرایند تعویض (هندآور)

خصوصیات و رویه‌های امنیت برای تحرک در E-UTRAN و نیز بین E-UTRAN و شبکه دسترسی رادیویی زمینی UMTS[۳۱] (UTRAN) / شبکه دسترسی رادیویی GSM EDGE[۳۲] (GERAN) / شبکه دسترسی غیر 3GPP وجود دارد که در زیر دسته‌بندی شده است.
۱- تحرک در داخل E-UTRAN
۲- تحرک بین E-UTRAN و UTRAN/GERAN

۲۳ Authentication and Key Agreement
۲۴ Ciphering key
۲۵ Integrity Key
۲۶ Extensible Authentication Protocol
۲۷ Universal Mobile Telecommunications Service
۲۸ Enhanced Data rates for GSM Evolution

۳- تحرک بین E-UTRAN و شبکه‌های دسترسیِ غیر 3GPP [۱]،[۶].

۳-۳- امنیت در IMS

شبکه‌های LTE/LTE-A در حال رشد و تکامل به سوی شبکه‌های all-IP و کاملاً PS هستند. IMS، که یک معماری کنترل سرویس مبتنی بر IP و مستقل از دسترسی است، توسط 3GPP ایجاد شده است. IMS، یک معماری جایگشتی است که سرویس‌های چندرسانه‌ای همچون Voice over IP (VoIP)، کنفرانس ویدئویی و غیره را برای شبکه-های LTE/LTE-A فراهم می‌کند. برای دسترسی به سرویس‌های چندرسانه‌ای، UE، نیاز به یک ماژول هویت مشترکین جدید IMS (ISIM) دارد که در کارت مدار مجتمع فراگیر (UICC[۳۳]) قرار داشته باشد [۱]،[۳].

۴-۳- امنیت در HeNB

HeNB، که نوعاً در منزل یا ادارات کوچک برای افزایش پوشش داخلی برای سرویس داده‌های صوتی و داده‌های پرسرعت توسط مشترک نصب می‌شود. HeNB دستگاهی جذاب نزد اپراتورها برای تامین سرویس های انبوه با مزایای هزینه کم و کیفیت سرویس بالا، می‌باشد. سه نوع دسترسی برای HeNB وجود دارد، که عبارتند از دسترسی بسته، دسترسی ترکیبی، و دسترسی باز. HeNB نیازمند پیکربندی و مجاز شناخته شدن توسط عملکرد، مدیریت و نگهداری می‌باشد. زمانیکه UE بخواهد توسط HeNB به شبکه دسترسی پیدا کند، MME نخست بررسی می‌کند که براساس فهرست گروه مجاز و بستهٔ مشترکین، آیا UE مجاز به دسترسی به HeNB ی موردنظر می‌باشد یا خیر. سپس، یک اعتبارسنجی دسترسی امن بین UE و MME توسط EPS AKA انجام خواهد شد [۱]،[۳].

۵-۳- امنیت در MTC

MTC، یا (M2M[۳۴]) ، به عنوان یکی از تکنیک‌های پیشرفته، برای ارتباطات بی‌سیم آینده، مورد ملاحظه قرار می-گیرد. متفاوت با ارتباطات انسان با انسان (H2H[۳۵]) که توسط شبکه‌های بی سیم فعلی طراحی‌شده، MTC به عنوان شکلی از مخابرات داده بین اجزایی تعریف می‌شود که لزوماً نیاز به مداخله انسان ندارد. و عمدتاً برای جمع‌آوری و تحویل خودکار اطلاعاتِ اندازه‌گیری مورد استفاده قرار می‌گیرد.که به ۳ نوع امنیت تفکیک می‌شود.

الف) امنیت برای MTC بین دستگاه MTC و شبکه 3GPP،

ب) امنیت برای MTC بین شبکه 3GPP و سرور MTC / کاربر MTC،

ج) امنیت برای MTC بین سرور MTC / کاربر MTC [۱]،[۷].

۴- آسیب پذیری های موجود در چهارچوب امنیت LTE

در این بخش، ضعف‌های موجود در چهارچوب امنیتِ LTE را خصوصاً در لایه MAC[۳۶] شرح می‌دهیم.

۱-۴- آسیب پذیری و ضعفِ معماری سیستم LTE

خصوصیات منحصربفردِ شبکه‌های LTE، چالش هایی جدید در طراحیِ مکانیزم‌های امنیت ایجاد می‌کند.

۱-۱-۴- معماری ساده مبتنی بر IP در شبکه‌های 3GPP LTE، منجر به ریسک‌های بیشتری در امنیت، همچون ضعف در برابر تزریق (جادهی)، اصلاح، حملات شنودی و ریسک‌های حریم شخصی بیشتری نسبت به شبکه‌های

۲۹ Universal integrated circuit card
۳۰ Machine to Machine
۳۱ Human to Human
۳۲ Media Access Control

GSM و UMTS می شود. دریافته شده که معماری LTE، دارای آسیب‌پذیری بیشتری در برابر حملات معمول در اینترنت، همچون آدرس IP ی تقلبی، حملات DoS، ویروس‌ها، کرم‌ها، و غیره می‌باشد.

۴-۱-۲- زمانی که حمله‌کننده یک ایستگاه مبنا را بخطر می‌اندازد، می‌تواند به دلیل ماهیتِ all-IP ی شبکه‌های LTE، کل شبکه را درمعرض خطر قراردهد. همچنین، بدلیل مطرح شدنِ ایستگاه‌های مبنای کوچک و کم‌هزینه، یعنی HeNB ها حمله‌کننده می‌تواند نسخه جعلی خود را که به کارکرد یک ایستگاه مبنا و کاربر بطور همزمان مجهز می‌باشد، ایجادکند. با استفاده از یک ایستگاه مبنای جعلی، وی می‌تواند آن را به عنوان یک ایستگاه مبنای اصلی یا حقیقی جا بزند تا کاربر را فریب دهد.

۴-۱-۳- معماری LTE ممکن است موجب مشکلات جدیدی در روند اعتبارسنجی تعویض یا هندآور گردد. از آنجایی که تعداد اندکی از سیستم‌های دسترسیِ ناهمگون می‌تواند در شبکه های LTE با هم موجود باشند، تهدیدات بیشتری برای امنیت شبکه ایجاد می‌کند، خصوصاً زمانیکه تحرک میان سیستم‌های ناهمگون دسترسی مورد پشتیبانی قرار گرفته باشد [۱].

۴-۲- آسیب پذیری های موجود در روند دسترسیِ LTE

EPS AKA، دارای اصلاحاتی درمقایسه با UMTS AKA است بطوری که می‌تواند از برخی حملات همچون حملات تعیین مسیر (هدایت پیام به مقصدی دیگر) ، حمله به ایستگاه‌های مبنا، و حملات MitM جلوگیری کند. هرچند، هنوز ضعف هایی در مکانیزم کنونی امنیت در دسترسی LTE به شرح ذیل وجود دارد:

۱- طرح EPS AKA، فاقد حفاظت از حریم شخصی می‌باشد. موارد بسیاری موجود است که منجر به افشای IMSI[۳۳] شده‌اند. زمانیکه IMSI به دست می‌آید، حمله‌کننده می‌تواند اطلاعاتِ مشترکین، اطلاعات موقعیتی، و حتی اطلاعات مکالمات را بدست آورد.

۲- طرح EPS AKA، نمی‌تواند جلوی حملات DoS را بگیرد.

۳- مشابه به UMTS AKA، در EPS-AKA ، یک مجموعه از حامل‌های اعتبارسنجی موجب مصرف پهنای باند و سربارِ سیگنال‌دهی اعتبارسنجی و مصرف حافظه ذخیره‌سازی می‌گردند.

۴- با افزایش تعداد شرکای رومینگ و مطرح‌شدن دیگر سیستم‌های دسترسی، مفروضات اصلیِ قابلیت اطمینان، میان شبکه‌های نامتجانس، منسوخ بنظر می‌رسد.

۵- زمانی که یک UE توسط یک شبکه دسترسی متعبر غیر 3GPP به یک EPC دسترسی پیدا می‌کند، معماری LTE از EAP-AKA یا ’EAP-AKA برای تامین اعتبارسنجی دسترسی امن مجدداً استفاده می‌کند. پروتکل EAP-AKA دارای نواقصی همچون افشای هویت کاربر، آسیب‌پذیری در برابر حملات MitM، فقدان همگام‌سازیِ شماره ترتیب (SQN[۳۴])، و مصرف زیاد پهنای باند می‌باشد [۱]،[۴]،[۵].

۴-۳- آسیب پذیری موجود در شیوه تعویض کانالLTE

برای کاهش تهدیدات امنیتی، مکانیزم امنیت LTE یک طرح جدید برای مدیریت کلید تعویض فراهم می‌کند تا کلیات و مقتضیات کلید را بین UE و eNB حین انتقال UE از یک eNB به دیگری، بهنگام‌سازی کند. که شامل آسیب-های ذیل است:

۱- فقدان امنیت پس‌گشتی (backward security)

۲- آسیب‌پذیری در برابر حملات ناهمگام‌سازی (de-synchronization)

۳- آسیب‌پذیری در برابر حملات خواندن مجدد داده (Replay) [۱].

---

۳۳ International Mobile Subscriber Identity
۳۴ Sequence number

۴-۴- آسیب پذیری ها و ضعف های موجود در مکانیزم امنیت IMS

IMS، بدلیل اتصال مستقیم به اینترنت، در معرض چندین نوع حمله می‌باشد. کمیته 3GPP، از طرح IMS AKA برای تضمین امنیت IMS استفاده کرده است که البته دچار ضعف‌هایی به شرح ذیل می‌باشد.

۱- روند اعتبارسنجی در IMS، مصرف انرژی UE و پیچیدگی سیستم را افزایش داده است.
۲- IMS AKA براساس طرح EAP AKA کار می‌کند. از اینرو، مشابه EAP AKA، دارای و ضعف‌هایی همچون آسیب‌پذیری در برابر حملات MitM، فقدان همگام سازیِ SQN، و مصرف پهنای باند بسیار زیاد می‌باشد.
۳- مکانیزم امنیت IMS در برابر چندین نوع حمله DoS آسیب پذیر می‌باشد [۱].

۴-۵- آسیب پذیری های موجود در مکانیزم امنیت HeNB

تهدیدات پیشِ روی HeNB ها و الزاماتِ امنیت HeNB مطابق ذیل می‌باشد.

۱- فقدان اعتبارسنجی متقابل میان UE و HeNB. مکانیزم امنیت کنونی HeNB، نمی‌تواند از حملات پروتکلی مختلفی همچون حملات شنود، حملات MitM، حملات تغییرچهره یا جعل هویت (masquerading)، و کشفِ فهرست دسترسی مشترکین جلوگیری کند.
۲- آسیب پذیری در برابر حملات DoS [۱].

۴-۶- ضعف ها در معماری امنیتMTC

دستگاه‌های MTC در برابر برخی حملات همچون حملات فیزیکی، افشای اعتبارنامه‌ها، حملات پروتکلی و حمله به شبکه مرکزی بسیار آسیب‌پذیر می‌باشند زیرا نیاز است که دستگاه‌های MTC نوعاً دارای قابلیت‌ها و امکانات کمی از لحاظ منابع انرژی و محاسباتی باشند. اعتبارسنجی همزمانِ گروه زیادی از دستگاه های MTC می‌تواند زمانی که بطور همزمان درخواست دسترسی به شبکه می‌دهند، موجب سربار در سیگنال‌دهی بین HSS و MME می‌شود [۱].

۵- راهکارهایی برای حل مسائل امنیتی مربوطه

در این بخش، مروری بر راهکارهای موجود برای رفع آسیب‌پذیری‌های مذکور خواهیم داشت.

۵-۱- معماری سیستمLTE

در معماری سیستم LTE، یک طرح جدید، ساده و قدرتمند برای اعتبارسنجی تعویض، براساس امضای پروکسیِ پیشرفته (improved proxy signature) که برای تمامی زمینه‌های تحرک همچون تعویض یا هندآور بین HeNB ها، تعویض بین eNBها و HeNBها، تعویض بین eNBها و تعویض میان MMEها، قابل بکارگیری است. با استفاده از این طرح، UEوeNB یا HeNBی موردنظر می توانند مستقیماً یک اعتبارسنجی متقابل را انجام دهند و یک کلید نشست (session key) را همراه با کلیدهای سرّیِ دراز مدت خود برقرار سازند. بنابراین، دارای فرایند اعتبارسنجی ساده‌ای بدون مدیریت پیچیده کلید می‌باشد و می‌تواند به بازدهی و بهره وری مطلوبی دست یابد [۱]،[۲]،[۵].

۵-۲- امنیت در سیستم سلولی LTE

موارد ذیل در بخش امنیت سلولی LTE قابل بیان است.

۱- در سیستم سلولی LTE، یک اعتبارسنجی ترکیبی، و یک تصدیق کلید و طرح اعتبارسنجی، براساس پلتفرم مدل اطمینان (TMP[۳۹]) و زیرساخت کلید عمومی (PKI[۴۰]) برای شبکه‌های موبایل 4G، مطرح شده است که می تواند استحکام قابل توجهی (قدرت پوشش حتی درصورت وجود خطاها) برای کاربران موبایل در دسترسی به سرویس‌های حساس و داده‌ها در سیستم‌های 4G را فراهم آورد.

۲- یک طرح اعتبارسنجی و تصدیق کلید، براساس کلید عمومی خودگواهی (self-certified) ، برای سیستم‌های بی-سیم 4G وجود دارد که یک پروتکل انتشار کلید عمومی را براساس روش احتمالاتی برای یک UE ایجاد می‌کند تا ایستگاه مبنای اصلی را شناسایی کند و از اینرو، نواقص و ضعف‌های طرح 3G AKA را رفع می‌کند.

۳- علاوه براین، سه پروتکل اعتبارسنجی، از قبیل اعتبارسنجی ثبتی، اعتبارسنجی مجدد، و اعتبارسنجی تعویض به ترتیب برای زمینه های مختلف اعتبارسنجی ارائه شده است که امنیتِ هویت کاربر و پیام تبادل شده را همراه با مصرف انرژی کم و با استفاده از رمزنگاری منحنی بیضوی (ECC[۴۱]) تضمین می کند [۱].

۵-۳- امنیت در تعویض یا هندآورLTE

برای انجام تعویض امن LTE، یک طرح ترکیبیِ اعتبارسنجی و تصدیق کلید مطرح شده تا از تحرک سرتاسری و ارتباطات امن در سیستم‌های بی سیم 4G پشتیبانی گردد. مثلا یک کلمه عبور پویا را با یک کلید عمومی همراه می‌سازد تا اعتبارسنجیِ سبک و سرویسی بدون قطع را فراهم سازد [۷].

۵-۴- امنیت IMS

دربارهٔ امنیت IMS، طرح‌های اعتبارسنجی، برای کاهش هزینه‌های سیگنال‌دهی پیشنهاد شده است که در زیر به آنها اشاره می‌شود.

۱- یک طرح برای اعتبارسنجی سرویس IMS، ارائه شده است که با استفاده از مفهومِ IBC[۴۲] و رمزنگاری منحنی بیضوی (ECC) اجازهٔ شخصی‌سازیِ سرویس‌های IMS را با اعتبارسنجی کاربران در حالتی شخصی درطول دسترسی به سرویس‌ها می‌دهد و حفاظت قدرتمندی از امنیت فراهم می‌کند.

۲- یک مکانیزم اصلاح شده اعتبارسنجی IMS برای شبکه‌های 3G-WLAN، با استفاده مجدد و موثر از کلید برای کاربر موبایل مطرح است که در آن بردارها یا حامل‌های اعتبارسنجی و کلیدهای رمزگذاریِ بدست‌آمده در روش اعتبارسنجی اولیه شبکه، با انتقال امن آنها با استفاده از HSS در اعتبارسنجی IMS آمده است [۱].

۵-۵- امنیت HeNB

برای سیستم های HeNB، مسائلِ اعتبارسنجی و کنترل دسترسیِ کاربران HeNB، بصورتیکه زمانی که یک UE می‌خواهد توسط HeNB به شبکه دسترسی پیداکند، CN، بطور تکمیلی مسئول انجام کنترل دسترسی برای UE می‌باشد. برای انجام کنترل دسترسی، CN باید فهرستی از اجزای CSG به نام‌های فهرست مجاز CSG را که UE برای آن سرویس می‌دهد، نگهداری و بروزرسانی‌کند. اطلاعات گنجانده شده در فهرست CSG مجاز UE، به صورت اطلاعات اشتراک، برای UE، در HSS ذخیره می‌شود و برای کنترل دسترسی، به MME ارائه می شود. پیش از اعتبارسنجی متقابل با UE، MME نیازمند بررسی این است که آیا UE، براساس فهرست مجاز CSG، مجاز به دسترسی به HeNB هست یا خیر. همچنین یک مکانیزم اعتبارسنجی متقابل و کنترل دسترسی جهت تضمین ارتباط امن برای HeNB، با استفاده از تنظیم یک امضای پروکسی، مطرح شده است. نهایتاً اعتبارسنجی متقابل بین UE و HeNB با امضای پروکسی به نیابت از OAM و

---

۳۵ Trust model platform
۳۶ Public key infrastructure
۳۷ Ellipse curve cipher
۳۸ Identity Based Cryptography

CN، قابل انجام است. این طرح می‌تواند از حملات
مختلف همچون جعل یک HeNB ی معتبر، حملاتِ MitM و حملات DoS جلوگیری کند [۱].

۵-۶- امنیت MTC

در راهکارهای مربوط به امنیت MTC، توصیه شده که متغیر قابلیت اطمینان (TrE[۴۳]) را می توان در دستگاه‌های MTC گنجاند تا از امنیت دستگاه‌های MTC محافظت شود، که این می‌تواند فعالیت‌های محفوظ‌تری برای اعتبارسنجی دسترسی فراهم‌کند و از برخی قابلیت‌های رمزنگاری همچون رمزگذاری و رمزگشایی متقارن و نامتقارن، پشتیبانی کند [۱].

۶- مسائل پژوهشی حل نشده

چند زمینهٔ پژوهشی دربارهٔ امنیت LTE به عنوان کارهای بالقوه آینده پیشنهاد می‌کنیم که به دو دسته کلی زیر قابل بیان است:

۱-۶- طراحی مکانیزم‌های امنیت MTC در شبکه‌های LTE/LTE-A، کار اصلیِ پژوهش‌های آینده برای امنیتLTE می‌باشد، شامل خصوصیات کشف نشدهٔ MTC که در ادامه به آن‌ها پرداخته می‌شود:

۱-۱-۶- مکانیزم‌های امنیت برای تضمین اتصال پرسرعت و متعبر برای داده‌های حساس ضروری هستند.

۲-۱-۶- نسبت سربار رمزگذاری و میزان اطلاعات ارسال شده باید درنظر گرفته شود. مطابق با امنیت کنونی در LTE، هم سیگنال‌دهی کنترل و هم بار مفید باید توسط عملیات‌های بررسی یکپارچگی و تمامیت، رمزگذاری شوند. از اینرو، شبکه های LTE نیازمند کاهش سربار در عملیات رمزنگاری هستند.

۳-۱-۶- به طرح‌های جدید دسترسی برای جلوگیری از تراکم در اعتبارسنجی همزمانِ چند دستگاه نیاز می‌باشد. زیرا در سیستم‌های 3GPP، باید از تعداد فراوانی از کاربردهای MTC بطور همزمان پشتیبانی شود.

۴-۱-۶- مکانیزم‌های امن انتها به انتها برای MTC لازم می‌باشند. از اینرو، شبکه‌های LTE نیازمند استقرار این مکانیزم‌های امن برای ارتباطات ماشین با ماشین بین دو دستگاه MTC هستند.

۵-۱-۶- به مکانیزم‌هایی ایمن برای پشتیبانی از تحرک محدود و پرسرعت دستگاه‌های MTC نیاز است و نیز مکانیزم حفاظت امن برای نظارت تغییرات موقعیتی دستگاه‌های MTC و جلوگیری از تحرک غیرمجازِ آنها در شبکه LTE باید طراحی گردد.

۲-۶- در رابطه با دیگر جوانب امنیت LTE، هنوز مسائل بسیاری از جمله موارد ذیل به بهبود و اصلاح نیاز دارند:

۱-۲-۶- در رابطه با معماری امنیت LTE، مکانیزم‌هایی باید برای حفظ ارتباط بین UE ها، eNB ها (HeNB) و EPC از حملات متداول پروتکلی و نفوذ فیزیکی به شبکه های LTE طراحی گردد.

۲-۲-۶- در رابطه با امنیت سلولی LTE، طرح EPS AKA در شبکه‌های LTE باید طوری ارتقا یابد تا قادر به جلوگیری از افشای هویت کاربر، حملات DoS و دیگرحملات، همراه با عملکرد بهتر در اعتبارسنجی باشد.

۳-۲-۶- در رابطه با امنیت تعویض در LTE، مکانیزم‌های مدیریت کلیدی و روش‌های اعتبارسنجی تعویض در شبکه‌های LTE باید بیشتر تصحیح شوند تا از برخی حملات پروتکلی نظیر حملات ناهمگام‌سازی و حملات پاسخ‌دهی جلوگیری‌کنند.

۳۹Trust environmental

۶-۲-۴- در رابطه با امنیت IMS، باید مکانیزم‌های سریع و قدرتمندی برای اعتبارسنجی دسترسیِ IMS طراحی گردد تا فرایند اعتبارسنجی را تسهیل کند و از حملات DoS و دیگر حملات در شبکه‌های LTE جلوگیری کند.

۶-۲-۵- در رابطه با امنیت HeNB، نیاز به طراحی مکانیزم‌هایی ساده و قدرتمند برای اعتبارسنجی متقابل بین UEها و HeNBها می باشد تا از حملات مختلف پروتکلی جلوگیری شود [۱]،[۲]،[۵].

۷- نتیجه گیری

دراین مقاله، مروری بر مسائل امنیتی در شبکه‌های بی سیم LTE/LTE-A 4G داشتیم. نخست معماری‌های امنیت و مکانیزم‌های تعیین شده با استاندارد 3GPP را ارائه کردیم و اهمیت این فناوری را در صنعت برودکست یادآور شدیم. آسیب‌پذیری‌ها و ضعف‌های موجود در معماری امنیتِ شبکه‌های بی‌سیم LTE/LTE-A را بررسی‌کردیم و مروری بر جدیدترین راهکارهای مطرح شده برای رفع این نواقص امنیت نمودیم. نهایتاً مسائل پژوهشی حل‌نشده بالقوه را به عنوان پیشنهادی برای فعالیت‌های پژوهشی آینده دربارهٔ امنیت در شبکه‌های بی سیم LTE/LTE-A بطور خلاصه بیان نمودیم.

تشکر و قدردانی

نویسندگان مقاله برخود لازم می‌دانند مراتب قدردانی و سپاسگزاری خود را از حمایت‌های شرکت صنایع گلدیران (جناب آقای مهندس علیرضا خزاعی و جناب آقای یانگ نام کیم) و شرکت ال جی الکترونیکس (دفتر ایران) بعمل آورند.

۸- مراجع

[1] Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo, “A Survey on Security Aspects for LTE and LTE-A Networks”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Vol. 16, NO.1, FIRST QUARTER 2014.

[2] Jin Wang, Zhongqi Zhang, Yongjun Ren, Jeong-Uk Kim, and Li Bin, “Issues toward Networks Architecture Security for LTE and LTE-A Networks”, International Journal of Security and Its Applications,Vol.8, NO.4, pp.17-24, 2014.

[3] Amruta Kokate, “A Survey on Different Security Solutions for Lte and Lte-A Networks”, INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH, Vol.4, Issue.12, pp.156-157, December 2015.

[4] Krishna Prakash, and Balachandra, “AUTHENTICATION AND KEY AGREEMENT IN 3GPP NETWORKS”, Computer Science & Information Technology (CS & IT), Vol.5, pp.143-154, 2015.

[5] Warda Ahmed, Sidra Anwar, and M. Junaid Arshad, “Security Architecture of 3GPP LTE and LTE-A Network: A Review”, INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING, Vol.7, NO.1, JANUARY 2016.

[6] Md Mehedi Masud, “Survey of security features in LTE Handover Technology”, Scientific Research Journal (SCIRJ), Vol.III, Issue.VIII, August 2015.

[7] Ali Saqib, Jianye Song, Alassane Coulibaly, and Mukhtar Abdirahman, “SEGHAS: A Secure & Efficient Group-Based Handover Authentication Scheme for Machine -to- Machine Communication in LTE-A Network”, American Journal of Engineering Research (AJER), Vol.6, Issue.2, pp-181-192, 2017.