امنیت دگرسپاری در شبکه‌های LTE

معصومه صفاخیل[1*] و علی پاینده[2]

[1] دانش‌آموخته کارشناسی ارشد مهندسی برق مخابرات، دانشگاه صنعتی مالک اشتر، تهران، ایران
m.safakheil87@gmail.com

[2] استاد، گروه مهندسی برق، دانشگاه صنعتی مالک اشتر، تهران، ایران
payandeh@mut.ac.ir

چکیده

سامانهٔ ارتباطی نسل چهارم مخابرات، مبتنی‌بر فناوری LTE است. LTE تکامل‌یافتهٔ شبکه‌های دسترسی بسته‌ای با سرعت بالا (HSPA) است و با تحقق نرخ داده بالاتر، سازگاری بیشتر با شبکه‌های ناهمگن و معماری شبکهٔ یک‌نواخت‌تر ارائه شده است. LTE از سری استانداردهای نسخهٔ ۸، 3GPP است. یکی از اهداف LTE و هر سامانهٔ بی‌سیمی، فراهم کردن دگرسپاری یک‌پارچه و سریع از یک سلول (سلول منبع) به سلول دیگر (سلول مقصد) است. با این‌که روندهای تعریف‌شدهٔ دگرسپاری LTE در نسخه ۸ با پشتیبانی از تحرک ارائه شده‌اند؛ اما برای تمام حالت‌های تحرک مناسب نیستند و حتی در مقایسه با سامانه‌های نسل ۲ و ۳، ممکن است موجب نارضایتی کاربر شوند. در این مقاله ابتدا معماری شبکه LTE و آسیب‌های موجود در آن مطرح شده است؛ سپس مفاهیم مرتبط با دگرسپاری در شبکه LTE و اقدامات اخیر در این حوزه بررسی شده است.

واژگان کلیدی: احراز اصالت، دگرسپاری سخت،دگرسپاری افقی، شبکه LTE

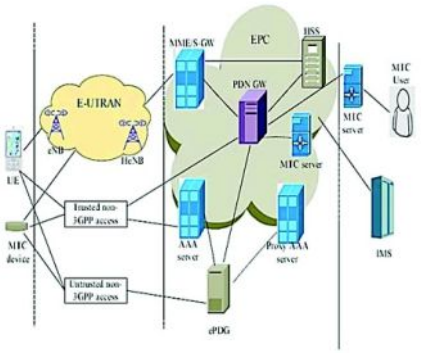
۱- معماری شبکه LTE

مطابق شکل (۱)، شبکهٔ LTE [1] از شبکهٔ مرکزی بسته‌ای تکامل‌یافتهٔ (EPC)[2] و شبکهٔ تکامل‌یافتهٔ دسترسی رادیویی زمینی UMTS[3] تشکیل شده است. EPC بسته‌ها را با استفاده از IP مسیردهی می‌کند و از دستگاه‌هایی که از IP نسخهٔ ۴، نسخهٔ ۶ و یا بستهٔ دوگانه IP نسخهٔ ۴ و ۶ استفاده می‌کنند، پشتیبانی می‌کند. همچنین وظیفهٔ برقراری ارتباط با شبکه‌های بیرونی داده مانند اینترنت، شبکهٔ اختصاصی سازمانی و یا زیرسامانهٔ چندرسانه‌ای IP[4] را بر عهده دارد[۱]. EPC شامل نهاد مدیریت تحرک (MME[5]) و درگاه خدمات (S-GW[6]) و درگاه شبکهٔ دادهٔ بسته‌ای(PDN GW[7]) به همراه سرور مشترکین خانگی(HSS[8]) است. MME کنترل عملکردهای سطح بالای موبایل را بر عهده دارد. یک شبکه ممکن است، دارای چندین MME باشد که هرکدام از آن‌ها منطقهٔ جغرافیایی خاصی را پوشش می‌دهد[۲].

هر موبایل به یک MME اختصاص داده می‌شود که این MME به‌عنوان MME خدمات‌دهنده برای تلفن همراه مذکور شناخته می‌شود. اگر تلفن همراه به اندازه قابل توجهی از MME دور شود، شبکه، تلفن همراه را به MME مناسب دیگری اختصاص می‌دهد. MME، همچنین وظیفه کنترل دیگر اجزای شبکه را از طریق پیام‌های سیگنالینگ بر عهده دارد.

[1] Long Term Evolution
[2] Evolved Packet Core
[3] E-UTRAN
[4] IP Multimedia Subsystem (IMS)
[5] Mobility Management Entity
[6] Serving Gateway
[7] Packet Data Network Gateway
[8] Home Subscriber System

* نویسندهٔ عهده‌دار مکاتبات



(شکل- ۱): معماری شبکه LTE [۲]

S-GW مانند یک مسیریاب عمل و داده‌ها را هنگام تحرک کاربر برای دگرسپاری میان eNodeBها و تحرک بین LTE و سایر فناوری‌های 3GPP جابجا می‌کند. یک شبکه به‌طورمعمول چندین S-GW دارد که هر کدام از آن‌ها در محدوده جغرافیایی خاصی از موبایل‌ها پشتیبانی می‌کند. هر موبایل به یک S-GW اختصاص داده می‌شود، اما درصورتی‌که موبایل به اندازهٔ معینی از S-GW خود فاصله بگیرد، به S-GW دیگری تحویل داده می‌شود.

PDN GW نقطهٔ اتصال EPC با جهان خارج است. هر موبایل به یک P-GW پیش‌فرض اختصاص داده می‌شود و از طریق آن ارتباط خود با شبکه داده بسته‌ای پیش‌فرض، به‌عنوان‌مثال اینترنت را برقرار می‌کند. پس از آن، درصورتی‌که موبایل بخواهد به شبکه‌های داده بسته‌ای دیگری، مانند شبکهٔ اختصاصی سازمانی خود متصل شود، به P-GW دیگری اختصاص داده می‌شود. هر P-GW در طول مدت برقراری اتصال داده، بازده عملیاتی یکسان دارد. HSS که پایگاه داده اصلی اطلاعات مشترکان شبکه است، یکی از معدود اجزای LTE است که از نسل‌های پیشین (GSM و UMTS) به LTE منتقل شده است. درون EPC، HSS و MME با استفاده از پروتکلی بر مبنای دیامیتر با یکدیگر ارتباط برقرار می‌کنند. پروتکل پایه‌ای دیامیتر یک پروتکل استاندارد IETF[1] برای احراز اصالت، اعطای صلاحیت[2] و محاسبه کارکرد[3] است که خود بر مبنای پروتکل قدیمی‌تر با نام RADIUS[4] است. هنگامی‌که UE[5] به EPC اتصال یابد، MME نشان می‌دهد که EPC احراز اصالت دوطرفه با UE را اجرا می‌کند.

[1] Internet Engineering Task Force
[2] Authorization
[3] Accounting
[4] Remote Authentication Dial In User Service
[5] User Equipment

E-UTRAN تنها شامل یک بخش است که eNB[6] نامیده می‌شود و با تجهیزات کاربر ارتباط برقرار می‌کند. هر eNB یک ایستگاه پایه است که موبایل‌های واقع در یک یا چند سلول[7] را کنترل می‌کند و هر سلول نیز اندازه محدودی دارد. اندازهٔ هر سلول برابر با حداکثر محدوده‌ای است که در آن یک گیرنده به‌طور موفق از فرستنده دریافت می‌کند. سلول همچنین دارای ظرفیتی محدود است که معادل مجموع حداکثر نرخ دادهٔ تمام موبایل‌ها در یک سلول است. این محدودیت‌ها باعث می‌شود که انواع مختلفی از سلول‌ها وجود داشته باشد. ماکروسل‌ها برای پوشش مناطق گسترده به‌کار می‌روند و به‌طورمعمول چندین کیلومتر را پوشش می‌دهند. میکروسل‌ها محدوده پوشش چند صد متری دارند و مناسب محیط‌های پرتجمع هستند. پیکوسل‌ها محدوده پوشش چند ده متری دارند و در محیط‌های داخلی وسیع مورد استفاده قرار می‌گیرند. فمتوسل‌ها برای مصارف خانگی مناسب و پوشش چند ده متری دارند. الگوریتم‌های تصمیم‌گیری در شبکه‌های فمتوسل در [۳] مورد بررسی قرار گرفته‌اند. در شکل (۲) مثالی از به‌کارگیری شبکه‌های فمتوسل به تصویر کشیده است. همچنین در [۴] روندهای دگرسپاری در شبکه‌های فمتوسل مبتنی‌بر LTE به تفضیل شرح داده شده است. در [۵] راه‌حلی برای دگرسپاری بین فمتوسل و ماکروسل در شبکهٔ LTE ارائه شده است.

در LTE، کنترل‌کنندهٔ شبکهٔ رادیویی (RNC[8]) از مسیر داده حذف و عملکردهای آن به eNB محول شده است. یک موبایل در هر لحظه تنها با یک سلول و یک ایستگاه پایه ارتباط برقرار می‌کند؛ بدین خاطر در LTE، دگرسپاری نرم[9] را نخواهیم داشت. ایستگاه پایه که در حال ارتباط با یک موبایل است، به‌عنوان eNB خدمات‌دهندهٔ آن موبایل یا eNB منبع شناخته می‌شود[۶].

eNB دو عملکرد اصلی دارد. نخست این‌که eNB وظیفه ارسال به تمام موبایل‌های تحت پوشش خود در پیوند فروسو و دریافت ارسال‌های آن‌ها در پیوند فراسو، با استفاده از عمل‌کردهای واسط هوایی LTE در زمینه پردازش سیگنال دیجیتال و آنالوگ را بر عهده دارد. دوم این‌که eNB تمام عمل‌کردهای سطح پایین موبایل‌های تحت پوشش خود را با ارسال پیام‌های سیگنالینگ به آن‌ها کنترل می‌کند. دستورهای مربوط به دگرسپاری، مثالی در این زمینه است.

[6] Evolved Node B
[7] Cell
[8] Radio Network Control
[9] Soft Handover/Macro-diversity

شکل ۲. مثالی از بکارگیری فمتوسل [۳]

در اجرای این عملکردها، eNB ترکیبی از عملکردهای Node B و RNC را استفاده می‌کند، تا هنگام مبادله اطلاعات بین موبایل و شبکه از تأخیر کاسته شود. در مقایسه با شبکه‌های 3G، شبکه‌های LTE/LTE-A نهادها و توابع دیگری را معرفی می‌کند.

۱- یک ایستگاه پایه جدید با نام HeNB[1] (eNB خانگی) توسط انجمن 3GPP برای بهبود پوشش داخلی و ظرفیت شبکه پیشنهاد شده است. ایستگاه پایه HeNB نقطه دسترسی[2] کم‌توانی دارد و به‌طور معمول توسط یک مشترک در محل اقامت و یا در یک دفتر کوچک جهت بهبود پوشش داخلی و ظرفیت شبکه نصب می‌شود و روی اینترنت از طریق باند پهن با EPC ارتباط برقرار می‌کند[۷]. یک eNB خانگی می‌تواند از طریق یک درگاه ایستگاه پایه خانگی که اطلاعات چندین eNB خانگی را جمع می‌کند، به EPC متصل شود.

۲- افزون‌بر E-UTRAN، سامانه LTE-A از ارتباط شبکه‌های دسترسی غیر 3GPP از قبیل WLAN[3]، سامانه‌های WiMAX و CDMA2000[4] با EPC پشتیبانی می‌کند. دو نوع شبکهٔ دسترسی غیر 3GPP، شبکهٔ دسترسی غیر 3GPP معتمد[5] و شبکهٔ دسترسی غیر 3GPP نامعتمد[6] وجود دارد[۸]. این‌که یک شبکهٔ دسترسی غیر3GPP مورد اطمینان است یا نه، از خواص شبکه‌های دسترسی نیست؛ بلکه به تصمیم اپراتورهای شبکه بستگی دارد. برای یک شبکه دسترسی غیر 3GPP نامعتمد، UE به گذر از درگاه داده بسته تکامل‌یافته (ePDG)[7] معتمد متصل به EPC نیاز دارد.

۳- سیستم LTE-A همچنین از نهادی به نام MTC[8]، که می‌تواند داده‌ها را بدون نیاز به هر نوع دخالت انسانی، مبادله و به اشتراک بگذارد، پشتیبانی می‌کند[۹].

۲- آسیب‌های معماری سیستم LTE

شبکه LTE با معماری یکنواخت مبتنی‌بر IP برای پشتیبانی از میان‌کاری[9] با شبکه‌های دسترسی رادیویی ناهمگن طراحی شده است. ویژگی‌های منحصربه‌فرد شبکه‌های LTE چالش‌های امنیتی جدیدی را در طراحی سازوکارهای امنیتی به ارمغان آورده است.

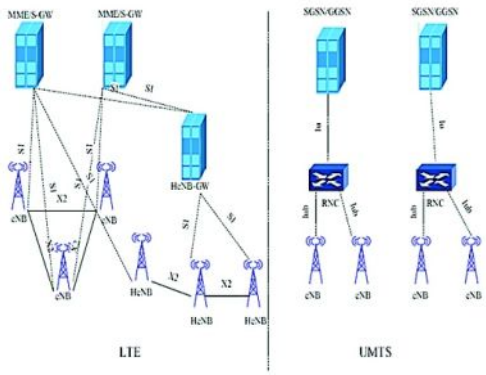
۱- معماری مبتنی بر IP شبکه‌های 3GPP LTE، نسبت به شبکه‌های GSM[10] UMTS، خطرات امنیتی بیشتری را از قبیل آسیب‌پذیری نسبت به افزایش درخواست دسترسی[11]، اصلاح[12]، حملات شنود[13]، حمله منع خدمات[14] و حریم خصوصی[15]، به همراه دارد.

۲- ضعف‌های دیگری نیز وجود دارد که از ایستگاه‌های پایه[16] موجود در سیستم‌های LTE ناشی می‌شود. شبکه تمام IP، امکان ایجاد یک مسیر مستقیم به ایستگاه‌های پایه را برای مهاجم فراهم می‌کند. همان‌طور که در (شکل (۳) نشان داده شده، از آن‌جاکه یک MME، eNBهای متعددی را در معماری LTE مدیریت می‌کند، ایستگاه‌های پایه در شبکه LTE در مقایسه با معماری UMTS، در برابر حملات مستعدتر هستند.

۳- هنگامی‌که مهاجمی یک ایستگاه پایه را به خطر می‌اندازد، با توجه به تمام IP بودن شبکه LTE، کل شبکه را به خطر می‌اندازد. به‌علاوه، با ارائهٔ ایستگاه‌های پایه کوچک و کم‌هزینه، HeNBs، مهاجم این امکان را دارد که نسخه تجهیز جعلی خود را ایجاد کند. درنتیجه با استفاده از یک ایستگاه پایهٔ جعلی، مهاجم می‌تواند برای جلب یک کاربر قانونی، خود را به‌عنوان پایگاه معتبر دیگری جا بزند. همچنین مهاجم می‌تواند یک کاربر قانونی را جعل تا با یک ایستگاه پایه معتبر ارتباط برقرار کند.

[1] Home eNB
[2] Access Point
[3] Wireless Local Area Networks
[4] Code Division Multiple Access
[5] Trusted non-3GPP Access Networks
[6] Untrusted non-3GPP Access Networks
[7] evolved Packet Data Gateway (ePDG)

[8] Machine-Type Communication
[9] Interworking
[10] Global System of Mobile Communication
[11] Injection
[12] Modification
[13] Eavesdropping Attacks
[14] Denial of Service (DoS)
[15] Privacy
[16] Base Station (BS)



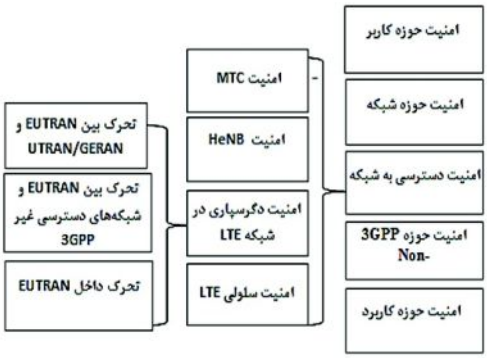
(شکل-۳): مقایسه معماری شبکه دسترسی LTE و UMTS[۲]

۴- معماری LTE مشکلات جدیدی را در روند احراز اصالت دگرسپاری درون شبکه‌ای و دگرسپاری با دیگر سیستم‌های غیر3GPP ایجاد می‌کند. همچنین 3GPPحالات متنوعی را برای تحرک میان HeNB و eNB پیشنهاد کرده است. اما روندهای احراز اصالت دگرسپاری مجزا در حالت‌های مختلف، از قبیل دگرسپاری بین eNBها، دگرسپاری بین HeNBها، دگرسپاری میان eNB و HeNB و دگرسپاری بین MMEها، هنگامی‌که ایستگاه‌های پایه توسط MMEهای متفاوتی مدیریت شوند، پیچیدگی کلی سیستم را افزایش می‌دهد.

۳- روش‌ها و ویژگی امنیتی LTE

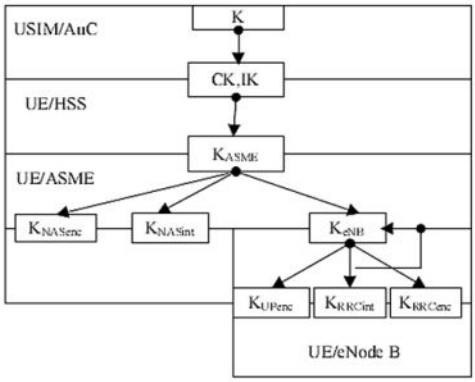
3GPP پنج سطح امنیتی را برای معماری LTE، مطابق شکل (۴) تعیین کرده است. امنیت دسترسی به شبکه روی پنج جنبه، (۱) امنیت سلولی LTE[1] (۲) امنیت دگرسپاری در شبکه LTE (۳) امنیت IMS[2] (۴) امنیتHeNB (۵) امنیتMTC[3]، متمرکز شده است. در اقدامات اخیر امنیت دگرسپاری در شبکه LTE بر حسب حالت‌های تحرک و معیارها و استانداردها بررسی شده است.

احراز اصالت دوطرفه بین UE و EPC از مهم‌ترین ویژگی‌های امنیتی در چارچوب امنیت شبکه LTE است. سیستم LTE از روند احراز اصالت و توافق کلید AKA برای دست‌یابی به احراز اصالت دوطرفه بین UE و EPC و تولید کلید رمزنگاری[4] و کلید تمامیت[5] که برای به‌دست‌آوردن کلید نشست استفاده می‌شوند تا تمامیت و محرمانگی حفظ شود، بهره می‌برد. برای پشتیبانی از دسترسی شبکه‌های غیر 3GPP، روندهای احراز اصالت و توافق کلید مختلفی در معماری امنیتی LTE بکار گرفته می‌شود.



(شکل- ۴): امنیت دسترسی به شبکه

هنگامی‌که UE با EPC از طریق E-UTRAN ارتباط برقرار می‌کند، MME نشان می‌دهد EPC احراز اصالت دوطرفه با UE را توسط پروتکل EPS AKA [۱۰] انجام می‌دهد. علاوه‌بر این، سلسله‌مراتب کلیدهای جدید برای حفاظت سیگنالینگ و ترافیک داده کاربر معرفی شده، که در شکل ۵ نشان داده شده است. K مقدار ویژه‌ای است که به‌صورت امن در HSS ذخیره شده و به‌صورت امن در کارت مدار مجتمع جهانی ذخیره شده است.



(شکل- ۵):. سلسله‌مراتب کلید برای شبکه 3GPP LTE [۲]

HSS و UICC از مقدار K، دو مقدار دیگر بدست می‌آورند، که CK و IK نام دارند؛ سپس از این دو مقدار کلید K_{ASME} به‌دست می‌آید. دو کلید $K_{NASence}$ و

[1] LTE cellular security
[2] IP Multimedia Subsystem
[3] Machine-Type Communication
[4] Ciphering key (CK)
[5] Integrity key (IK)

K_{NASint} برای حمایت از جامعیت در پیام‌های سیگنالینگ لایهٔ غیردسترسی (NAS) بین موبایل و MME به‌کار می‌روند و کلید K_{eNB} به ایستگاه پایه فرستاده می‌شود. موبایل و ایستگاه پایه نیز از این کلید سه کلید K_{UPenc}، K_{RRCenc}، K_{RRCint} را برای رمزنگاری داده، رمزنگاری سیگنالینگ RRC و حمایت از جامعیت پیام‌های سیگنالینگ RRC به‌دست می‌آورند [۲].

۴- انواع دگرسپاری در شبکه LTE

دگرسپاری عملی است که در آن یک پایانهٔ سیار (MT)[1] از یک سلول/ فناوری بی‌سیم به سلول/ فناوری دیگری انتقال یابد [۱۱]. دگرسپاری در شبکه‌های بی‌سیم سیار به پارامترها و عوامل مختلفی از قبیل حوزه‌های اجرایی[2]، تعداد اتصالات[3]، نوع شبکه‌ها، مجوز کنترل کاربر[4]، ضرورت و لزوم دگرسپاری و فرکانس کاری [5] بستگی دارد[۱۲]. در LTE سه نوع دگرسپاری داریم:

(۱) دگرسپاری درون LTE (دگرسپاری بین سلول‌های منبع و مقصد که بخشی از یک شبکه LTE یکسان هستند.)

(۲) دگرسپاری با دیگر شبکه‌های LTE (دگرسپاری به نهادهای موجود در شبکه LTE دیگر).

(۳) دگرسپاری بین فناوری‌های رادیویی متفاوت (دگرسپاری بین LTE و دیگر شبکه‌ها از قبیل WCDMA). به‌طور کلی، دگرسپاری در شبکه LTE بر حسب نوع شبکه به دو دسته طبقه‌بندی شده است[۲].

۴-۱- دگرسپاری افقی

دگرسپاری بین دو ایستگاه کاری (BS) موجود در یک سیستم، دگرسپاری افقی نامیده می‌شود. این نوع دگرسپاری به زیرشاخه‌های زیر دسته‌بندی می‌شود [۱۳]:

۱-دگرسپاری لایهٔ پیوند[6]

۲- دگرسپاری درون‌سامانه‌ای [7]

دگرسپاری افقی بین دو BS تحت یک اپراتور خارجی (FA)[8] به‌عنوان دگرسپاری لایهٔ پیوند شناخته می‌شود. مانند دگرسپاری بین eNBها و دگرسپاری بین HeNBها.

در دگرسپاری درون‌سامانه‌ای، دگرسپاری افقی بین دو BS که متعلق به دو اپراتور مختلف باشند و هر دو اپراتور به یک سیستم تعلق داشته باشند، اتفاق می‌افتد؛ از این‌رو درگاه اپراتور خارجی، یکسانی (GFA)[9] دارند[۱۳]. مانند دگرسپاری بین MMEها.

۴-۲- دگرسپاری عمودی (VHO)[10]

دگرسپاری عمودی به جابه‌جایی از یک فناوری به فناوری دیگر، با حفظ ارتباط اشاره دارد[۱۳]. با ارائه این نوع دگرسپاری، اپراتور می‌تواند دسترسی به شبکه خود را با استفاده از یک‌پارچه‌کردن دو یا بیش از دو فناوری متفاوت، گسترش دهد. درواقع سازوکار دگرسپاری عمودی اجازه می‌دهد یک دستگاه پایانه، شبکهٔ خود را بین انواع شبکه‌ها تغییر دهد و از این طریق درخواست کاربر را اجرا کند. مانند دگرسپاری بین شبکه‌های نسل ۳ و نسل ۴.

بر حسب نوع اتصالات دگرسپاری به دو نوع، سخت و نرم دسته‌بندی می‌شود. اما در LTE تنها دگرسپاری سخت را داریم و از این جهت یک‌پارچگی دگرسپاری در LTE بسیار مهم است.

۴-۳- دگرسپاری سخت[11]

در دگرسپاری سخت هم‌زمان با برقراری پیوند رادیویی به ایستگاه پایه جدید، پیوند رادیویی ایستگاه پایه قدیمی آزاد می‌شود. به عبارت دیگر، با دگرسپاری سخت، گرهٔ سیار تنها مجاز است با یک ایستگاه پایه در هر زمان ارتباط داشته باشد.

۵- امنیت در روند دگرسپاری LTE

مطابق شکل (۶) انجمن 3GPP ویژگی‌های امنیتی و روندهایی را برای تحرک درون EUTRAN و همچنین بین EUTRAN و شبکهٔ دسترسی رادیویی زمینی UMTS (UTRAN)/ شبکهٔ دسترسی رادیویی GSM EDGE (GERAN) / شبکه‌های دسترسی غیر 3GPP، [۱۴]- [۱۵] تعیین کرده است.

۱- تحرک داخل EUTRAN، [۱۶]. به‌منظور دست‌یابی به دگرسپاری امن درون EUTRAN، شبکه LTE روش

[1] Mobile Terminal
[2] Administrative Domains Involved
[3] Number of Connections
[4] User Based Handover
[5] Frequency Engaged
[6] Link-layer handoff
[7] Intra-system handoff
[8] Foreign Agent
[9] Gateway Foreign Agent
[10] Vertical handover
[11] Hard handoff

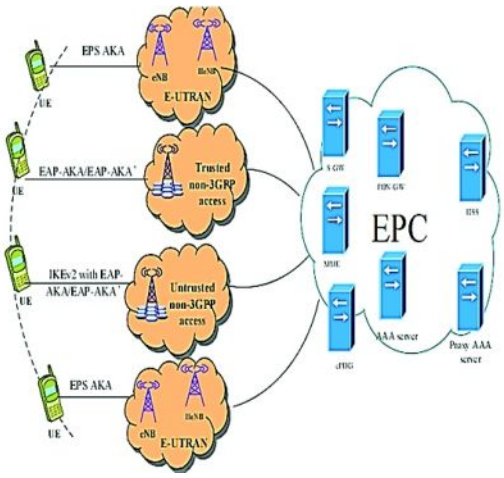
مدیریت کلید جدیدی را به‌کار می‌گیرد.

۲- تحرک بین EUTRAN و UTRAN/GERAN [۱۷].

۳- تحرک بین EUTRAN و شبکه‌های دسترسی غیر متعلق به 3GPP.

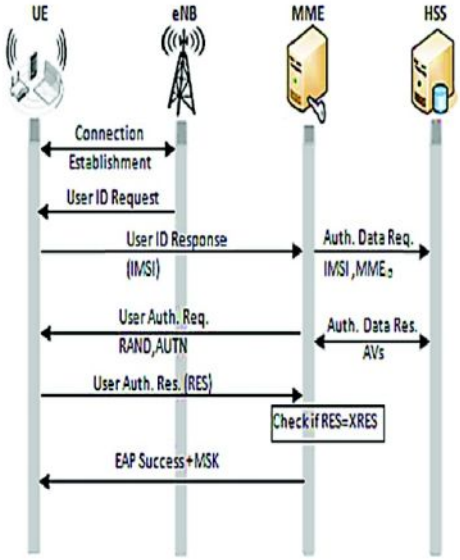
انجمن 3GPP چندین رویکرد تحرک را برای EPC به‌منظور دست‌یابی به دگرسپاری یک‌پارچه امن بین EUTRAN و شبکه‌های دسترسی غیر 3GPP پیشنهاد کرده است. با توجه به مشخصات [۱۴] 3GPP، هنگامی‌که تجهیزات کاربر از یک شبکهٔ دسترسی رادیویی به دیگری انتقال یابد، تجهیزات کاربر، شبکهٔ دسترسی مقصد و EPC احراز اصالت دسترسی کامل را اجرا خواهد کرد.

در LTE روندهای احراز اصالت متفاوتی در حالت‌های تحرک مختلف، مانند EPS AKA[1] هنگام دگرسپاری به EUTRAN، EAP-AKA[2] یا EAP – AKA′[3] هنگام دگرسپاری به شبکه‌های دسترسی غیر 3GPP معتمد و IKEv2[4] همراه با EAP-AKA یا EAP – AKA′ هنگام دگرسپاری به شبکه‌های دسترسی غیر 3GPP نامعتمد، استفاده می‌شود.



(شکل- ۶): دگرسپاری بین EUTRAN و شبکه‌های دسترسی غیر 3GPP [۲]

در شکل (۷) پروتکل احراز اصالت EPS-AKA نشان داده شده است. این پروتکل در 3GPP به‌عنوان استانداردی در نسخه ۹ برای شبکه نسل چهار مطرح شده است؛ اما، نتوانسته بسیاری از ضعف‌های پروتکل پیشین ، UMTS AKA را، که استانداری برای نسل سه است، برطرف سازد. از معایب این پروتکل می‌توان به حمله تغییر مسیر، افشای شناسهٔ کاربر، حملهٔ فردی در میان، حملهٔ منع خدمات و برخی مسائل امنیتی از قبیل نداشتن حفظ حریم خصوصی و امنیت کلید پیشرو/پسرو (KFS/KBS) اشاره کرد[۱۸]. مطابق شکل (۷) کاربر شناسه دائمی خود را در ارتباطات استفاده می‌کند که همین امر باعث افشای شناسه برای مهاجم می‌شود و زمینهٔ حملات بعدی را فراهم می‌کند. همچنین در مرحله پاسخ احراز اصالت از طرف شبکه نیز امکان به‌خطرافتادن کلیدها وجود خواهد داشت. پس از این پروتکل، طرح‌های پیشنهادی بسیاری روی کار آمد؛ اما هر یک از این طرح‌ها آسیب‌هایی داشتند؛ پس از EPS AKA پروتکل بهبودیافته آن با نام SE-EPS AKA مبتنی‌بر ساختار کلید عمومی بی‌سیم (WPKI) برای بهبود امنیت احراز اصالت در شبکه LTE مطرح شد [۱۹]. این پروتکل از امضای دیجیتال جهت غیرقابل انکاربودن پیام، پشتیبانی می‌کند و از اطلاعاتی که رد و بدل می‌شود به‌صورت همه‌جانبه محافظت می‌کند؛ اما، از معایب این طرح می‌توان به حملهٔ جستجوی جامع، حملهٔ جستجوی جامع هوشمند اشاره کرد[۲۰].



(شکل- ۷): پروتکل EPS AKA [۲۱]

مقایسه‌ای از انواع پروتکل‌های احراز اصالت در جدول (۱) ارائه شده است.

[1] Evolved Packet System Authentication and Key Agreement
[2] Extensible Authentication Protocol- Authentication and Key Agreement
[3] Improved EAP-AKA
[4] Internet Key Exchange Protocol Version 2

(جدول- ۱): مقایسه طرح‌های احراز اصالت

طرح‌های پیشنهادی	تمامیت	محرمانگی	حریم خصوصی	احراز اصالت دو طرفه
SEPS-AKA [۲۲]	√	√	√	√
EC-AKA [۲۵]	*	√	√	√
SP-AKA [۲۳]	*	√	*	√
HSK-AKA [۲۴]	*	*	*	√
EPS-AKA [۲۰]	*	*	*	√

همان‌طورکه در جدول (۱) نشان داده شده است، با افزودن محرمانگی اطلاعات به پروتکل احراز اصالت و توافق کلید EPS-AKA پروتکلی تحت عنوان EC-AKA [۲۵] و سپس نسخه جامع‌تر آن EC-AKA2 [۲۶] مطرح شدند. این پروتکل‌ها به‌منظور دست‌یابی به محرمانگی و تمامیت کلید پیشنهاد شدند. در این طرح‌ها از رمزنگاری متقارن استفاده شده است. ازآن‌جاکه الگوریتم‌های متقارن سریع‌تر از الگوریتم‌های نامتقارن هستند، این امر منجر به کاهش تأخیر می‌شود[۲۰]. در [۲۷] نیز یک پروتکل احراز اصالت گروهی (SE-AKA) پیشنهاد شده است.

(جدول- ۲): پهنای باند مصرفی طرح‌های احراز اصالت

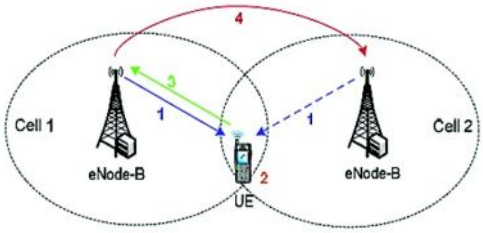
طرح	پهنای باند مصرفی (بایت)
SEPS- AKA [۲۲]	۶۷۶
EC-AKA[۲۵]	۸۱۶
SP-AKA[۲۳]	۲۴۰
HSK-AKA[۲۴]	۳۳۶
EPS-AKA[۲۰]	۲۷۶

از نتایج موجود در جدول (۲) درمی‌یابیم که پروتکل SEPS-AKA پهنای باند مصرفی کمتری نسبت به پروتکل EC-AKA دارد؛ اما در مقایسه با پروتکل‌های SP-AKA، HSK-AKA و EPS-AKA پهنای باند بزرگتری را مصرف می‌کند. پروتکل SP-AKA پهنای باند مصرفی پایینی دارد؛ اما از چارچوب پروتکل EPS-AKA پیروی نمی‌کند. پروتکل HSK-AKA مبتنی بر رویکرد مستعار بدون PKI است و EPS-AKA از نظر امنیتی کامل نیست.

۶- مراحل دگرسپاری LTE

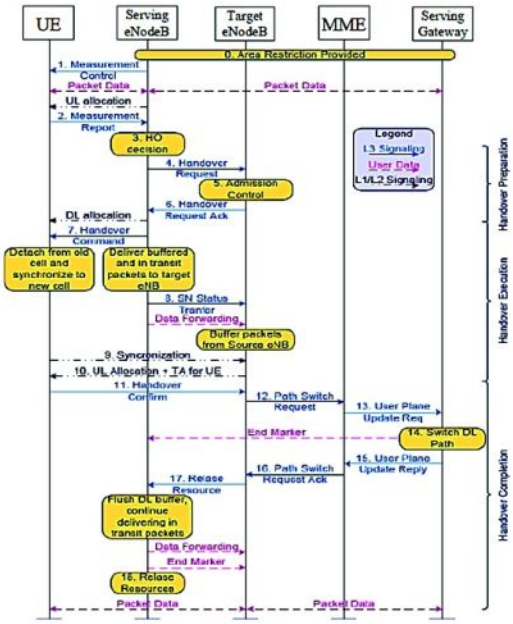
برای کاهش تهدیدات امنیتی در روند امنیتی LTE یک روش مدیریت کلید جدید برای به‌روزکردن کلیدهای بین UE و eNB، هنگامی‌که UE از یک eNB به سمت eNB دیگری (دگرسپاری افقی) حرکت کند، فراهم شده است. به‌علاوه، انجمن 3GPP الزامات و راه‌حل‌های امنیتی را برای پشتیبانی از تحرک امن بین سامانه‌های دسترسی ناهمگن تعیین کرده است؛ اما، هنوز آسیب‌های بسیاری در روند دگرسپاری عمودی LTE یافت می‌شود.

به‌طورکلی مطابق شکل (۸) روند دگرسپاری را می‌توان به چهار بخش تقسیم کرد. (۱) UE توان سیگنال پیوند فروسو را اندازه‌گیری، (۲) نتایج اندازه‌گیری‌شده را پردازش، (۳) مقادیر اندازگیری‌شده را به eNodeB خدمات‌دهنده ارسال، (۴) و eNodeB خدمات‌دهنده بر مبنای گزارش‌های ارسالی تصمیم دگرسپاری را اتخاذ می‌کند.



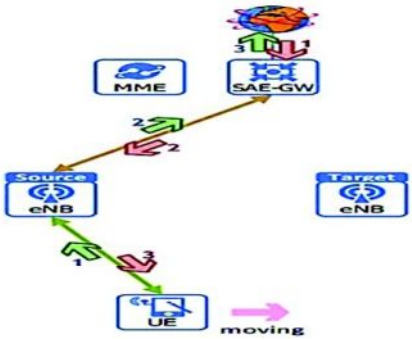
(شکل- ۸): مراحل دگرسپاری 3GPP LTE [۴]

مطابق شکل (۹) دگرسپاری LTE، شامل سه مرحله آماده‌سازی یا برپایی دگرسپاری، اجرای دگرسپاری و تکمیل دگرسپاری است. دو مرحلهٔ آخر شامل دستورهایی برای تشخیص داده‌ی از دست رفته و بازیابی اطلاعات است.



(شکل- ۹):. رویه دگرسپاری LTE [۲۸]

جزئیات مراحل دگرسپاری به‌ترتیب در شکل‌های (۱۰-۱۴) نشان داده شده است. شکل (۱۰) وضعیت تجهیزات کاربر (UE)[1] و ایستگاه‌های پایه را قبل از دگرسپاری، نشان می‌دهد.



(شکل- ۱۰): وضعیت نهادها و اجزای شبکه قبل از دگرسپاری [۲۹]

در این حالت UE با ایستگاه کاری که در محدوده آن قرار داشته، اتصال دارد. S-GW و eNB از طریق واسط هوایی S1 با یکدیگر ارتباط برقرار می‌کنند.

هنگامی‌که UE از محدوده پوشش این ایستگاه کاری خارج شود، UE باید به ایستگاه پایه جدید دگرسپاری کند.

[1] User Equipment

در این مرحله قبل از این‌که UE به سلول جدید انتقال یابد، UE، eNB منبع و eNB مقصد، آماده‌سازی می‌شوند، که این موضوع در شکل (۱۱) نشان داده شده است. در این مرحله دو ایستگاه پایه با استفاده از پروتکل کاربردی X2 با یکدیگر ارتباط برقرار می‌کنند (که در شکل با رنگ قرمز نشان داده شده است). واسط X2 به‌طوراساسی برای سیگنالینگ و انتقال بسته‌ها هنگام دگرسپاری، مورد استفاده قرار می‌گیرد. مطابق آنچه در شکل (۹) نشان داده شد، این مرحله شامل روال‌های زیر است:

(۱) کنترل/ گزارش اندازه‌گیری‌ها (پیام‌های ۱،۲)

در این مرحله eNodeB منبع مقادیر قابل اندازه‌گیری UEرا تنظیم می‌کند؛ سپس UE مقادیر اندازه‌گیری‌شده را به eNodeB خدمات‌دهنده ارسال می‌کند.

(۲) تصمیم دگرسپاری (پیام‌های۳،۴)

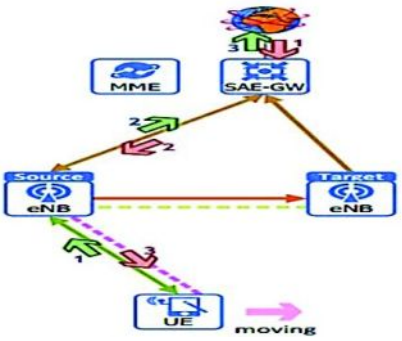
eNB منبع تصمیم دگرسپاری را اتخاذ می‌کند. این تصمیم‌گیری می‌تواند بر مبنای پارامترهای مؤثر و الزامات و استانداردها اتخاذ گردد.

(۳) کنترل پذیرش (پیام‌های ۵،۶)

eNodeB مقصد، کنترل پذیرش را با توجه به کیفیت سرویس (QoS) انجام می‌دهد و آماده دگرسپاری با L1/L2 می‌شود.

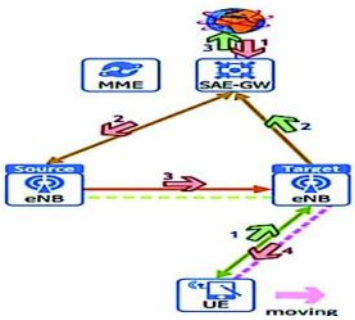
(۴) فرمان دگرسپاری (پیام ۷)

eNodeB منبع، دستور دگرسپاری را به UE می‌فرستد.



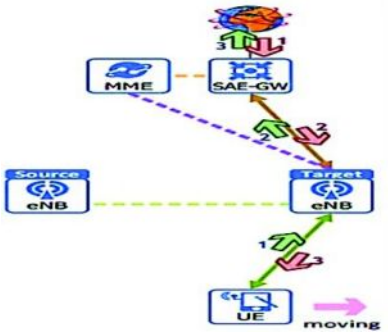
(شکل- ۱۱): فاز آماده‌سازی دگرسپاری [۲۹]

پس از مرحلهٔ آماده‌سازی، مرحلهٔ انتقال UE به ایستگاه پایه بعدی اجرا می‌شود. بنابراین مطابق شکل (۱۲)، UE اتصال خود را با ایستگاه پایه پیشین قطع و با eNB جدید اتصال برقرار می‌کند. همچنین eNB پیشین اطلاعات مرتبط با UE را به ایستگاه کاری جدید تحویل می‌دهد تا از تلفات و تأخیر جلوگیری کند. این عملیات مطابق مراحل ۸-۱۰ شکل (۹) است.



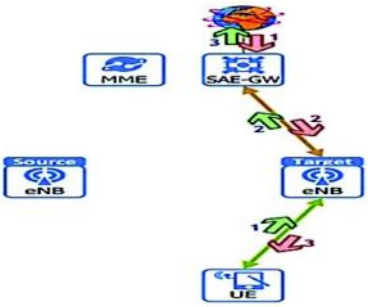
(شکل- ۱۲): فاز اجرای دگرسپاری [۲۹]

همان‌طور که در شکل (۱۳) نشان داده است، در این مرحله eNB پیشین، اتصالش را با S-GW قطع می‌کند.



(شکل- ۱۳): فاز تکمیل دگرسپاری [۲۹]

همچنین اتصال S2 را با eNB جدید قطع می‌کند. ایستگاه پایه جدید با MME ارتباط برقرار می‌کند و دگرسپاری تکمیل می‌شود. شکل (۱۴) نیز وضعیت تحرک UE و ارتباطات بین نهادهای شبکه را پس از دگرسپاری نشان می‌دهد.



شکل۱۴. وضعیت نهادها و اجزای شبکه پس از دگرسپاری [۲۹]

۷- روندهای دگرسپاری نسخهٔ ۸

در نسخهٔ ۸، پشیبانی از تحرک کاربر برای تجهیزات کاربر در وضعیت اتصال شامل دو روند دگرسپاری است[۳۰]:

۱) دگرسپاری پسرو[1]

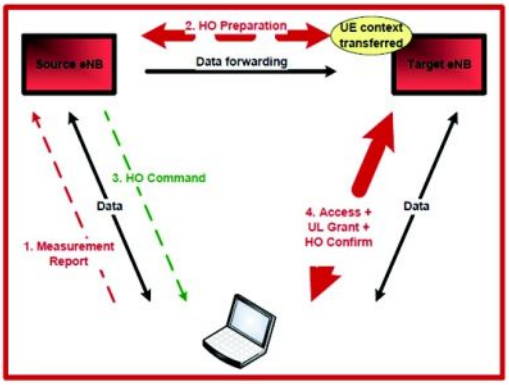
۲) دگرسپاری پیوند رادیویی ناموفق (RLF)[2]

در هر دو روند دگرسپاری، نیاز است که eNB منبع یک سلول مقصد را با توجه به تصمیمات دگرسپاری برای ادامه ارتباط در نظر بگیرد.

همان‌طور که پیش از این اشاره شد، دگرسپاری در LTE از نوع دگرسپاری سخت است، بدین معناکه هنگام دگرسپاری، در خدمات وقفه کوتاهی وجود دارد. این موضوع مرتبط با دگرسپاری بین eNBها است. همچنین به‌منظور به‌کمینه‌رساندن اتلاف بسته‌ها، eNB منبع، داده‌های پیوند فروسو[3] (یا حتی پیوند فراسو[4]) سطح کاربر را به eNB مقصد ارسال می‌کند.

۷-۱- دگرسپاری پسرو[5]

شکل (۱۵) روند دگرسپاری پسرو را نشان می‌دهد. همان‌طور که در این شکل نیز مشاهده می‌شود، اطلاعات مرتبط با دگرسپاری بین UE و eNB منبع از طریق مسیرهای رادیویی قبلی مبادله می‌شوند (از این‌رو، از اصطلاح پسرو استفاده می‌شود).



(شکل- ۱۵): روند دگرسپاری پسرو [۳۰]

در این روند نیاز است که شرایط رادیویی برای eNB منبع به‌اندازهٔ کافی خوب باشند، تا قادر به اندازه‌گیری مقادیر از UE باشد و درنتیجه سلول مقصد را برای دگرسپاری فراهم کند. همچنین شرایط رادیویی برای UE باید به‌اندازهٔ کافی خوب باشد تا بتواند دستورهای دگرسپاری را از eNB

[1] Backward handover
[2] Radio Link Failure
[3] Downlink
[4] Uplink
[5] Backward handover

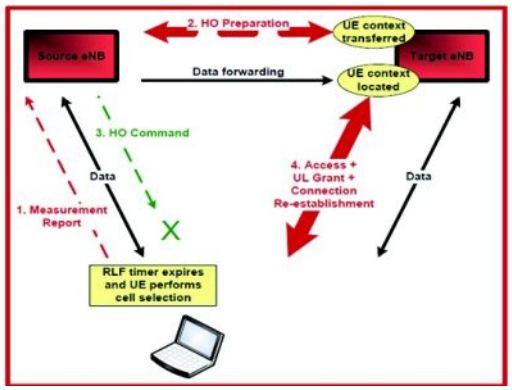
منبع بگیرد.

در این روش وقفه کوتاهی در خدمات، زمانی‌که UE دستورهای دگرسپاری را می‌گیرد و زمانی‌که eNB مقصد تصدیق دگرسپاری را از UE دریافت می‌کند، وجود دارد؛ اما، ارسال داده و تحویل آن تضمین می‌کند که هیچ‌یک از داده‌های بافرشده در eNB منبع از بین نمی‌روند.

۷-۲- دگرسپاری RLF

شکل (۱۶) روند دگرسپاری RLF را نشان می‌دهد. دگرسپاری RLF، تحرک مبتنی‌بر UE است، هنگامی‌که سیگنالینگ دگرسپاری پسرو با سلول منبع، با توجه به شرایط رادیویی ضعیف اندکی افت پیدا کند، یک روش بازیابی را فراهم می‌کند. شرایط رادیویی برای eNB باید به اندازهٔ کافی خوب باشد، تا eNB بتواند اندازه‌گیری‌ها را از UE بگیرد؛ اما نیاز نیست شرایط رادیویی برای UE خوب باشد تا دستورهای دگرسپاری را از eNB منبع دریافت کند.

روند دگرسپاری RLF در مقایسه با دگرسپاری پسرو از تأخیر اضافی رنج می‌برد و درنتیجه، وقفه طولانی‌تری در خدمات وجود خواهد داشت؛ اما، در این روش نیز ارسال داده و تحویل آن تضمین می‌کند که داده‌های بافرشده در eNB مقصد از بین نمی‌روند.

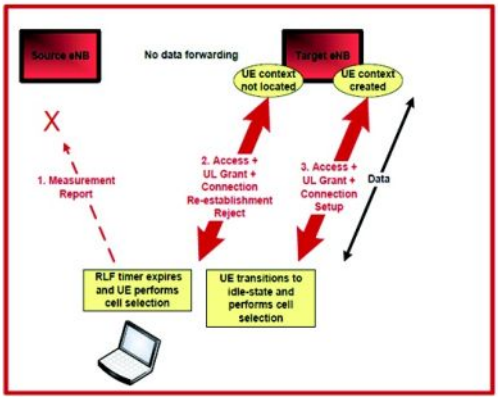


(شکل-۱۶): روند دگرسپاری LTE RLF [۳۰]

۷-۳- بازیابی NAS

شکل (۱۷) روند بازیابی NAS را نشان می‌دهد. بازیابی NAS، تحرک مبتنی‌بر کاربر است. از آنجاکه در این روش، شرایط رادیویی برای eNB منبع خوب نیست، قادر نیست گزارش اندازه‌گیری‌ها را از UE بگیرد. بنابراین eNB منبع، سلول مقصد را برای دگرسپاری نمی‌تواند انتخاب نماید.

با بازیابی NAS، UE نمی‌تواند حالت اتصال حفظ کند، در عوض به محض شکست ارتباط، UE از حالت اتصال به حالت آماده به‌کار[1] می‌رود و اتصال جدیدی را اتخاذ می‌کند. گذر به حالت idle از تاخیر بیشتری در مقایسه با روند دگرسپاری RLF رنج می‌برد و در نتیجه، منجر به وقفه طولانی‌تری در خدمات خواهد شد. همچنین از آنجاکه امکان ارسال داده و تحویل آن وجود ندارد، داده‌های بافر شده در eNB منبع از بین می‌روند.



(شکل- ۱۷): روند بازیابی LTE NAS [۳۰]

۷-۴- دگرسپاری پیشرو[2]

روند این نوع دگرسپاری در شکل (۱۸) به تصویر کشیده شده است. این دگرسپاری از نوع تحرک مبتنی بر کاربر است. اطلاعات مرتبط با دگرسپاری بین UE و eNB مقصد از طریق مسیر رادیویی جدید، پس از اینکه اطلاعات UE توسط eNB مقصد از eNB منبع گرفته شود، مبادله می‌شود. (از این‌رو اصطلاح پیشرو استفاده شده است)؛ حتی اگر شرایط رادیویی برای eNB منبع به اندازه کافی مناسب نباشد که بتواند گزارش اندازه‌گیری‌ها را از UE بگیرد و سلول مقصد را فراهم کند، دگرسپاری پیشرو موفقیت‌آمیز است.

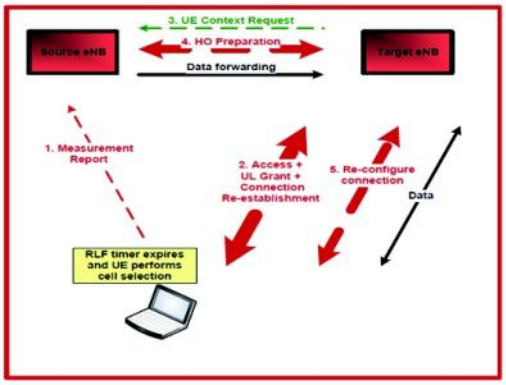
حتی با شکست کامل سیگنالینگ eNB منبع روند دگرسپاری موفقیت‌آمیز است و باعث می‌شود دگرسپاری پیشرو نسبت به تغییرات سریع نامزدهای توان سیگنال مقاوم باشد. همانند دیگر روندهای دگرسپاری، هنگامی‌که UE مشکلات پیوند رادیویی را تشخیص دهد، زمان‌سنج RLF را آغاز می‌کند؛ اما برخلاف دگرسپاری RLF و روند

[1] Idle
[2] Forward

بازیابی NAS، ارائه‌دهنده خدمات می‌تواند زمان‌سنج را به مقدار بالاتری تنظیم کند و درنتیجه هزینهٔ RLF کاهش می‌یابد.

این روند دگرسپاری در مقایسه با روند دگرسپاری پسرو، همچنان از تأخیر اضافی رنج می‌برد و درنتیجه وقفهٔ طولانی‌تری را در خدمات به همراه خواهد داشت؛ اما، در مقایسه با دگرسپاری RLF و روند بازیابی NAS، با توجه به توانایی تنظیم مقدار بالاتر برای اندازه زمان‌سنج RLF، منجر به وقفه کوتاه‌تر می‌شود؛ به‌علاوه، ارسال داده و تحویل، تضمین می‌کند که هیچ‌یک از داده‌های بافرشده در eNB منبع از بین نمی‌روند (برخلاف روند بازیابی NAS). از منظر UE، دگرسپاری پیشرو نیاز به هیچ تغییری در مشخصات نسخه ۸، 3GPP ندارد. از نظر eNB تنها تفاوت این است که eNB مقصد نیاز به گرفتن اطلاعات UE از eNB منبع دارد، هنگامی‌که UE می‌خواهد با سلول مقصد ارتباط برقرار کند اما، سلول مقصد هنوز آمادگی لازم را نداشته باشد.

تحرک با استفاده از دگرسپاری پیشرو مقاوم و از نظر هزینه در توپولوژی شبکه بهینه است، چراکه در شبکه‌های ad-hoc با افزودن گره سیار نیاز به هزینه اضافی محاسبات مجدد برای تایمر RLF ندارد.



(شکل- ۱۸): شکل دگرسپاری LTE Forward [۳۰]

۸- الگوریتم‌های تصمیم دگرسپاری برای فمتوسل‌ها

گرچه موضوع دگرسپاری بین ماکروسل‌ها و فمتوسل‌ها حوزهٔ پژوهشی تا حدودی جدید است، با این حال پژوهش‌های بسیاری مرتبط با الگوریتم‌های دگرسپاری درون شبکه LTE انجام شده است. در بیشتر الگوریتم‌ها از ترکیب ویژگی‌ها برای اتخاذ تصمیم نهایی صحیح استفاده می‌شود. بر اساس اقدامات انجام‌شده در این حوزه، الگوریتم‌ها را می‌توان به پنج گروه کلی به‌صورت، (۱) الگوریتم‌های مبتنی‌بر توان سیگنال دریافتی(RSS)[1] (۲) الگوریتم‌های مبتنی‌بر سرعت[2] (۳) الگوریتم‌های مبتنی‌بر تابع هزینه[3] (۴) الگوریتم‌های آگاه از تداخل[4] (۵) الگوریتم‌های مبتنی‌بر بهینه انرژی[5]، تقسیم‌بندی کرد. در ادامه هر یک از این الگوریتم‌ها به‌اختصار شرح داده می‌شوند.

۸-۱- الگوریتم‌های مبتنی‌بر توان سیگنال دریافتی

الگوریتم‌های مطرح در این دسته به مقدار توان سیگنال دریافتی مورد استفاده بستگی دارند. تاکنون رویکردهای متعددی در مورد این‌که چگونه RSS حین مرحله تصمیم‌گیری دگرسپاری مورد استفاده قرار گیرد، مطرح شده‌اند. از جمله:

الف) مقایسه مقدار RSS سلول خدمات‌دهنده و سلول مقصد(RSS نسبی)

ب)مقایسه RSS سلول مقصد و سلول مقصد با مقدار آستانه RSS (مقدار مطلق RSS)

پ) ترکیب دو طرح بالا. به‌عنوان مثال از طرح‌های این دسته می‌توان به [۳۱]، [۳۲]، [۳۳] اشاره کرد.

۸-۲- الگوریتم‌های مبتنی‌بر سرعت

این الگوریتم‌ها از سرعت UE به‌عنوان معیار اولیه تصمیم دگرسپاری استفاده می‌کنند، که از طرح‌های ارائه‌شده به [۳۴]، [۳۵]، [۳۶] می‌توان اشاره کرد. تصمیم دگرسپاری با مقایسهٔ سرعت مطلق UE با مقدار آستانه که در برخی موارد به‌صورت اختیاری تعیین می‌گردد، اتخاذ می‌شود. الگوریتم‌های مبتنی‌بر سرعت از سایر معیارهای تصمیم دگرسپاری از قبیل، RSS، نوع ترافیک کاربر، پهنای باند موجود در شبکه مقصد و وضعیت UE نیز بهره می‌برند.

۸-۳- الگوریتم‌های مبتنی‌بر تابع هزینه

الگوریتم‌های این طبقه گستره وسیعی از پارامترهای تصمیم دگرسپاری به‌عنوان مثال، طول عمر باتری، نوع ترافیک، بار

[1] Received signal strength based algorithms
[2] Speed based algorithms
[3] Cost-function based algorithms
[4] Interference-aware algorithms
[5] Energy-efficient algorithms

سلول، RSS و سرعت را توسط یک تابع هزینه ترکیب می‌کنند. تصمیم دگرسپاری از مقایسه نتیجه تابع هزینه برای سلول خدمات‌دهنده و سلول‌های نامزد، به‌دست می‌آید. طرح‌های این دسته [۳۷]، [۳۸]، [۳۹]، [۴۰] یا از ترکیب پارامترهای تصمیم‌گیری در یک تابع و یا از مجموع وزن‌ها استفاده می‌کنند.

۸-۴- الگوریتم‌های مطلع از تداخل

الگوریتم‌های این طبقه برای محاسبه تأثیری که تداخل روی تجهیزات کاربر یا سلول‌ها می‌گذارد، مورد استفاده قرار می‌گیرند. از طرح‌های ارائه‌شده این طبقه می‌توان به [۴۱]، [۴۲] اشاره کرد. پارامترهای اصلی تصمیم‌گیری در این طبقه شامل موارد زیر است:

الف) اندازه‌گیری کیفیت سیگنال دریافتی(RSQ)[1]

ب) توان تداخل دریافتی(RIP)[2] در سلول‌ها

پ) توان انتقالی سیگنال‌های منابع (RS)[3] در سلول‌ها

ت) محدوده تداخل در سلول‌ها

الگوریتم‌های مبتنی‌بر RSQ به‌طورعمومی مقدار RSQ خدمات‌دهنده و مقصد را با هم مقایسه یا اجازه تحرک را در فمتوسل، هرگاه که RSQ فمتوسل مجاور از مقدار RSQ آستانه بیشتر شود، فراهم می‌کنند. از طرف دیگر، الگوریتم‌هایی که توان انتقالی RS، سطح تداخل، یا محدوده تداخل را در سلول‌ها محاسبه می‌کنند، عملکرد SINR را بهبود می‌بخشند؛ اما، مشارکت این پارامترها روندهای سیگنالینگ شبکه را مانند طرح [۴۳] پیچیده‌تر می‌سازد.

۸-۵- الگوریتم‌های مبتنی‌بر بهینه انرژی

الگوریتم‌های این طبقه، با هدف بهره‌وری از صرفه‌جویی انرژی با عملکرد توان کم مصرف فمتوسل‌ها ارائه شده‌اند. الگوریتم‌های بهینه انرژی از معیارهای تصمیم دگرسپاری از قبیل توان باتری، انرژی مصرفی UE یا توان انتقالی UE استفاده می‌کنند. مصرف انرژی در گره‌های شبکه بسیار به تداخل بستگی دارد. این الگوریتم‌ها به الگوریتم‌های مطلع از تداخل بسیار نزدیک هستند. طرح [۴۳] از الگوریتم‌های مبتنی بر بهینه انرژی است.

۹- احراز اصالت دگرسپاری در شبکه LTE

احراز اصالت از مفاهیم اصلی و امنیتی مرتبط با دگرسپاری است؛ چون حین دگرسپاری نباید شبکه در معرض حمله قرار گیرد و امنیت و دسترسی آن به خطر افتد. باتوجه به حالت‌های مختلف تحرک در شبکه LTE در سال‌های اخیر روندهای احراز اصالت متعددی برای استفاده در شبکه LTE پیشنهاد شده است. این طرح‌ها بیش‌تر به چهار دسته به‌صورت زیر تقسیم‌بندی می‌شوند:

(۱) طرح‌های مبتنی‌بر AAA: طرح‌های مبتنی بر سرور AAA از امنیت بالایی برخوردارند؛ اما از ترافیک بالا بین UE و شبکه رنج می‌برند؛ زیرا در هر بار اجرای دگرسپاری به مخابره اطلاعات بین UE و AAA نیاز دارند. همچنین از آنجاکه eNB ممکن است دور از سرور AAA باشد، ممکن است دسترسی با مشکلاتی همراه و منجر به تأخیر غیرقابل پذیرش در شبکه شود. بنابراین با توجه به آسیب‌پذیری این قبیل طرح‌ها در برابر حمله DOS، مصرف پهنای باند اضافی و ناکارامدی کمتر از این طرح‌ها استفاده می‌شود.

(۲) طرح‌های مبتنی بر امنیت محتوا (SCT): این طرح‌ها شامل ارتباط با سرور AAA نیستند. از آنجاکه این طرح‌ها مستلزم برقراری ارتباطی امن بین هر دو eNB هستند و این موضوع هنگامی‌که دو eNB در شبکه‌های مختلفی باشند، صحت ندارد، در شبکه LTE نیز قابل پیاده‌سازی نیستند.

(۳) طرح‌های احراز اصالت مستقیم: مبتنی‌بر رمزنگاری کلید عمومی هستند. این طرح‌ها به سه دست تکانی بین UE و eNB نیاز دارند؛ به‌علاوه به کلیدهای از پیش توزیع شده و ارتباط امن بین اجزا نیازی ندارند و روند احراز اصالت ساده‌ای دارند؛ اما این طرح‌ها به‌طورمعمول قادر به تحقق محرمانگی پیشروی کامل نمی‌شوند. با استفاده از سامانهٔ رمزنگاری مبتنی‌بر شناسه، طرح‌های احراز اصالت جدیدی در شبکه‌های سیار ارائه شده است. در برخی از این طرح‌ها از زوج‌نگار دوخطی استفاده می‌شود که امنیت بالایی را در شبکه تضمین می‌کنند؛ اما از نظر کارایی، شبکه را کمی با بحران روبه‌رو می‌کند. بنابراین، این طرح‌ها با بهبود کارایی سعی بر اجرایی‌شدن در شبکه‌های سیار دارند. در برخی دیگر از زوج‌نگار دو خطی استفاده نشده تا کارایی سطح قابل قبولی داشته

[1] Received Signal Quality
[2] Received interference power
[3] Reference signals

باشد، امنیت شبکه نیز با سازوکارهای امنیتی دیگر تامین شده است.

(۴) طرح‌های ترکیبی: در این طرح‌ها UE امضا تولید و eNB مقصد بر اساس درستی امضا به UE اعتماد می‌کند. طرح‌های مبتنی‌بر امضا و SCT به ارتباط با سرور AAA نیازی ندارند. مشابه طرح‌های مبتنی‌بر SCT به برقراری کانال امن بین eNBها نیاز دارد. بنابراین این طرح نیز با وجود احتمال قراگیری دو ایستگاه کاری در دو شبکهٔ متفاوت، غیر عملی است.

مطابق توضیحات بالا، طرح‌های مبتنی‌بر AAA، طرح‌های مبتنی‌بر SCT و طرح‌های ترکیبی روند احراز اصالت تاحدودی پیچیده دارند. به‌علاوه، طرح‌های ترکیبی و مبتنی‌بر SCT از ترافیک احراز اصالت بین eNBها ، که با توجه به فقدان واسط مستقیم بین eNBها و HeNBها در شبکه‌های LTE غیرعملی هستند، رنج می‌برند. طرح‌های مستقیم نیز روند احراز اصالت ساده‌ای دارند؛ اما از نظر کارایی و یا امنیت آسیب‌پذیر هستند؛ بنابراین در اقدامات اخیر بیشتر بر این نوع طرح‌ها تمرکز شده است. همچنین روندهای احراز اصالت یکنواخت که برای تمام حالات تحرک در شبکه‌های سیار مورد استفاده قرار گیرند، با توجه به سادگی بیشتر مورد توجه قرار گرفته‌اند.

۹- نتیجه‌گیری و اقدامات آتی

شبکه‌های نسل چهار از استانداردهای نسل جدید مخابرات سیار است که با ارائه نرخ داده و منطقه تحت پوشش بالاتر، طیف گسترده‌تری از کاربران را به همراه دارد. امنیت دسترسی در هر شبکه‌ای نسبی است. همواره آسیب‌هایی در طراحی یا سازوکارهای به‌کاررفته در شبکه‌ها وجود دارد. در این مقاله سعی شد تا پس از معرفی نسل چهار مخابرات به آسیب‌ها و چالش‌های حوزه امنیت دسترسی شبکه LTE و اقدامات اخیر اشاره شود. روندهای تحرک، الگوریتم‌های دگرسپاری در شبکه LTE و پروتکل‌های احراز اصالت مورد استفاده در تحرک درون‌شبکه‌ای LTE نیز به تفضیل بررسی شد. فعالیت بعدی ارائه الگوریتم بهینه با پیکربندی خودکار در شبکه LTE است.

۱۰- مراجع

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); (Rel 11), 3GPP TS 23.228 V11.6.0 ,Sep. 2012.

[2] J. Cao et al, "A survey on security aspects for LTE and LTEA networks," Communications Surveys & Tutorials, IEEE 16.1 (2014): 283-302, 2014.

[3] Xenakis et al., "mobility management for femtocells in LTE-Advanced: key aspects and survey of HO ALGS, " IEEE communications surveys & tutorials,vol. 16, no. 1, first quarter, 2014.

[4] Ardian Ulvan et al., "The Study of Handover Procedure in LTE-based Femtocell Network," wireless and mobile networking conference.2010.

[5] Shih-Jung Wu .," A New Handover Strategy between Femtocell and Macrocell for LTE-Based Network" Ubi-Media Computing (U-Media) . July 2011.

[6] T. Ali-Yahiya., "Understanding LTE and its Performance," Chapter 2, Network Architecture and Protocols. Springer, 2011.

[7] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB) (Rel 11), 3GPP TS 22.220 V11.6.0 Sep. 2012.

[8] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks (Rel 11), 3GPP TS 24.302 V11.4.0 Sep. 2012.

[9] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC) (Rel 12), 3GPP TS 22.368 V12.0.0 Sep. 2012.

[10] 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Rel 12) 3GPP TS 33.401 V12.5.0, Sep. 2012.

[11] M. Zekri et al., " A review on mobility management and vertical handover solutions over heterogeneous wireless networks"Computer Communications 35 (2012) 2055–2068

[12] Ravichandra M et al.," A Survey on Handovers Literature for Next Generation Wireless Networks," International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 12, December 2013.

[13] Abdoul-Aziz IssakaHassane et al., "Handover Decision Based on User Preferences in Heterogeneous Wireless Networks" College of Information Science and Engineering, Hunan University, China 2012.

[14] 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Rel 11), 3GPP TS 33.402 V11.4.0, June 2012.

[15] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-

Description," . 2008.
[29] www.3glteinfo.com/intra-lte-handover-using-x2-interface/ Dec 4, 2013.
[30]https://www.qualcomm.com/.../lte-mobility-enhancements /Jul 18, 2013 .
[31] J. Moon, D. Cho, "Efficient handoff algorithm for inbound mobility in hierarchical macro/femto cell networks," IEEE Commun. Mag. Letters, vol.13, no.10, pp.755-757, Oct. 2009.
[32] J. Moon, D. Cho, "Novel Handoff Decision Algorithm in Hierarchical Macro/Femto-Cell Networks," IEEE Wireless Commun. and Netw. Conf. (WCNC) 2010, pp.1-6, Apr. 2010.
[33] P. Xu et al, "An efficient handoff algorithm based on received signal strength and wireless transmission loss in hierarchical cell networks," Telecom. Sys. J., Elsevier, pp. 1-9, Sept. 2011.
[34] A. Ulvan et al., "Handover Scenario and Procedure in LTE-based Femtocell Networks," The 4th Internat. Conf. on Mob. Ubiq. Comput., Syst., Serv. and Technolog., pp. 213-218, Oct. 2010.
[35] H. Zhang et al., "Signalling Cost Evaluation of Handover Management Schemes in LTE-Advanced Femtocell," 2011 IEEE 73rd Vehic. Techn. Conf. (VTC Spring), pp.1-5, May 2011.
[36] W. Shaohong et al., " Handover Study Concerning Mobility in the Two-Hierarchy Network," IEEE 69th Vehic. Techn. Conf. (VTC), pp.1-5, Apr. 2009.
[37] H. Zhang et al., "A Novel Handover Mechanism Between Femtocell and Macrocell for LTE Based Networks," IEEE 2nd Internat. Conf. on Comm. Softw. and Nets. 2010 (ICCSN), pp.228-231, Feb. 2010.
[38] P. Xu et al., "A User's State and SINR-Based Handoff Algorithm in Hierarchical Cell Networks," 2010 IEEE 6th Internat. Conf. on Wirel. Comm. Netw. and Mobile Comp. (WiCOM),pp.1-4, Sept. 2010.
[39] D. Lee et al., "A Cost-Based Adaptive Handover Hysteresis Scheme to Minimize the Handover Failure Rate in 3GPP LTE System," EURASIP J. on Wirel. Comm. and Netw., vol. 2010, no. 6, Feb. 2010.
[40] K. S. B. Reguiga et al., "Handoff Management in Green Femtocell Network," Internat. J. of Comp. Apps., vol. 27, no.4, pp. 1-7, Aug. 2011.
[41] Z. Becvar, P.Mach, "Adaptive Hysteresis Margin for Handover in Femtocell Networks," IEEE 6th Internat. Conf. on Wirel. and Mobile Comm., pp.256-261, Sept. 2010.
[42] G. Yang et al., "Handover control for LTE femtocell networks," 2011 IEEE Internat. Conf. on Electronics, Comm. And Control (ICECC), vol., no., pp.2670-2673, Sept. 2011.
[43] K. Zheng et al.," Energy-efficient wireless in-home: the need for interference-controlled femtocells," IEEE Wireless Commun., vol.18, no.6, pp.36-44, Dec. 2011.
3GPP accesses (Rel11), 3GPP TS 23.402 V11.4.0 Sep. 2012.
[16] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN);Overall description; (Rel 11), 3GPP TS 36.300 V11.3.0 Sep. 2012.
[17] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Rel 11), 3GPP TS 23.401 V11.3.0 Sep. 2012.
[18] C. Lai et al.," SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," Computer Networks, Elsevier,2013.
[19] L. Xiehua et al., "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network, " Wireless Communications, Networking and Mobile Computing (WiCOM), 2011, pp.1-4.
[20] Jacques Bou Abdo et al., "Ensured Confidentiality Authentication and Key Agreement Protocol for EPS", Proc. Broadband Networks and Fast Internet (RELABIRA 2012), pp.73-77, May 2012.
[21] Kamal Ali Alezabi et al ., " An Efficient Authentication and Key Agreement Protocol for 4G (LTE) Networks" IEEE Region 10 Symposium .2014.
[22] Z. J. Haddad et al., "SEPS-AKA:A Secure Evolved Packet System Authentication and Key Agreement Scheme For LTE-A Networks, " Computer Sciecne and Impormation Technology, Vol.4, No.12, pp. 57-70, 2014.
[23] J. Bou Abdo et al., "EPS mutual authentication and cryptanalyzing SPAKA," IEEE International Conference on Computing, Management and Telecommunications, 2013.
[24] K. Hamandi et al ., "Privacy enhanced and computationally efficient hsk-aka lte scheme," in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, pp. 929–934, 2013.
[25] J. Abdo et al ., "Ensured Confidentiality Authentication and Key Agreement Protocol for EPS," Proc. Broadband Networks and Fast Internet (RELABIRA 2012), pp.73-77, , May 2012.
[26] Abdo et al ., "EC-AKA2 a revo-lutionary AKA protocol," In: International Conference on Computer ApplicationsTechnology (ICCAT), pp. 1–6. , 20–22 January .2013.
[27] C. Lai et al., "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," Computer Networks, 14 August 2013.
[28] 3GPP-TS36.300 v8.5.0, "E-UTRAN Overall

معصومه صفاخیل مدرک کارشناسی خود را در رشتهٔ مهندسی برق گرایش الکترونیک از دانشگاه آزاد اسلامی واحد کرج در سال ۱۳۹۱ و مدرک کارشناسی ارشد را در رشتهٔ مهندسی برق- مخابرات گرایش رمز از دانشگاه صنعتی مالک اشتر در سال ۱۳۹۴ اخذ کرد. عنوان پایان‌نامهٔ ایشان " تحلیل و بهبود پروتکل احراز اصالت دگرسپاری عمودی" است که با رتبهٔ عالی دفاع شده است. تحلیل پروتکل‌های امنیتی و امنیت شبکه‌های بی‌سیم از جمله زمینه‌های پژوهشی ایشان است.

علی پاینده مدرک کارشناسی ارشد خود را در رشتهٔ مهندسی برق گرایش مخابرات از دانشگاه تربیت مدرس در سال ۱۳۷۳ و همچنین مدرک دکترای خود را در رشتهٔ مهندسی برق مخابرات از دانشگاه خواجه نصیرالدین طوسی در سال ۱۳۸۵ اخذ کرد. وی در سال‌های ۱۳۷۵ تا ۱۳۸۵ به‌عنوان یکی از مدیران انجمن تحقیقات علوم کاربردی بوده است که در زمینهٔ ارتباطات ماهواره‌ای امن فعالیت داشته است. ایشان در حال حاضر استادیار مجتمع دانشگاهی فناوری اطلاعات، ارتباطات و امنیت دانشگاه صنعتی مالک اشتر تهران است. از ایشان بیش از ۷۵ مقاله علمی در کنفرانس‌ها و مجلات بین‌المللی به چاپ رسیده است. تئوری اطلاعات، تئوری کدینگ، رمزنگاری، پروتکل‌های امنیتی، مخابرات امن و مخابرات ماهواره‌ای از جمله زمینه‌های پژوهشی ایشان است.