مروری بر پروتکل احراز اصالت و توافق کلید EAP-AKA در شبکهٔ میان‌کاری 3GPP-WLAN

محمدرضا گوهره‌یی[1]، مجید بیات[2]، علی پاینده[3]
[1 و 3]دانشگاه مالک اشتر، تهران، ایران
mrgmohammad@gmail.com, payandeh@mut.ac.ir
[2]دانشکده برق، دانشگاه صنعتی شریف، تهران، ایران
bayat@ee.sharif.ir

چکیده

پوشش‌دهی مناسب، دسترس‌پذیری و سرعت بالای انتقال داده از مهم‌ترین مسائل در مخابرات نسل جدید است. بر همین اساس از مخابرات نسل سوم، ارائهٔ خدمات میان‌کاری مطرح شد و در مخابرات نسل چهارم بیشتر مورد توجه قرار گرفت. بر همین اساس فناوری‌های متفاوتی برای ارائهٔ خدمات میان‌کاری، در مخابرات نسل جدید مطرح شد که از این بین، فناوری WLAN بیشتر از همه مورد استقبال قرار گرفت. مرجع استانداردسازی 3GPP برای ارائهٔ خدمات میان‌کاری، شش سناریوی کلی را مطرح کرده است که براساس این سناریوها می‌توان نحوهٔ دسترسی کاربر به شبکه، معماری شبکه و پشتهٔ پروتکلی را می‌توان تعیین و طراحی کرد. در این مقاله به معرفی مفهوم میان‌کاری، سناریوهای شش‌گانه، معماری شبکه و مروری بر کارهای انجام‌شده می‌پردازیم.

واژگان کلیدی: میان‌کاری، احراز اصالت، EAP-AKA

۱- مقدمه

میان‌کاری، امکان برقراری ارتباط توسط سایر نسل‌های مخابراتی همچون نسل ۲ و ۳ و با سایر فناوری‌ها مانند WLAN[1]، WiMAX[2] و Bluetooth برای بهره‌برداری از خدمات شبکه‌های 3GPP[3] فراهم می‌شود[1]. مسألهٔ ارائهٔ خدمات مبتنی‌بر میان‌کاری از مخابرات نسل سوم مطرح شد و در LTE[4] و مخابرات نسل چهارم مورد توجه قرار گرفت. از بین فناوری‌های مطرح برای میان‌کاری، فناوری WLAN از همه بیشتر مورد توجه قرار گرفت. این توجه به دو دلیل اصلی صورت گرفت: نخست این که فناوری WLAN در بیشتر وسایل ارتباطی مانند تلفن‌های همراه، تبلت‌ها و لپ‌تاپ‌ها وجود دارد؛ بر همین اساس زیرساخت ارتباطی برای توسعهٔ میان‌کاری مبتنی‌بر این فناوری وجود دارد؛ دوم این که استفاده از میان‌کاری WLAN با مخابرات نسل‌های جدید، امکان بهره‌برداری هم‌زمان از دو شبکهٔ سلولی (شبکه تلفن همراه) و رایانه‌ای (شبکه WLAN) برای کاربران فراهم می‌شود.

در بین مسائل موجود جهت توسعهٔ میان‌کاری، مسأله برقراری امنیت از مهم‌ترین مسائل است؛ چون امنیت در دو سطح شبکهٔ WLAN و 3GPP مورد بحث قرار می‌گیرد. یکی از مسائل مهم در امنیت، پروتکل‌های احراز اصالت است. مرجع استانداردسازی 3GPP برای شبکهٔ میان‌کاری 3GPP-WLAN نیز پروتکل EAP-AKA[5] را معرفی کرده است. پروتکل EAP-AKA یکی از روش‌های چهارچوب EAP[6] است؛ چون خودEAP به‌تنهایی یک پروتکل نیست؛ بلکه چهارچوبی برای توسعهٔ پروتکل‌های احراز اصالت است و روش‌های گوناگونی را دربرمی‌گیرد. این چهارچوب توسط نهاد استانداردسازی IETF تحت استاندارد RFC 3748 در سال ۲۰۰۴ استاندارد شده است.[۲]

1 Wireless Local Area Network
2 Worldwide Interoperability for Microwave Access
3 3rd Generation Partnership Projec
4 Long Term Evolution
5 EAP-Authentication and Key Agreement
6 Extensible Authentication Protocol

در بخش دوم میان‌کاری 3GPP-WLAN، در بخش سوم: پروتکل EAP-AKA ، در بخش چهارم مروری بر کارهای انجام‌شده و در بخش آخر، پیشنهادها ارایه می‌شود.

۲- میان‌کاری 3GPP-WLAN

بنا به استاندارد 3GPP برای بهره‌برداری از شبکهٔ میان‌کاری، شش سناریوی متفاوت در نظر گرفته شده است. روند این سناریوها به‌گونه‌ای است که هر سناریو، سناریوی قبلی خود را تکمیل می‌کند و ساختار هرکدام به‌گونه‌ای در نظر گرفته شده است که با سناریوی دیگر متفاوت باشد. این تفاوت سناریوها برای ایجاد تمایز بین آن‌ها در نظر گرفته شده است[۳].

روند سناریوها به‌شرح زیر است:

سناریوی نخست: به‌عنوان پایهٔ سناریوها در نظر گرفته می‌شود و فقط برای حالت صدور صورت‌حساب و حمایت از مشتری است.

سناریوی دوم: برای بررسی کنترل دسترسی و حسابرسی به هزینه‌ها طراحی شده است. در این سناریو کاربر قادر به بهره‌برداری از خدمات PS[1] شبکه 3GPP نیست؛ ولی خدمات خود را مانند اینترنت و ... از نهاد WLAN AN دریافت می‌کند.

سناریوی سوم: برای دسترسی کاربر به خدمات PS شبکهٔ 3GPP طراحی شده است؛ به‌گونه‌ای که علاوه‌بر کنترل دسترسی و حسابرسی هزینه‌های کاربر، امکان بهره‌برداری از خدمات کلیدزنی بسته‌ای شبکهٔ 3GPP به کاربر داده می‌شود. درواقع این سناریو مکمل سناریوی دوم است.

سناریوی چهارم: برای ارایهٔ پیوستگی خدمات بین دو شبکهٔ سلولی و میان‌کاری مطرح شده است؛ هدف از این سناریو بهبود سناریوی سوم است.

سناریوی پنجم: برای ارایهٔ یک‌پارچگی خدمات بین دو شبکهٔ سلولی و میان‌کاری مطرح شده است. درواقع این سناریو برای بهبود سناریوی چهارم است؛ چون در استفاده از سناریوی چهارم در هنگام واگذاری بین شبکه‌ها امکان قطعی دریافت خدمات وجود دارد.

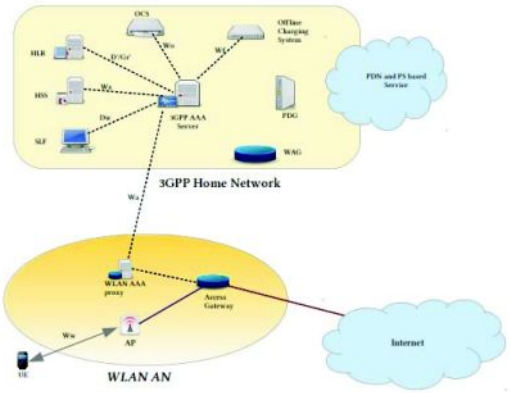
سناریوی ششم: برای بهره‌برداری از خدمات کلیدزنی مداری در شبکهٔ میان‌کاری مطرح شده است. این سناریو به‌دلیل ساختار شبکهٔ میان‌کاری 3GPP-WLAN قابل استفاده نیست.

۲-۱- معماری دسترسی

براساس سناریوهای دوم و سوم نیز دو حالت دسترسی خاص در شبکهٔ میان‌کاری 3GPP-WLAN مطرح می‌شود که عبارتند از:

Direct IP Access: این دسترسی مبتنی‌بر سناریوی دوم طراحی‌شده است. همان‌طور که در شکل نشان داده شده است،کاربر در این دسترسی، خدمات ترافیکی خود را از نهاد WLAN AN دریافت می‌کند؛ ولی سیگنالینگ این نوع دسترسی توسط شبکهٔ 3GPP کنترل می‌شود. باید توجه داشت که در این دسترسی کاربر مجاز به بهره‌برداری از خدمات PS شبکهٔ 3GPP نیست، برای مثال کاربر فقط می‌تواند خدماتی مانند اینترنت را از نهاد WLAN AN دریافت کند؛ ولی کنترل دسترسی، حسابرسی و هزینه توسط 3GPP HomeNetwork موردبررسی قرار می‌گیرد.

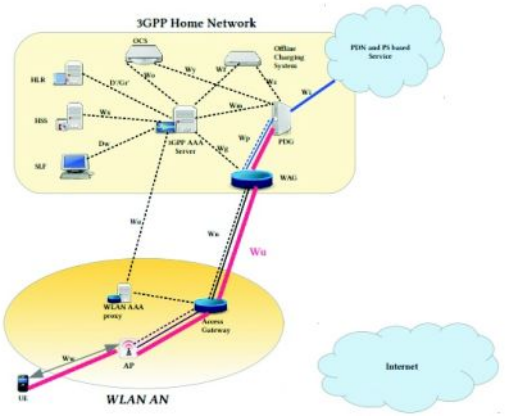
IP Access 3GPP: این دسترسی مبتنی‌بر سناریوی سوم طراحی شده است. همان‌طور که در شکل ۲ نشان داده شده است، کاربر در این دسترسی خدمات ترافیکی خود را از نهاد PDG[2] از شبکهٔ 3GPP دریافت می‌کند و سیگنالینگ این نوع دسترسی هم توسط شبکهٔ 3GPP کنترل می‌شود. درواقع این نوع دسترسی برای ارائهٔ خدمات PS شبکهٔ 3GPP طراحی شده است.



شکل ۱. معماری دسترسی Direct IP Access [۴][۵]

[1] Packet Switch

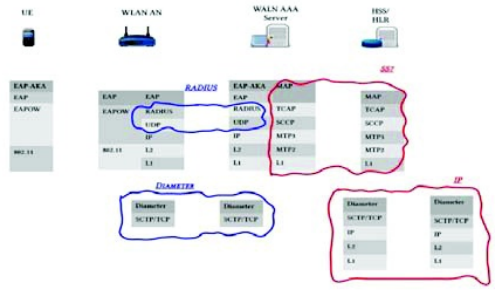
[2] Packet Data Gateway



شکل ۲. معماری دسترسی 3GPP IP Access [۴][۶]

۲-۲- پشتهٔ پروتکلی

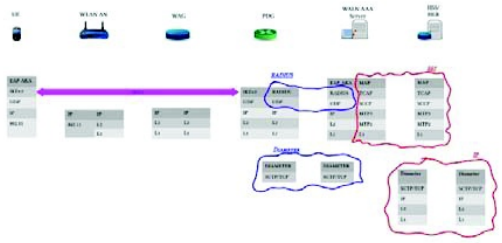
در دسترسی Direct IP Access براساس سناریوی دوم میان‌کاری و شکل ۱ برای داده‌های سیگنالینگ چهار نهاد اصلی به نام‌های UE [1], WLAN AN [2], 3GPP AAA Server [3] HSS/HLR [4] وجود دارد که براساس ساختار معماری در دسترسی Direct IP Access و این نهادها پشتهٔ پروتکلی این نوع دسترسی طراحی می‌شود. پشتهٔ پروتکلی طراحی‌شده در شکل ۳ نشان داده شده است.

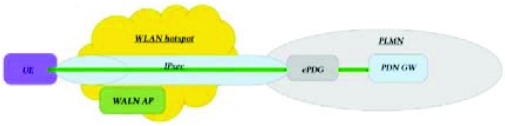


شکل ۳. پشتهٔ پروتکلی دسترسی Direct IP Access [۷][۸][۹]

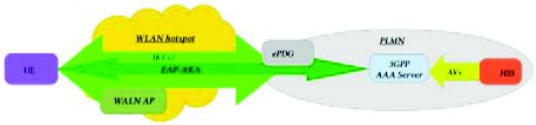
در دسترسی 3GPP IP Access که براساس سناریوی سوم و شکل ۲ برای داده‌های سیگنالینگ نیز شش نهاد اصلی به نام‌های UE و WLAN AN, 3GPP AAA Server و PDG, HSS/HLR WAG وجود دارد. در ساختار معماری دسترسی 3GPP IP Access علاوه‌بر لایه‌های پشتهٔ پروتکلی نیز همان‌طور که در شکل‌های ۶ و ۵ نشان داده شده است، یک تونل توسط رابط Wu وجود دارد. برای داده‌های سیگنالینگ این تونل از پروتکل IKEv2 و برای داده‌های ترافیکی نیز از پروتکل IPSec استفاده می‌کند.

شکل ۴. پشتهٔ پروتکلی دسترسی 3GPP IP Access [5][7][9]





شکل ۵. انتقال داده در پروتکل EAP-AKA با استفاده از IPSec [۱۰]



شکل ۶. احراز اصالت در پروتکل EAP-AKA با استفاده از IKEv2 [10]

۳- چارچوب EAP

EAP یک پروتکل نیست؛ بلکه چارچوبی برای توسعهٔ پروتکل‌های احراز اصالت است که براساس پروتکل‌هایی که در این چارچوب قرار می‌گیرند، روش‌های EAP را ایجاد می‌کنند.EAP در سال ۲۰۰۴ توسط مرجع استانداردسازی IETF در استاندارد RFC 3748 معرفی شد [۲]. چارچوب EAP امکان توسعهٔ پروتکل‌های احراز اصالت را فراهم و سه ساز وکار امنیتی متفاوت را کنار یکدیگر ارائه می‌کند که عبارتند از:

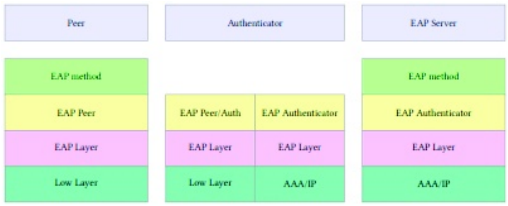
زیرساخت گواهی‌نامه و محدودهٔ خاصی از پروتکل‌های احراز اصالت مانند: (U)SIM، مراکز احراز اصالت و پروتکل‌های تعریف‌شده برای 3GPP .

پروتکل‌های AAA تعریف‌شده برای IETF.

پروتکل‌های امنیتی مخصوص لایهٔ پیوند، مانند: پروتکل‌های تعریف‌شده برای WLAN مثل IEEE 802.11i.

---

1 User Equipment
2 WLAN Access Network
3 3GPP Authentication, Authorization and Accounting Server
4 Home Subscriber Server/Home Location Register



شکل ۷. ساختار کلی چارچوب EAP [۲]

ساختار کلی این چارچوب در شکل ۷ نشان داده شده است [۱۱]. همان‌طور که در شکل ۷ نشان داده شده است EAP با معماری پنج‌لایه نشان داده شده است.

۳-۱- پروتکل EAP-AKA

پروتکل EAP-AKA یکی از روش‌های مطرح‌شده برای چارچوب EAP است که در سال ۲۰۰۶ توسط نهاد استانداردسازی IETF در استاندارد RFC 4187 معرفی شد [۱۲].

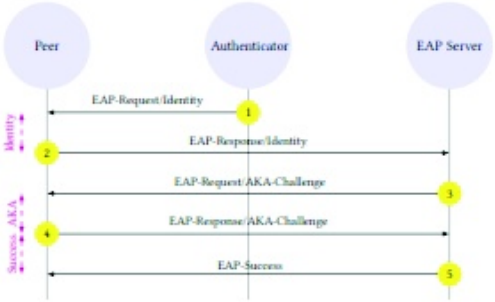
در شکل ۷ سه نهاد مطرح شده است که عبارتند از:

Peer: به‌عنوان کاربر که پاسخ‌دهنده به درخواست‌ها و چالش‌هاست.

Authenticator: به‌عنوان شروع‌کنندهٔ پروتکل و عامل میانی برای رله پیام‌هاست.

EAP Server: نهاد مدیریتی و مطرح کننده درخواست‌ها و چالش‌هاست.

ساختار کلی پروتکل EAP-AKA به‌صورت شکل ۸ است.



شکل ۸. پروتکل EAP-AKA [۱۱]

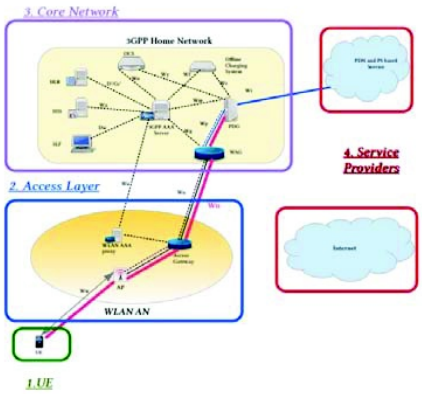
۳-۲- ساختار پروتکل EAP-AKA

برای دسترسی به خدمات شبکهٔ میان‌کاری 3GPP-WLAN توسط هر یک از دسترسی‌های Direct IP Access و 3GPP IP Access ابتدا کاربر باید خود را توسط پروتکل EAP-AKA به‌عنوان مشترک مجاز در محدودهٔ WLAN معرفی کند؛ به همین دلیل تحلیل کارایی و امنیت این پروتکل در روند اجرای دسترسی به شبکه بسیار حائز اهمیت است.

در این بخش ابتدا ضعف‌های شبکهٔ میان‌کاری 3GPP-WLAN به‌صورت کلی دسته‌بندی می‌شوند؛ سپس براساس همین دسته‌بندی جایگاه تحلیل پروتکل EAP-AKA تعیین می‌شود.

در ادامه به بررسی پروتکل‌های مطرح شده برای جبران ضعف‌های EAP-AKA پرداخته می‌شود.

همان‌طور که در شکل ۹ نشان داده شده است می‌توان از نظر امنیتی، دسترسی کاربر به شبکه را به چند قسمت اصلی تقسیم کرد که عبارتند از:



شکل ۹. بخش‌های معماری شبکه میان‌کاری شبکه 3GPP-WLAN ازنظر امنیتی

بخش اوّل: در محدودهٔ UE که بیان‌کنندهٔ تجهیزات کاربر برای اتصال به شبکه است که شامل UICC[1] و ME[2] است.

بخش دوم: لایهٔ دسترسی کاربر به شبکه؛ در این بخش واسطه‌های برقرارکنندهٔ ارتباط UE با شبکه وجود دارد، که همان‌طور که در شکل ۹ نشان داده شده است، این بخش شامل رابط Ww، نهاد WLAN AN و رابط‌های WLAN AN با شبکهٔ شامل رابط‌های Wa و Wu است.

بخش سوم: محدودهٔ هستهٔ شبکه و نهادهای درونی آن است.

بخش چهارم: فراهم‌کنندهٔ خدمات که این بخش شامل نهادهای اینترنت، اینترانت و یا PDN[3] است.

---

[1] Universal Integrated Circuit Card
[2] Mobile Equipment
[3] Packet Data Network

۳-۳- معرفی ضعف‌های امنیتی پروتکل EAP-AKA

با توجه به تقسیم‌بندی امنیت دسترسی کاربر به شبکه، ضعف‌های پروتکل احراز اصالت و توافق کلید در بخش دوم (جایی که شایع‌ترین حملات صورت می‌گیرد) قرار دارد. برای بررسی ضعف‌های پروتکل EAP-AKA می‌توان به موارد زیر اشاره کرد.

۱. **افشای شناسهٔ کاربر:** کاربر در پاسخ به درخواست شناسه، شناسه دائم و یا موقت خود را در قالب مشخصی برای شبکه ارسال می‌کند. در این صورت یک مهاجم غیرفعال با استراق سمع این پیام می‌تواند به این شناسه‌ها دست یابد؛ همچنین یک مهاجم فعال با توانایی ایجاد یک WLAN AN جعلی، توانایی اجرای درخواست شناسه، برای به‌دست‌آوردن هویت دائمی کاربر را دارد؛ به‌گونه‌ای که این شناسه را به دست آورد.

۲. **مصرف پهنای باند اضافی:** در روند اجرای پروتکل، دو مرتبه به کاربر درخواست شناسه ارائه داده می‌شود.

i. در مرحلهٔ دوم توسط WLAN AN برای اتصال به شبکهٔ WLAN این پیام در قالب پروتکل EAP تحت پیام EAP Request/Identity ارسال می‌شود و کاربر در مرحلهٔ سوم، شناسه خود را در قالب NAI[1] و پروتکل EAP تحت پیام EAP Response/Identity برای شبکه ارسال می‌کند.

ii. در مرحلهٔ هفتم توسط شبکهٔ 3GPP به‌وسیله نهاد AAA Server در قالب پروتکل EPA-AKA تحت پیام EAP Request/AKA-Identity ارسال می‌شود. این درخواست به این دلیل است که شبکهٔ 3GPP به شناسه دریافتی در مرتبه اول اعتماد کامل ندارد. کاربر در مرحلهٔ نهم این امر، شناسهٔ هویت خود را در قالب پروتکل EPA-AKA تحت پیام EAP Response/AKA-Identity برای شبکه ارسال می‌کند. این امر باعث افزایش پهنای باند مصرفی و ایجاد سربار به شبکه می‌شود.

۳. **مقدار SQN[2]:** در روند اجرای پروتکل شبکه برای ایجاد هم‌زمانی و تازگی پیام بین UE و شبکه، از یک دنباله در مرحلهٔ چهاردهم در پیام AUTN استفاده می‌شود. UE پس از دریافت این مقدار بررسی می‌کند آیا این مقدار در محدودهٔ مناسب قرار دارد یا نه؛ اگر این مقدار در محدودهٔ نباشد، پس UE یک درخواست برای انجام فرایند هم‌زمانی به شبکه ارسال می‌کند که AAA Server این پیام را به HSS ارائه دهد و باعث تولید مقدار SQN جدید شود که این امر باعث ایجاد سربار به شبکه می‌شود.

۴. **حملهٔ فردی در میان:** سناریوی حملهٔ فردی در میان براساس ربودن نشست و اطلاعات کاربر هنگام برقراری ارتباط است. برای جلوگیری از این حمله باید از همان ابتدای ارتباط، حفاظت لایهٔ فیزیکی با سازوکارهای رمزنگاری صورت گیرد؛ در روش‌های مبتنی‌بر EAP (مانندEAP-AKA) به‌دلیل نداشتن حفاظت لایهٔ فیزیکی چنین حمله‌ای امکان‌پذیر است[۱۳][۱۴]. برای جلوگیری از این حمله باید روش‌های حفاظت داخلی و یا حفاظت خارجی مانند روش PEAP اعمال شود [۱۲].

۵. **ارائهٔ خدمات همزمان**: برای یک مشترک در چندین دستگاه متفاوت با خدمات گوناگون؛ شبکهٔ میان‌کاری 3GPP-WLAN دارای خدمات گوناگونی است؛ به‌گونه‌ای که اگر کاربر بخواهد از این خدمات استفاده کند نیاز است. علاوه‌بر اجرای فرایند احراز اصالت اولیه در شبکهٔ 3GPP برای برخی از خدمات احراز اصالت مجزایی داشته باشد. حال اگر فردی بخواهد از یک پروفایل مشترک در چند دستگاه مجزا خدمات متفاوت درخواست کند، به‌دلیل آنکه ساختار پروتکل EAP-AKA دستگاه‌گرا (مبتنی‌بر یک دستگاه) است؛ پس در روند احراز اصالت سربار زیادی به شبکه تحمیل می‌شود؛ پس پروتکل EAP- AKA برای ارائه این خدمات ناکارآمد است[۱۵].

۴- مروری بر کارهای انجام‌شده

ضعف‌های امنیتی و کارایی مطرح شده بر روی پروتکل EAP-AKA باعث شد پروتکل‌هایی پیشنهاد شود که این ضعف‌ها را جبران کنند. اغلب این پروتکل‌های پیشنهادی

[1] Network Access Identifier

[2] Sequence Number

مبتنی‌بر ساختار ECDH [1] است که از سامانهٔ رمزنگاری متقارن و نامتقارن استفاده می‌کنند[۱۶][۱۷][۱۸][۱۹].

۱. **پروتکل EAP-FAKA:** این پروتکل مبتنی‌بر پروتکل EAP-AKA طراحی‌شده است؛ ولی برای حفاظت شناسه از ساختار ECDH به همراه سامانهٔ رمزنگاری کلید متقارن و پروتکل EAP استفاده می‌کند. در برخی از پروتکل‌های ارائه‌شده برای جبران برخی از ضعف‌های EAP-AKA از قبیل حفاظت شناسهٔ دائم کاربر در برابر استراق سمع و یا سرقت شناسه هنگام ارسال از ساختار پروتکل ترکیبی ECDH استفاده می‌شود. پروتکل ECDH ترکیبی از پروتکل دیفی-هلمن و روش خم بیضوی است. استفاده از ECDH باعث می‌شود که کلید مورد نظر برای حفاظت داده‌ها به‌صورت توافقی بین کاربر و شبکه با استفاده از روش توافق کلید دیفی-هلمن و مبتنی‌بر روش محاسباتی خم بیضوی ایجاد شود. در این روش قبلاً برای هر یک از طرفین کلید عمومی/خصوصی و محدودهٔ خم در نظر گرفته شده است که طرفین با انتخاب یک مقدار تصادفی به کلید می‌توانند به کلید توافقی دست پیدا کنند.

این پروتکل دارای دو اشکال عمده است [۱۹].

i. در پروتکل EAP-FAKA، روند درخواست و ارسال شناسه مبتنی‌بر ساختار ECDH و استفاده از کلید عمومی شبکه و کلید خصوصی کاربر است؛ پس برای اجرای این روند، کاربر باید مجموعه‌ای از کلید عمومی‌های تمامی AAA Server های شبکه‌ها را در برداشته باشد که نیازمند ذخیره‌سازی این اطلاعات در UICC است؛ چون امنیت احراز اصالت باید مبتنی‌بر UICC باشد و از طرفی برای استفاده از خدمات با وجود توسعهٔ شبکه‌ها نیازمند تعویض و یا به‌روزرسانی UICC است؛ این عوامل باعث ایجاد ضعف کارایی و امنیتی در شبکه می‌شود.

ii. بررسی پاسخ چالش، صدور پیام موفقیت و تخصیص کلید نهایی توسط نهاد WAAA (یا همان AAA proxy) انجام می‌گیرد، این امر باعث می‌شود که اختیارات بررسی پروتکل از نهاد درون‌هستهٔ شبکه‌ای AAA Server به نهاد بیرون‌هستهٔ شبکه‌ای AAA Proxy سپرده شود، که این امر یک مشکل امنیتی است.

۲. **پروتکل SFR [2]:** این پروتکل برای جبران ضعف‌های امنیتی در ساختار پروتکل احراز اصالت مجدد ـ سریع در شبکهٔ میان‌کاری 3GPP-WLAN ارائه شده است. در این پروتکل فقط با افزودن پارامترهای امنیتی اضافی سعی در بالابردن سطح امنیت است؛ ولی همین کار باعث کاهش کارایی می‌شود. باید توجه داشت در میان‌کاری یکی از مهم‌ترین مسائل، بالابردن امنیت با حفظ کارایی است؛ چون اگر کارایی کاهش یابد باعث عدم موفقیت در ارائه خدمات می‌شود [۲۰].

۳. یکی از موارد مهم در میان‌کاری بحث جایگشت است. روند احراز اصالت و توافق کلید در جایگشت بین شبکهٔ سلولی و میان‌کاری باید به‌گونه‌ای باشد که کیفیت ارائهٔ خدمات در هر یک از شبکه‌ها کاهش نیابد. در برخی از روش‌های ارائه‌شده برای کاهش زمان فرایند احراز اصالت و موفق کلید برای شبکه میان‌کاری باعث ایجاد سربار زیادی به شبکه سلولی می‌شود [۱۸]؛ از طرفی اگر بخواهیم چنین مدلی داشته باشیم که در آن بخشی از روند احراز اصالت در شبکهٔ میان‌کاری 3GPP-WLAN از طریق کانال شبکه سلولی انجام گیرد، پس باید معماری UICC به‌گونه‌ای باشد که بین اطلاعات شبکهٔ میان‌کاری و شبکه سلولی اشتراکی وجود داشته باشد؛ درواقع معماری UICC باید از مدل شکل ۱۰ پیروی کند که در این صورت در UICC مربوط به شبکه سلولی در معرض آسیب‌پذیری توسط حملات مربوط به شبکه میان‌کاری قرار می‌گیرد.

شکل ۱۰. معماری UICC [۲۱]

[1] Elliptic Curve Diffie Hellman

[2] Selection Forward Routing

۴. **پروتکل SEMMAP**[1]: این پروتکل برای ارائهٔ خدمات در یک پروفایل مشترک در دستگاه‌های مختلف برای خدمات گوناگون به‌صورت همزمان در یک شبکه است. در این پروتکل سطح امنیت مبتنی‌بر EAP است.

چالش مطرح شده در این پروتکل یکی از جذاب‌ترین خدمات در میان‌کاری است. همان‌طور که بیان شد برای ارائهٔ خدمات شبکه میان‌کاری3GPP-WLAN از پروتکل EAP-AKA استفاده می‌شود که یکی از ویژگی‌های این پروتکل، دستگاه-گرابودن است؛ یعنی اینکه کاربر برای دریافت خدمات در هر دستگاه جداگانه باید روند احراز اصالت پروتکل EAP-AKA را به‌صورت مجزا انجام دهد؛ ولی در پروتکل SEMMAP این امکان فراهم شده است که فقط با اجرای یک‌بار پروتکل SEMMAP کاربر بتواند خدمات گوناگون را در دستگاه‌های مجزای خود دریافت کند. بر همین اساس پروتکل EAP-AKA قادر به برآورده‌کردن سازوکار ارائه‌شده در پروتکل SEMMAP نیست. البته پروتکل SEMMAP علاوه‌بر اینکه ضعف‌هایی همچون عدم حفاظت شناسه کاربر، نداشتن پیام Notification برای اطلاع‌رسانی از وضعیت اجرای پروتکل به طرفین، نداشتن پیام تخصیص کلید بین WLAN AN و UE در انتهای پروتکل دارد، به دلیل نیاز به ایجاد هماهنگی برای اجرای این پروتکل در هسته شبکه باعث بالارفتن پیچیدگی کنترل دسترسی و مدیریت هزینه در هستهٔ شبکه به‌صورت روی خط می‌شود[۱۵].

۵. **پروتکل EAP-AKA'**: مرجع استانداردسازی 3GPP برای اجرای روند احراز اصالت و توافق کلید در شبکهٔ میان‌کاری3GPP-non3GPP پروتکل EAP-AKA' را معرفی کرده است؛ این پروتکل حالت تکامل‌یافته پروتکل EAP-AKA است؛ ولی مانند EAP-AKA دارای ضعف حفاظت شناسه است[۲۲] [۲۳].

پروتکلEAP-AKA' از پروتکل‌های استاندارد IETF است که در سری RFC5448 است[۲۴]. برخی از ویژگی‌های پروتکلEAP-AKA' به شرح زیر است:

i. در احراز اصالت کامل برای EAP-AKA'، بردارهای احراز اصالت UMTS و کلیدهای CK و IK تولید می‌شوند. البته کلیدهای CK و IK در EAP-AKA' به‌صورت مستقیم مورد استفاده قرار نمی‌گیرد؛ بلکه جفت‌کلیدهای (CK' و IKs')که اشتقاق‌یافته از جفت کلیدهای (CK و IK) است برای شناسهٔ دسترسی به شبکه به کار می‌روند.

ii. بیشتر کلیدهای EAP که اشتقاق‌یافته از (CK' و IKs') می‌باشند، سریع‌تر از جفت کلید (CK و IK) هستند.

iii. روش محاسباتی کلیدهای MSK[2]، EMSK[3] و TEKs[4] کلیدهای K_{aut} و K_{encr} نسبت به روش محاسباتی EAP-AKA متفاوت است.

iv. تابع اشتقاق کلیدها بر اساس تابع چکیده‌ساز SHA-256 است، که به‌جای نسخهٔ ضعیف‌تر SHA-1در نظر گرفته شده است.

پروتکل EAP-AKA' همانند پروتکل EAP-AKA ممکن است برای احراز اصالت کامل یا احراز اصالت مجدد سریع مورد استفاده قرار گیرد. همچنین EAP-AKA از همان روش EAP-AKA برای نام مستعار و شناسهٔ احراز اصالت مجدد استفاده می‌کند.

در برخی از روش‌ها برای بهبود پروتکل EAP-AKA در حفاظت شناسه، از ساختار رمزنگاری متقارن استفاده می‌شود. در رمزنگاری متقارن برای حفاظت شناسه باید به این نکته توجه کرد که شبکه هنگام دریافت شناسهٔ رمزشده باید بتواند هویت کاربر را تشخیص دهد به‌گونه‌ای که بتواند کلید محرمانه مشترک را تعیین کند و پس از رمزگشایی هویت کاربر تأیید شود؛ ولی در برخی از روش‌های مطرح‌شده فقط به حفاظت شناسهٔ تأکید شده و تعیین هویت کاربر توسط شبکه مورد توجه قرار نگرفته است، که باعث ناکارآمدی پروتکل می‌شود [۲۵].

۶. در برخی از پروتکل‌ها برای استفاده از سامانهٔ رمزنگاری متقارن در روند احراز اصالت اولیه

[1] Secure and Efficient Multi-Device and Multi-Service Authentication Protocol

[2] Master Session Key
[3] Extended Master Session Key
[4] Transient EAP Keys

به‌دلیل عدم تبادل و یا توافق کلید بین طرفین، کاربر مجبور است دو راه‌کار را پیش‌رو بگیرد:

i. حالت نخست، آنکه برای رمزنگاری اولیه جهت حفاظت شناسه از کلید محرمانهٔ خود به‌صورت مستقیم استفاده کند، که در این صورت خلاف معیارهای امنیتی در شبکه است؛ چون به‌هیچ‌وجه نباید از این کلید به‌صورت مستقیم استفاده شود.

ii. حالت دوم، کاربر با استفاده از مقادیر تصادفی از کلید محرمانهٔ خود مشتق بگیرد و با استفاده از کلید جدید رمزنگاری انجام دهد؛ در این صورت کاربر باید توانایی تولید یک مقدار تصادفی مناسب را داشته باشد.

در هر یک از حالات مطرح شده، کاربر هنگام ارسال هویت، خود را در روند احراز اصالت اولیه، به‌صورت رمزشده ارسال می‌کند. نکته‌ای که وجود دارد، این است که شبکه چه‌طور بتواند هویت رمزشده کاربر را تعیین کند. برای رفع این مشکل کاربر مجبور است دو راه‌کار در پیش‌گیرد:

i. کاربر از هویت ثانویه استفاده کند. این هویت می‌تواند مبتنی‌بر ID و یا گواهی‌نامه ازپیش‌تعیین‌شده باشد؛ در این صورت امنیت هویت کاربر در شبکه از سطح امنیت UICC به سطح امنیت ID و یا گواهی‌نامه کاهش می‌یابد که این امر خود نوعی ضعف و آسیب‌پذیری امنیتی است.

ii. کاربر از قبل یک هویت ثانویهٔ ثابت غیر از IMSI[1] با شبکه توافق کرده باشد؛ در این صورت در روند احراز اصالت اولیه، کاربر هیچ‌گاه مقدار IMSI را ارسال نمی‌کند؛ ولی در هر مرتبه از احراز اصالت اولیه یک مقدار ثابت را ارسال می‌کند که این امر خود نوعی ضعف امنیتی است که در بخش بعدی به آن پرداخته می‌شود.

۷. **تحلیل‌های صوری:** برخی از پروتکل‌های پیشنهادی برای تحلیل از روش‌های صوری بهره‌گرفته‌اند که به‌دلیل ضعف در فرضیات مسأله، پروتکل طراحی‌شده، امن در نظر گرفته شده است و برای اجرای روند احراز اصالت در شبکه پیشنهاد شده‌اند. اگرچه روش‌های تحلیل صوری به‌نوبهٔ خود جزء معتبرترین روش‌های بررسی امنیت پروتکل‌ها می‌باشند؛ ولی در این تحلیل‌ها یا فرضیات درست در نظر گرفته نشده است و یا ویژگی‌های شبکه برای پروتکل در نظر نگرفته نمی‌شود؛ بر همین اساس ممکن است پروتکلی از نظر برخی از تحلیل‌های صوری، امن باشد؛ ولی به‌دلیل ویژگی‌های شبکه؛ ممکن است آسیب‌پذیر باشند. پس پروتکل‌های که مبتنی‌بر تحلیل صوری ارائه می‌شوند تا قبل از اینکه مبتنی‌بر معیارهای شبکه مورد بررسی قرار نگیرند، به‌طور کامل قابل اطمینان نیستند[۲۶][۲۷][۲۳].

۸. **پروتکل مبتنی‌بر کلید عمومی/خصوصی:** در برخی از روش‌های ارائه‌شده برای حفاظت شناسه کاربر در روند احراز اصالت از ساختار کلید عمومی/خصوصی استفاده می‌شود. در حالت کلی برای استفاده از این ساختار دو حالتِ استفاده از گواهی‌نامه یا ID وجود دارد. البته هر یک از روش‌ها محدودیت‌هایی دارند. محدودیت‌های استفاده از ساختار مبتنی‌بر گواهی‌نامه عبارتند از:

i. در این ساختار تولید کلید بر عهده[2] PKI است؛ پس نیاز به یک شخص سوم مورد اطمینان است.

ii. امنیت هویت کاربر مبتنی‌بر امنیت گواهی‌نامه‌های ذخیره‌شده برای کاربر است.

iii. محدودیت عملیات به‌روزرسانی و ابطال گواهی‌نامه‌ها براساس نیاز کاربر و شبکه مطرح است؛ چون یکی از مهم‌ترین مسائل در ساختار مبتنی‌بر گواهی‌نامه ابطال و به‌روزرسانی گواهی‌نامه‌ها برای ایجاد امنیت و دریافت خدمات به‌صورت تضمین‌شده است.

iv. محدودیت در انتشار کلیدها برای برقراری نشست. کاربر برای بهره‌برداری از خدمات مبتنی‌بر گواهی‌نامه نیازمند است که این گواهی‌نامه را از مرکز معتبر دریافت کند. برای دریافت معتبر نیاز به دسترسی به کانال امن است؛ به‌گونه‌ای که کاربر بتواند به گواهی‌نامهٔ دریافتی اطمینان کامل کند و همچنین بتواند هر زمان که لازم باشد و به تعداد مورد نیاز گواهی‌نامه دریافت کند.

[1] International Mobile Subscriber Identity

[2] Public-Key Infrastructure

v. ساختار بهره‌برداری و دسترسی به گواهی‌نامه باید به‌گونه‌ای باشد که کاربر نیازی به اتلاف وقت نداشته باشد.

vi. روش‌های معتبر و کارآمد برای ابطال و به‌روزرسانی گواهی‌نامه وجود داشته باشد.

vii. مسألهٔ ذخیره‌سازی گواهی‌نامه‌ها در UICC یا ME و استفاده مجدد از آن‌ها مطرح است.

محدودیت‌ها در روش مبتنی‌بر ID عبارتند از:

i. برای ایجاد یک‌پارچگی و زبان مشترک در بین شبکه‌های گوناگون نیاز به یک قالب استاندارد جهت ایجاد و ارسال شناسه‌های کاربر (ID) است. همچنین به‌دلیل محدودیت‌های ساختاری ID به‌طور معمول از این ساختار برای استفاده در شناسهٔ کمکی کاربر در تعیین هویت اولیهٔ کاربر به شبکه استفاده می‌شود [۲۸].

ii. شناسهٔ ID کاربر باید به‌صورت منحصربه‌فرد و قابل ره‌گیری در شبکه باشد.

iii. شناسه دارای دو حالت کلی است:

- شناسهٔ مبتنی‌بر هویت کاربر، مانند IMSI در شبکهٔ تلفن همراه منحصربه‌فرد است.
- شناسهٔ مبتنی‌بر هویت UE مانند IMEI در شبکهٔ تلفن همراه، منحصربه‌فرد است،

بر این اساس باید مشخص شود که هویت مشترک مبتنی‌بر کدام‌یک از حالت بالاست. اگر هویت مبتنی‌بر IMSI باشد هویت مشترک مبتنی‌بر شخص دارنده UICC می‌شود؛ ولی اگر هویت مبتنی‌بر IMEI باشد، هویت مشترک مبتنی‌بر دستگاه در اختیار مشترک می‌شود. حالت دیگری وجود دارد که هویت مبتنی‌بر IMSI و IMEI باشد که در این صورت هویت مشترک مبتنی‌بر قرارگرفتن UICC در دستگاه با IMEI خاص است.

۹. **پروتکل مبتنی‌بر ECDH:** یکی از روش‌های مطرح جهت جایگزینی پروتکل EAP-AKA، پروتکل‌های ارائه‌شده مبتنی‌بر ساختار ECDH است که برای حفاظت شناسهٔ کاربر از ساختار کلید متقارن و برای انتقال داده‌های ترافیکی به‌صورت امن از ساختار خم بیضوی بهره می‌گیرند. در این پروتکل به‌طور معمول از مهر زمانی برای تازگی پیام‌ها استفاده می‌شود. در این پروتکل دو اشکال عمده وجود دارد:

i. نخست: شناسهٔ کاربر مبتنی‌بر ID و حفاظت‌شده است؛ ولی در برابر حملات ره‌گیری ضعیف است؛ چون شناسهٔ کاربر به‌صورت ثابت ارسال می‌شود.

ii. دوم: برای تولید مهر زمانی نیاز به تنظیم زمان مشترک در شبکه است؛ که این امر باعث ایجاد سربار به شبکه می‌شود [۱۶].

در بحث پروتکل‌های مبتنی‌بر ECDH باید توجه کرد که امنیت کلیدهای کاربر مبتنی‌بر چه ساختاری است؛ چون ذخیره‌سازی این کلیدها به دو صورت امکان‌پذیر است:

i. ذخیره‌سازی در UICC، در این صورت باید زیرساخت UICC قابلیت این ذخیره‌سازی را داشته باشد؛ همچنین باید الگوریتم‌های محاسباتی موجود در UICC از قبیل f_iها تغییر کنند و یا آنکه الگوریتم‌های مناسب به همراه دسترسی در اختیار ME قرار داده شود.

ii. ذخیره‌سازی در ME، در این صورت باید کلیدها از طریق گواهی‌نامه دریافت شوند؛ در این حالت علاوه‌بر اینکه باید الگوریتم‌های مناسب به همراه دسترسی در اختیار ME قرار داده شود، امنیت کاربر از سطح UICC به گواهی‌نامه کاهش می‌یابد.

۱۰. **احراز اصالت گروهی:** در ساختار پروتکل‌های احراز اصالت برای بهبود کارایی در شبکه از پروتکل‌های احراز اصالت گروهی استفاده می‌شود. در ساختار احراز اصالت گروهی ابتدا یک گروه ازپیش‌تعیین‌شده ایجاد می‌شود که روش تشکیل این گروه می‌تواند مبتنی‌بر مکان و یا ... باشد. برای بهبود کارایی شبکه در روند احراز اصالت از بین اعضای تشکیل‌دهنده گروه یک سرگروه تعیین می‌شود که این امر می‌تواند به‌صورت تصادفی و یا از پیش تعیین‌شده باشد. درروند احراز اصالت گروهی ابتدا سرگروه باید روند کلی احراز اصالت را طی کند پس از آن سایر اعضای گروه به اعتماد احراز اصالت سرگروه و عضویت در گروه مد نظر نیز روند احراز اصالت ثانویه را طی می‌کنند؛ که این روند احراز اصالت ثانویه، باعث بهبود کارایی روند احراز اصالت کاربران در سطح شبکه می‌شود. یکی

از این پروتکل‌ها، پروتکل SE-AKA مبتنی‌بر ساختار ECDH و زیرساخت PKI است. این پروتکل باعث بالارفتن کارایی در روند احراز اصالت و توافق کلید می‌شود؛ اما دارای ضعف‌هایی در تعیین گروه‌های جدید، ضعف‌های مربوط به ساختار ECDH و همچنین آسیب‌پذیری در برابر حملات ره‌گیری است [۲۹].

۵- نتیجه‌گیری

استفاده از میان‌کاری یکی از مناسب‌ترین روش‌ها برای توسعه ارایه خدمات در شبکه‌های نسل جدید است. از میان فناوری‌های مطرح‌شده برای میان‌کاری با شبکه‌های مخابراتی نسل جدید، میان‌کاری 3GPP-WLAN به‌عنوان مناسب‌ترین روش میان‌کاری در نظر گرفته شده است. اگر چه مرجع استانداردسازی 3GPP پروتکل EAP-AKA را برای تأمین امنیت احراز اصالت و توافق کلید مطرح کرده است؛ ولی این پروتکل دارای ضعف‌های امنیتی است که در این مقاله به برخی از آنها اشاره شد. با توجه به معماری شبکهٔ میان‌کاری 3GPP-WLAN که در شکل ۱۰ نشان داده شده است، پیشنهاد می‌شود به‌منظور بهبود امنیت در این شبکه موارد زیر مورد ارزیابی قرار گیرد:

۱. یکی از مهم‌ترین مسائل در شبکه‌های میان‌کاری واگذاری کاربر بین شبکه 3GPP و WLAN و بالعکس است. برهمین اساس پیشنهاد می‌شود پروتکل احراز اصالت و توافق کلید سبک وزنی در چارچوب EAP طراحی شود که علاوه‌بر امنیت قابل قبول در هنگام واگذاری کاربر، کم‌ترین سربار و از بین رفت بسته‌ها را داشته باشد. همچنین پیشنهاد می‌شود که پروتکل‌های طراحی شده از نظر کارایی و امنیت با سایر پروتکل‌ها مقایسه شود.

۲. برقراری ارتباط بین eNodeB و WLAN AN با هسته شبکه از دیگر بخش‌های مهم در شبکه LTE و میان‌کاری است که این ارتباط توسط پروتکل‌های Diameter وRADIUS [1] صورت می‌پذیرد. پیشنهاد می‌شود این دو پروتکل از نظر کارایی و امنیت مورد ارزیابی قرار گیرند و در صورت امکان برای جبران ضعف‌های آن‌ها در شبکه پروتکل‌هایی طراحی شود.

۳. همان‌طور که بیان شد، در دسترسی 3GPP IP Access کاربر خدمات ترافیک خود را مبتنی‌بر تونل IPSec دریافت می‌کند. پیشنهاد می‌شود پروتکل IPSec از نظر کارایی و امنیت در شبکه میان‌کاری 3GPP-WLAN مورد ارزیابی قرار گیرد و در صورت وجود ضعف امنیتی و کارایی، پروتکل‌هایی پیشنهاد شود.

۴. از آنجا که یکی از معیارهای ITU برای شبکهٔ نسل جدید انتقال داده با نرخ بالاست و کاربر در شبکهٔ میان‌کاری 3GPP-WLAN قادر است خدمات خود را توسط هریک از شبکه‌های سلولی و WLAN دریافت کند، پیشنهاد می‌شود، مدلی برای ارائهٔ دریافت خدمات در شبکهٔ میان‌کاری 3GPP-WLAN ارائه شود کاربر قادر باشد خدمات خود را به‌صورت هم‌زمان از شبکه‌های سلولی و WLAN دریافت کند؛ این امر باعث افزایش نرخ انتقال داده کاربر در شبکه می‌شود.

۵. از آنجا که عمل واگذاری کاربر در شبکهٔ میان‌کاری 3GPP-WLAN باید به‌صورت نرم‌افزاری صورت گیرد، پیشنهاد می‌شود نرم‌افزارهایی طراحی شود که علاوه‌بر امنیت قابل قبول نیز سناریوی پنجم میان‌کاری را به‌صورت کامل انجام دهد.

۶. یکی دیگر از خدمات مهم در شبکه‌های نسل جدید، ارائهٔ خدمات مبتنی‌بر مکان است. پیشنهاد می‌شود پروتکل‌هایی طراحی شود که عملیات مکان‌یابی و ارائهٔ خدمات به کاربر را با حفظ حریم خصوصی در بهینه‌ترین حالت ممکن انجام دهد. درصورتی‌که ارائهٔ خدمات مبتنی‌بر مکان به‌صورت بهینه انجام گیرد، باعث کاهش سربار شبکه می‌شود.

۶- مراجع:

[1] T. Specification, Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking (3GPP TS 22.234 version 11.0.0 Release 11), vol. 0. 3GPP, 2012.

[2] J. Carlson and H. Levkowetz, Extensible Authentication Protocol (EAP) 3748. IETF, 2004.

[3] 3GPP, Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Feasibility study on 3GPP system to Wireless Local Area Network (WLAN) interworking (3GPP

[1] Remote Authentication Dial In User Service

TR 22.934 version 11.0.0 Release 11), vol. 0. ETSI, 2012.

[4] Y. Xiao, U. S. A. University of Alabama, Y. Pan, U. S. A. Georgia State University, and World, Eds., Security in Distributed and Networking Systems. Security in Distributed and Networking Systems eds. Xiao Yang et al., 2007.

[5] J. Sanchez and M. Thioune, Universal Mobile Telecommunications System (UMTS); LTE; 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (3GPP TS 23.234 version 11.0.0 Release 11), vol. 0. 3GPP, 2012.

[6] 3GPP TS 22.115, "GSM; UMTS; Service aspects; Charging and billing," Version 7.1.0 Release 7, 2007.

[7] V. Garg, Wireless Communications and Networking. Morgan Kaufmann, 2010.

[8] I. Press, H. Lane, and F. Canavero, WiMAX Technology and Network Evolution. Wiley, 2010.

[9] D. Hutchison and J. C. Mitchell, Information Security Theory and Practices Smart Devices, Convergence. Springer, 2008.

[10] C. Mulligan, M. Olsson, S. Rommer, S. Sultana, and L. Frid, SAE and the Evolved Packet Core. 2009.

[11] V. N. Dan Forsberg, Gunther Horn, Wolf-Dietrich Moeller, LTE Security, 2nd ed. John Wiley & Sons, 2012.

[12] J. A. Ericsson and H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA); RFC 4187. IETF, 2006.

[13] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS," in Proceedings of the 3rd ACM workshop on Wireless security, 2004, pp. 90–97.

[14] N. Asokan, V. Niemi, and K. Nyberg, "Man-in-the-Middle in Tunnelled Authentication Protocols," 2002.

[15] J. Huang and C.-T. Huang, "A Secure and Efficient Multi-Device and Multi-Service Authentication Protocol (SEMMAP) for 3GPP-LTE Networks," in 2012 21st International Conference on Computer Communications and Networks (ICCCN), 2012, pp. 1–7.

[16] R. Shankar, K. T. Rajkumar, and P. Dananjayan, "Security enhancement with optimal QoS using ECDH for converged 3G-WLAN system," 2010, pp. 1709–1713.

[17] H. Mun, K. Han, and K. Kim, "3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA," in 2009 Wireless Telecommunications Symposium, 2009, pp. 1–8.

[18] I. El Bouabidi, I. Daly, and F. Zarai, "Secure handoff protocol in 3GPP LTE networks," in Third International Conference on Communications and Networking, 2012, pp. 1–6.

[19] Y. Idrissi, N. Zahid, and M. Jedra, "Security analysis of 3GPP (LTE)—WLAN interworking and a new local authentication method based on EAP-AKA," in …Technology (FGCT), 2012 …, 2012, pp. 137–142.

[20] T. Feng, H. Chen, and J. Ma, "Secure Re-authentication Scheme for 3G-WLAN Integrating Network Based on Protocol Composition Logic," in 2012 International Conference on Computer Science and Service System, 2012, pp. 800–805.

[21] "Use of smart cards in WLAN interworking," 3GPP TSG SA WG3 Secur. – S3#25, no. October, 2002.

[22] T. Specification, Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (3GPP TS 33.402 version 11.4.0 Release 11), vol. 0. 3GPP, 2012.

[23] P. Liu and P. Zhou, "Formal analysis of improved EAP-AKA based on Protocol Composition Logic," in 2010 2nd International Conference on Future Computer and Communication, 2010, pp. V3–86–V3–90.

[24] V. Lehtovirta, Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') ;RFC 5448. IETF, 2009.

[25] L. Wenju, S. Yuzhen, Z. Yan, and W. Ze, "An analysis of the improved EAP-AKA protocol," in 2010 2nd International Conference on Computer Engineering and Technology, 2010, pp. V1–10–V1–13.

[26] X. Li, L. Hao, S. Yang, and J. Li, "Formal Verification of EAP-AKA with Improved Authentication Tests," in 2006 International Conference on Wireless Communications, Networking and Mobile Computing, 2006, pp. 1–4.

[27] X. Li and X. Zhang, "Formal Verification for EAP-AKA Protocol in 3G Networks," in 2009 International Conference on Computational Intelligence and Software Engineering, 2009, pp. 1–4.

[28] L. Wenju, W. Wei, and W. Ze, "An IBE based fast authentication among WLANs for 3G users," in 2010 2nd International Conference on Computer Engineering and Technology, 2010, pp. V1–1–V1–4.

[29] C. Lai, H. Li, R. Lu, and X. (Sherman) Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," Comput. Networks, no. August, Aug. 2013.

محمد رضا گوهره‌یی درجهٔ کارشناسی خود را در رشتهٔ مهندسی برق گرایش الکترونیک از دانشکده فنی مهندسی دانشگاه رازی در سال ۱۳۹۰ درجهٔ کارشناسی ارشد خود را در رشتهٔ مهندسی مخابرات گرایش رمز از دانشگاه صنعتی مالک اشتر در سال ۱۳۹۳ اخذ کرد. تحلیل پروتکل‌های امنیتی، ارتباطی و امنیت در شبکه‌های مخابراتی سیار از جمله زمینه‌های پژوهشی ایشان است.

مجید بیات درجهٔ دکترای خود را در رشته ریاضیات و علوم کامپیوتر از دانشگاه خوارزمی در سال ۱۳۹۳ اخذ کرد. وی در حال حاضر به‌عنوان پژوهش‌گر در دانشگاه خوارزمی و آزمایشگاه تئوری اطلاعات و مخابرات امن دانشگاه شریف (ISSL) مشغول به فعالیت است. شبکه‌های اقتضایی(VANETs)، شبکه‌های هوشمند (Smar Grid)، پروتکل‌های رمزنگاری و امنیت قابل اثبات از جمله زمینه‌های تحقیقاتی ایشان می‌باشد.

علی پاینده درجهٔ کارشناسی ارشد خود را در رشتهٔ مهندسی برق گرایش مخابرات از دانشگاه تربیت مدرس در سال ۱۳۷۳ و همچنین درجه دکترای خود را در رشتهٔ مهندسی مخابرات از دانشگاه خواجه نصیر الدین طوسی در سال ۱۳۸۵ اخذ کرد. وی در سال‌های ۱۳۷۵ تا ۱۳۸۵ به‌عنوان یکی از مدیران انجمن تحقیقات علوم کاربردی ایران بوده است که در زمینه ارتباطات ماهواره‌ای امن فعالیت داشته است. نامبرده 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 می‌باشد.