مجله علمی - پژوهشی " پدافند الکترونیکی و سایبری "

سال سوم، شماره ۴، زمستان ۱۳۹۴، ص ۸۰- ۷۱

پروتکل احراز هویت مجدد امن و سریع برای جابه‌جایی‌های گسترده کاربران در شبکه‌های بی‌سیم 802.1X

علی محمدی[1*]، ناصر مدیری[2]

۱- دانشجوی دکتری مهندسی کامپیوتر، دانشگاه جامع امام حسین(ع)

۲- دانشیار مهندسی کامپیوتر، دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد زنجان

(دریافت:۹۴/۷/۲۶، پذیرش: ۹۴/۱۰/۲۲)

چکیده

تامین امنیت شبکه‌های بی‌سیم، مقارن با حفظ کارآیی، مهم‌ترین موضوع در این شبکه‌ها است. پروتکل احراز هویت نوعی پروتکل رمزنگاری است که وظیفه آن سنجش اعتبار موجودیت‌ها است. موسسه IETF پروتکل‌های امنیتی معتبر ارائه‌شده را قالب استاندارد منتشر می‌کند. در این پژوهش ضمن بررسی پروتکل‌های ارائه‌شده در این حوزه و بیان مشکلات هریک، پروتکل جدیدی برای احراز هویت مجدد براساس استانداردهای IETF (RFC 6696) طراحی و ارائه گردیده است. از جمله مزایای پروتکل پیشنهادی استفاده از رمزنگاری متقارن، توابع رقابت- پاسخ و تابع درهم‌سازی است. به‌منظور ارزیابی جامع امنیتی پروتکل پیشنهادی از تحلیل امنیتی صوری استفاده شده است. همچنین، ارزیابی انجام‌گرفته به‌وسیله ابزار AVISPA نشان می‌دهد که این پروتکل در مقابل حملات متعارف، مقاوم و امن است. نتایج حاصل از ارزیابی محاسباتی پروتکل نیز نشان می‌دهد زمان احراز هویت در پروتکل پیشنهادی فقط ۲۲/۸۵ درصد پروتکل‌های مبتنی بر TLS است. همچنین، از طریق شبیه‌سازی در محیط NS2 نیز نتایج به‌دست‌آمده مورد تایید قرار گرفت.

واژه‌های کلیدی: شبکه‌های بی‌سیم، امنیت شبکه‌های بی‌سیم، شبکه‌های 802.1X، پروتکل EAP، احراز هویت مجدد

۱- مقدمه

با پیشرفت شبکه‌های بی‌سیم و گسترش این شبکه‌ها در سطح جهانی، دستگاه‌های ارسال و دریافت امواج در دو حوزه افزایش پهنای باند و ارسال سیگنال به منطقه تحت پوشش بزرگ‌تر ارتقاء یافتند. در چنین محیط‌هایی، کاربران از دستگاه موبایل جهت دسترسی به انواع سرویس مانند جست‌وجو در اینترنت، VOIP [۱] کنفرانس ویدیویی و برنامه‌های چندرسانه‌ای [۲] استفاده می‌کنند. کاربران ترجیح می‌دهند که سیستمی امن و کارا را در حرکت به نقاط متفاوت تجربه کنند. در زندگی روزمره با استفاده از روش‌های متداول نقل و انتقال مانند کشتی، قطار، مترو و اتوبوس، گره‌های سیار به‌صورت یک توده عظیم با هم حرکت می‌کنند. البته باید توجه داشت که هرکدام عضو یک شبکه با سرویس‌دهنده خاص هستند. IETF[1] مدل AAA[2]، [۶-۳] را برای حل مساله مدیریت امنیت گره‌های سیار ارائه کرد. احراز هویت[3] مهم‌ترین و اولین بخش مدل AAA است، اگر در این مرحله خطایی رخ دهد کل ساختار با مخاطره مواجه می‌شود و درصورتی‌که نفوذی در این مرحله صورت گیرد مکانیزم کنترل‌کننده دیگری وجود ندارد، زیرا خروجی هر مرحله ورودی مرحله بعد است. به‌همین جهت اصولا سرویس‌دهنده جداگانه‌ای برای احراز هویت درنظر گرفته می‌شود. وظیفه این سرویس‌دهنده انجام فرآیند تولید کلید، ذخیره‌سازی یا درهم‌ریزی کلید و درنهایت پخش کلید در بین موجودیت‌های موجود در شبکه است. طی سالیان گذشته، پروتکل‌های مختلفی برای سرویس احراز هویت ارائه گردید. برخی از این پروتکل‌ها تاکنون چندین بار مورد آزمایش قرار گرفته است که منجر به تولید نسخه‌های متعدد در قالب RFC منطبق با استانداردهای IETF شده است. یک خانواده از پروتکل‌های استاندارد در حوزه امنیت شبکه‌های بی‌سیم مربوط به EAP[4] است. در این پژوهش، پروتکلی براساس یکی از استانداردهای EAP طراحی، سپس امنیت و کارآیی آن مورد ارزیابی قرار گرفته است.

* رایانامه نویسنده مسئول: mohammadi@ihu.ac.ir

1- Internet Engineering Task Force
2- Authentication, Authorization, Accounting
3- Authentication
4- Extended Authentication Protocol

در ادامه این مقاله، ابتدا کارهای مرتبط با موضوع پژوهش بیان شده و سپس پروتکل پیشنهادی تشریح گردیده است. در ادامه، ارزیابی پروتکل در دو بخش ارزیابی امنیتی و ارزیابی محاسباتی بیان شده و نتایج حاصل از شبیه‌سازی آورده شده است. نهایتاً نتیجه‌گیری و کارهای آینده بیان شده است.

۲- کارهای مرتبط

بسیاری از پروتکل‌های امنیتی به‌کار گرفته‌شده در شبکه‌های بی‌سیم بر پایه EAP [۹-۷] می‌باشند. از جمله این پروتکل‌ها می‌توان به EAP-TLS[۱] [۸ و ۱۰]، EAP-TTLS[۲] [۱۱]، PEAP[۳] [۱۲]، LEAP[۴] [۱۳ و ۱۴]، EAP-SIM[۵] [۱۵] و EAP-FAST [۱۶] اشاره کرد. همان‌طورکه دیده می‌شود EAP قابلیت ترکیب با زیربرنامه‌ها، توابع داخلی‌ها و سایر پروتکل‌ها را دارد. به‌علاوه ساختار داخلی EAP نیز قابل تغییر است. توابع رمزنگاری EAP ضمن پشتیبانی از ساختار رمزنگاری متقارن، توابع درهم‌ساز و رشته‌های تصادفی، از توابع رمزنگاری نامتقارن و گواهی‌های اعتباری[۶] نیز پشتیبانی می‌کنند. این توابع شامل گواهی‌های دیجیتال، نام کاربران و رمز عبور آن‌ها، نشان‌های[۷] امن و رمزهای SIM می‌باشند که متناسب با شرایط و پیکربندی شبکه مورد استفاده قرار می‌گیرند. برای مثال EAP-TLS، PEAP، EAP-TTLS و EAP-FAS بر مبنای رمزنگاری نامتقارن و گواهی‌های اعتباری کار می‌کنند [۱۷]. ممکن است مدیران و مهندسان از ساختار داخلی پروتکل‌هایی که استفاده می‌کنند آگاه نباشند. به‌عنوان مثال پروتکل‌های مبتنی بر رمزنگاری نامتقارن اگرچه در حالت کلی امنیت بالایی را فراهم می‌کنند و تنها ممکن است در موارد خاصی آسیب‌پذیر باشند؛ اما نباید در تمامی کاربردها از این پروتکل‌ها استفاده نمود. زیرا پروتکلی که از رمزنگاری نامتقارن استفاده می‌کند به‌شدت می‌تواند تاثیرات منفی بر کارایی ارتباطات و محاسبات داخل شبکه داشته باشد. از جمله حملات موثر بر روی رمزنگاری نامتقارن، حمله جعل هویت[۸] [۱۸] و مرد میانی[۹] [۱۹ و ۲۰] بوده است. در طرف دیگر رمزنگاری متقارن قرار دارد. این شیوه از دوره باستان در مورد متون و یا نامه‌نگاری‌ها مورد استفاده بوده است و تنها مخاطره آن آشکارشدن رمز مورد استفاده بوده است. امروزه نیز این مخاطره همچنان وجود دارد. بدین‌منظور روش‌هایی جهت ذخیره‌سازی، استخراج و ارسال کلید به‌وجود آمده است. با استفاده از تابع درهم‌ساز مناسب می‌توان روش رمزنگاری متقارن را بسیار امن نمود به‌گونه‌ای که در مقابل تمامی حملات مقاوم باشد.

ضروری است نوع پروتکل‌های احراز هویت، متناسب با سطح امنیت مورد نیاز در شبکه انتخاب گردد. موضوع مهمی که لازم است مورد توجه قرار گیرد این است که، نقطه ورود کاربران به شبکه از اهمیت ویژه‌ای برخوردار بوده و معمولا آسیب‌پذیرترین نقطه شبکه محسوب می‌شود، زیرا این قسمت با خارج از شبکه و انواع کاربران ارتباط دارد و درنتیجه مساعد انواع حملات است. بنابراین لازم است در این مرحله از مکانیزم‌های امنیتی خاص استفاده شود. بر مبنای آن‌چه که قبلا به‌نام زیربرنامه‌ها و توابع داخلی EAP ذکر شد باید اضافه کرد که EAP مکانیزم‌های متفاوتی را برای احراز هویت به‌کار می‌گیرد. این زیربرنامه‌ها و توابع متناسب با مکانیزم‌های امنیتی تغییر می‌کنند. مکانیزم‌هایی که در EAP پشتیبانی می‌شوند شامل رمزنگاری نامتقارن (کلید عمومی)، رمزنگاری متقارن، کلیدهای از قبل به اشتراک گذاشته شده[۱۰] و گواهی‌های دیجیتال می‌باشند [۱۰-۷]. یک همه‌پرسی انجام‌گرفته نشان می‌دهد که کاربران حاضر هستند تا اتصال اینترنت خود را درصورت تضمین امنیت با یک‌دیگر به اشتراک بگذارند، برای این منظور لازم است روابطی بین نقاط اتصال تعریف گردد [۲۱ و ۲۲] که البته موانعی نیز در این موضوع وجود دارد [۲۳، ۲۴ و ۲۵]. توابع داخلی پروتکل EAP توانایی تولید کلید دارند. لازم است دو کلید پس از انجام فرآیند کامل احراز هویت تولید گردد [۹]. کلید اول، کلید اصلی نشست (MSK[۱۱]) و کلید دوم، کلید نشست توسعه‌یافته (EMSK[۱۲]) نام دارد [۶]. کلید MSK در فرآیند احراز هویت بین سرویس‌دهنده و کاربر تولید شده و سپس به نقطه اتصال ارسال شده و در پایان به‌منظور ایجاد امنیت در محاورات بین کاربر و نقطه اتصال استفاده می‌شود. کلید EMSK نیز در فرآیند احراز هویت بین سرویس‌دهنده و کاربر تولید می‌شود و یک کلید اضافی برای کاربردهای آینده است [۲۶]. امروزه همچنان مساله احراز هویت مجدد در پروتکل EAP مطرح است و انتظار می‌رود تا در آینده از کلید EMSK به‌عنوان کلید اصلی در راه‌حل‌هایی به‌منظور احراز هویت مجدد، البته در سناریوهایی خاص استفاده گردد [۳۲-۲۷ و۹]. هنگامی‌که گره سیار به محدوده جدید وارد می‌شود، باید نقطه

1- EAP Transport Level Security
2- Tunneled Transport Layer Security
3- Protected EAP
4- Lightweight Extended Authentication Protocol
5- Subscriber Identity Module
6- Certificate Authority
7- Token
8- Impersonate
9- Man In The Middle
10- Pre-shared Key
11- Master Session Key
12- Extended Master Session Key

اتصال جدیدی انتخاب گردد، پس الزاما گره سیار باید توسط نقطه اتصال جدید احراز هویت گردد، البته باید توجه داشت هویت گره سیار برای سرویس‌دهنده مشخص است. بسیار مطلوب خواهد بود که بدون آن‌که فرآیند احراز هویت به‌صورت کامل اجرا شود، بتوان احراز هویت را در گام‌ها و زمان کم‌تری انجام داد. برای این منظور از احراز هویت مجدد استفاده می‌شود. در احراز هویت مجدد، دو هدف کاهش زمان احراز هویت و کاهش محاسبات بر روی سرویس‌دهنده و دستگاه موبایل مورد توجه است [۹، ۱۵، ۳۰ و ۳۲]. امروزه مساله احراز هویت سریع در پروتکل EAP یکی از مهم‌ترین مسائل در حوزه احراز هویت است. راه‌حل‌های بسیاری برای این موضوع پیشنهاد شده و موانعی نیز مطرح شده‌اند که غالبا مربوط به مورد حملات محتمل در فرآیند احراز هویت مجدد است [۳۲]. یک ساختار به‌نام گراف همسایگی به‌منظور استخراج رابطه‌های میان نقاط اتصال[1] در [۳۳] ارائه شده است. در اینجا از گراف همسایگی برای انتخاب مجموعه نقاط اتصال که ممکن است در آینده در ارتباط با گره سیار باشند استفاده می‌شود. بنابراین کلید خام اولیه بین مجموعه نقاط اتصال انتخاب شده توزیع می‌گردد. به‌علاوه یک درخت کلید خام به‌منظور تولید کلید، ساخته می‌شود. این طرح به‌نام توزیع کلید پیش‌گستر[2] شناخته می‌شود، زیرا نقاط اتصال، کلید را قبل از عمل هندآف دریافت می‌کنند. طرح دیگری به‌نام احراز هویت پیش‌بینی‌کننده[3] در [۳۴] ارائه شده است که براساس مناطقی که کاربران تردد بیش‌تری دارند منطقه‌ای که احتمالا کاربر قصد رفتن به آنجا را دارد پیش‌بینی می‌کند. به بیان دیگر، تعدادی از نقاط اتصال را به‌عنوان مجموعه نقاط اتصال محتمل بعدی، برای پیوند انتخاب می‌کند. قبل از این‌که کاربر قصد حرکت به یک نقطه اتصال جدید را داشته باشد پیامی به سرویس‌دهنده احراز هویت می‌فرستد و سرویس‌دهنده به مجموعه نقاط اتصال محتمل، اطلاعات اولیه فرآیند احراز هویت را ارسال می‌کند. این طرح مستلزم آن است که نقطه اتصال امکان انجام محاسبات سنگین برای محاسبه مجموعه نقاط اتصال محتمل بعدی را داشته باشد که همین موضوع به‌عنوان نقطه ضعف بزرگ این طرح محسوب می‌شود.

۳- پروتکل پیشنهادی

همان‌طورکه در بخش قبل بیان شد دستگاه بی‌سیم دائماً در حال تغییر مکان در مناطق تحت پوشش و واردشدن به مناطقی است که احراز هویت کنندگان جدیدی وجود دارند، بنابراین نیاز به احراز هویت مجدد وجود دارد. در این پژوهش یک پروتکل احراز هویت بر روی لایه پیوند داده‌ها[4] پیشنهاد شده است که مبتنی بر استانداردهای IETF توسعه داده‌شده است. از جمله مزایای پروتکل پیشنهادی استفاده از رمزنگاری متقارن، توابع رقابت- پاسخ و تابع درهم‌سازی است. باتوجه به سربار محاسباتی پایین پروتکل پیشنهادشده، تاخیر زمانی کمی در فرآیند احراز هویت ایجاد می‌شود بنابراین این پروتکل در کاربردهای بلادرنگ مانند ارتباطات تصویری و ویدئو کنفرانس بسیار مناسب می‌باشد. پروتکل پیشنهادی شامل دو زیر پروتکل است. در این پروتکل، گره متحرک بی‌سیم در هنگام خروج از منطقه تحت پوشش نقطه اتصال (احراز هویت‌کننده[5]) و ورود به منطقه جدید تحت پوشش نقطه اتصال جدید، به‌جای اجرای کامل فرآیند احراز هویت پروتکل EAP[6]، فقط فرآیند احراز هویت مجدد پروتکل را اجرا می‌کند [۳۵]. فرآیند کامل احراز هویت شامل ۱۰ پیام رفت و برگشت بین کاربر، نقطه اتصال و سرویس‌دهنده است. همچنین، لازم است سرویس‌دهنده با استفاده از اطلاعات دریافت‌شده درخصوص کاربر، کلید متناظر به‌منظور ارتباط با کاربر و همچنین، یک جفت کلید به‌منظور ارتباط کاربر و نقطه اتصال تولید نماید. درصورتی‌که در فرآیند احراز هویت مجدد که در پروتکل پیشنهادی ارائه گردیده است، ضمن کاهش تعداد پیام‌های مبادله‌شده بین کاربر، نقطه دسترسی و سرویس‌دهنده به ۵ پیام، نیازی به تولید کلید مشترک کاربر و سرویس‌دهنده نمی‌باشد. درنتیجه سربار محاسباتی سرویس‌دهنده به نحو چشم‌گیری کاهش پیدا می‌کند. نمودار مراحل پروتکل پیشنهادی در شکل (۱) و نمودار زمانی آن در شکل (۲) آورده شده است. در ادامه گام‌های پروتکل پیشنهادی بیان می‌گردد.

۳-۱- نمادها و نشان‌گذاری

در نمادهای زیر منظور از نقطه اتصال قدیم یا دیده‌شده نقطه اتصالی است که با آن کلید مشترک وجود دارد و نقطه اتصال جدید نقطه اتصالی که قرار است با آن کلید مشترک برقرار گردد.

U: کاربر یا گره سیار

S: سرویس‌دهنده احراز هویت

OAP: نقطه اتصال قدیم

NAP: نقطه اتصال جدید

U_{ID}: شناسه کاربر

1- Access Points
2- Proactive Key Distribution
3- Frequent Handoff Region

4- Data Link Layer
5- Authenticator
6- EAP Complete Authentication

MAC_{NAP}: آدرس فیزیکی[1] نقطه اتصال جدید

N_X: دنباله تصادفی تولیدشده توسط موجودیت X

$\{M\}_X$: رمز پیام M به‌وسیله کلید X

$Auth\_Rq_X$: درخواست احراز هویت مجدد از موجودیت X

$K_{X,Y}$: کلید از پیش به‌اشتراک گذاشته‌شده بین دو موجودیت X و Y

$H(X,Y)$: محاسبه چکیده درهم‌ساز الحاق‌شده دو مقدار X و Y

۳-۲- شرح عملکرد پروتکل

در ادامه عملکرد پروتکل پیشنهادی آورده شده است.

۳-۲-۱- زیرپروتکل ۱

1) $U \mapsto OAP : U_{ID}$, N_U , $Auth\_Rq_S$, $H(U_{ID}, K_{U,S})$, $\{MAC_{NAP}, U_{ID}, N_U\}_{K_{U,OAP}}$, $\{U_{ID}, MAC_{NAP}, N_{NAP}\}_{K_{U,S}}$

۱) در گام نخست، کاربر ابتدا یک دنباله تصادفی[2] تولید کرده آن را به‌همراه شناسه[3] خود (آدرس MAC دستگاه بی‌سیم کاربر)، درخواست احراز هویت مجدد، نتیجه حاصل از اعمال تابع درهم‌ساز SHA-1 روی "شناسه خود و کلید مشترک خود و سرویس‌دهنده" را به‌همراه دو بسته رمزگذاری‌شده زیر به نقطه اتصال قدیم که با آن کلید مشترک دارد ارسال می‌کند:

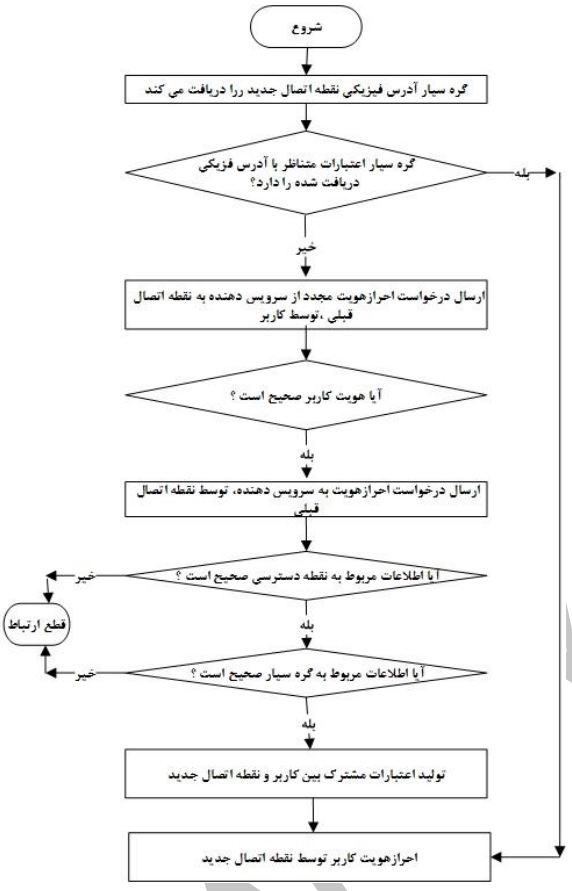
الف) بسته اول شامل: ۱. آدرس فیزیکی نقطه اتصال جدید ۲. شناسه کاربر و ۳. یک رشته تصادفی است که با کلید بین سرویس‌دهنده و نقطه اتصال قدیم رمز شده است.

ب) بسته دوم شامل: ۱. شناسه کاربر ۲. آدرس فیزیکی نقطه اتصال قدیم و ۳. دنباله‌ای تصادفی از حروف و اعداد که از نقطه اتصال جدید دریافت شده است و با کلید بین کاربر و سرویس‌دهنده رمز شده است.

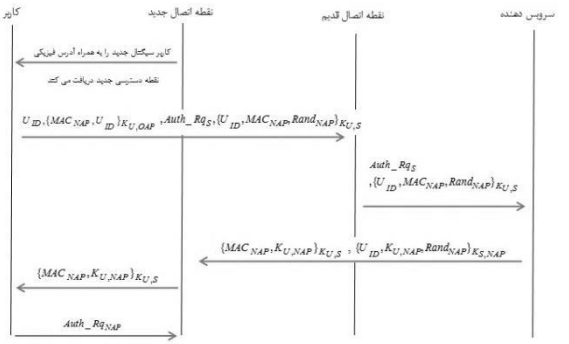
2) $OAP \mapsto S$: U_{ID} , $Auth\_Rq_S$, $H(U_{ID}, K_{U,S})$, $\{U_{ID}, MAC_{NAP}, N_{NAP}\}_{K_{U,S}}$

۲) در گام دوم، نقطه اتصال قدیم پس از ثبت شناسه کاربر، با استفاده از کلید مشترک خود و کاربر (K_U,OAP) بسته اول را رمزگشایی نموده و از صحت رشته تصادفی (N_U) اطمینان حاصل می‌نماید. همچنین، آدرس فیزیکی متعلق به نقطه اتصال جدید را استخراج نموده و متوجه درخواست کاربر برای اتصال به نقطه اتصال جدید می‌شود. سپس شناسه کاربر، درخواست احراز هویت مجدد، چکیده درهم‌ساز دریافتی و بسته دوم دریافتی را به سرویس‌دهنده ارسال می‌کند.

3) $S \mapsto NAP$: $\{U_{ID}, K_{U,NAP}, N_{NAP}\}_{K_{S,NAP}}$, $\{MAC_{NAP}, K_{U,NAP}\}_{K_{U,S}}$



شکل (۱). نمودار مراحل پروتکل پیشنهادی



شکل (۲). نمودار زمانی پروتکل پیشنهادی

1- MAC Address
2- Nonce
3- ID

۳) در گام سوم، سرویس‌دهنده ابتدا شناسه کاربر (U_{ID}) را ثبت کرده و با توجه به آن، کلید مشترک با کاربر را استخراج کرده و سپس تابع درهم‌ساز SHA-1 را روی رشته حاصل از "الحاق شناسه و کلید مشترک خود و کاربر" اعمال می‌کند. درصورت تساوی مقدار به‌دست‌آمده با مقدار رشته دریافتی، پیام را می‌پذیرد و بسته دریافتی از نقطه اتصال قدیم را رمزگشایی نموده و ضمن استخراج آدرس فیزیکی نقطه اتصال جدید، آن‌را با آدرس فیزیکی نقطه اتصال قدیم مقایسه[1] نموده و متوجه درخواست ارتباط با نقطه اتصال جدیدی می‌شود. نهایتاً ضمن تولید یک کلید مشترک بین کاربر و نقطه اتصال جدید، دو بسته رمزشده زیر را به نقطه اتصال جدید می‌فرستد:

الف) بسته اول شامل ۱. شناسه کاربر ۲. کلید مشترک کاربر و نقطه اتصال جدید و ۳. دنباله‌ای از حروف و اعداد است که با کلید بین سرویس‌دهنده و نقطه اتصال جدید رمز می‌شود.

ب) بسته دوم شامل ۱. آدرس فیزیکی نقطه اتصال جدید و ۲. کلید مشترک کاربر و نقطه اتصال جدید است که با کلید بین کاربر و سرویس‌دهنده رمز می‌شود.

4) $NAP \mapsto U : \{MAC_{NAP}, K_{U,NAP}\}_{K_{U,S}}$

۴) در گام چهارم، نقطه اتصال جدید بسته رمزشده اول مرحله قبل را بازگشایی نموده و پس از استخراج شناسه کاربر و کلید مشترک خود و کاربر، بسته دوم مرحله قبل را به کاربر ارسال می‌کند.

5) $U \mapsto NAP : Auth\_Rq_{NAP}$

۵) نهایتا در گام پنجم، درخواست احراز هویت کاربر به نقطه اتصال جدید ارسال می‌شود.

۳-۲-۲- زیرپروتکل ۲

بعد از احراز هویت مجدد موفق، ممکن است یک گره موبایل سیار، دوباره به محلی باز گردد که قبلا در آنجا احراز هویت شده و قبلا کلید مشترک با احراز هویت‌کننده دریافت کرده بود. اگر دستگاه موبایل دوباره به نقطه اتصالی برخورد کند که قبلا کلید مشترک با آن داشته و همچنین، از زمان ایجاد کلید بیش از حد آستانه نگذشته باشد، آن‌گاه نیازی به احراز هویت مجدد (زیرپروتکل ۱) نیست. بنابراین درصورتی‌که کاربر موبایل توانایی ذخیره جدولی از آدرس فیزیکی نقاط اتصال (احراز هویت‌کنندگان) به‌همراه کلید مشترک متناظر را در یک برهه زمانی داشته باشد، درصورتی‌که در محلی مکررا رفت و برگشت داشته باشد نیازی به انجام فرآیند احراز هویت ندارد.

۴- ارزیابی پروتکل

در این بخش ابتدا ارزیابی امنیتی و سپس ارزیابی محاسباتی پروتکل پیشنهادی بیان می گردد.

۴-۱- ارزیابی امنیتی

با بهره‌گیری از سه اصل هدایت امن[2]، احراز هویت متقابل[3] و پیاده‌سازی نظم در ارسال پیام‌ها با استفاده از تکنیک‌هایی چون تقریب دنباله‌ها و رشته‌های تصادفی و یا برچسب زمانی، از حمله جعل هویت[4] و تکرار[5] جلوگیری شده است. در ادامه، حملات اصلی و مرسوم بر روی پروتکل بررسی شده است و نتایج حاصل از این بررسی‌ها نشان‌دهنده امنیت این پروتکل در مقابل این حملات می‌باشد. همچنین، پروتکل ارائه‌شده با استفاده از زبان HLPSL [۳۶] پیاده‌سازی گردیده و در نرم‌افزار AVISPA نیز مورد آزمون قرار گرفته است. نتایج حاصله نیز موید امنیت پروتکل می‌باشد.

۴-۱-۱- حمله از کارانداختن سرویس[6]

در پروتکل پیشنهادشده تمامی پیام‌ها به‌صورت رمزشده ارسال نمی‌شود و هویت ارسال‌کننده پیام به‌صورت رمزنشده ارسال می‌شود بنابراین هرکدام از طرفین ارتباط یعنی نقطه دسترسی یا سرویس‌دهنده پیام را دریافت کنند، ابتدا شناسه فرستنده پیام را ثبت می‌کنند لذا پیام دیگری با این شناسه را نمی‌پذیرند. بنابراین درصورت ارسال انبوه پیام از طرف مهاجم تنها یک عمل عطف[7] برای شناسه پیام‌های دریافت‌شده در یک دوره زمانی صورت می‌پذیرد که سربار محاسباتی ناچیزی دارد لذا حمله ممانعت از سرویس نمی‌تواند موفق باشد.

۴-۱-۲- حمله جعل هویت

در این حمله، مهاجم بین کاربر و نقطه اتصال قرار گرفته و خود را به‌عنوان نقطه اتصال معرفی می‌کند و مانع رسیدن پیام‌ها به نقطه اتصال اصلی می‌شود. اما در پروتکل پیشنهادی مکانیزم درهم‌سازی رشته الحاق‌شده حاصل از شناسه کاربر و کلید مشترک، برای مهاجم غیرقابل کشف است، بنابراین درصورت درخواست‌های مکرر از کاربر و دریافت تعداد زیادی پیام مشابه، مهاجم نمی‌تواند بسته‌ها را رمزگشایی کند. همچنین، در این

1- XOR

2- Forward Secrecy
3- Mutual Authentication
4- Impersonate Attack
5- Replay Attack
6- Denial of Service
7- AND

پروتکل از رشته تصادفی[1] و دنباله‌های تصادفی[2] برای مقاومت در مقابل حمله تکرار استفاده شده است که این مقادیر نیز به‌صورت رمزشده ارسال می‌شوند و قابل استفاده مجدد نیستند، بنابراین پروتکل در مقابل این حمله نیز مقاوم است.

۴-۱-۳- حمله تکرار

در این نوع حمله، مهاجم پیام‌های ارسالی از کاربر و یا نقطه دسترسی را دریافت و ذخیره نموده و پس از اعمال تغییرات و جایگذاری بخش یا کل پیام، آن‌ها را ارسال می‌نماید. اگر مهاجم V مانع رسیدن پیام به کاربر گردد، سناریوی زیر قابل تصور است:

$U \mapsto OAP : U_{ID}, \{MAC_{NAP}, U_{ID}, N_U\}K_{U,OAP}$ ،
$H(U_{ID}, K_{U,S}),\ \{U_{ID}, MAC_{NAP}, Rand_{NAP}\}K_{U,S}$ ،
$Auth\_Rq_S$

مهاجم اجازه رسیدن پیام کاربر را به نقطه دسترسی نمی‌دهد و پیام زیر را می‌فرستد:

$V \mapsto OAP : V_{ID}, \{MAC_{NAP}, U_{ID}, N_U\}K_{U,OAP}$ ،
$H(U_{ID}, K_{U,S}),\ \{U_{ID}, MAC_{NAP}, Rand_{NAP}\}K_{U,S}$ ،
$Auth\_Rq_S$

مکانیزم درهم‌سازی رشته الحاق‌شده حاصل از شناسه کاربر و کلید مشترک تنها یک‌بار در پروتکل استفاده‌شده برای مهاجم غیرقابل کشف است لذا نمی‌توان آن‌را دوباره به‌کار برد. به‌علاوه در این پروتکل، رشته تصادفی که برای مقاومت در مقابل حمله تکرار به‌کار برده شده است به‌صورت رمزشده ارسال می‌شود و قابل استفاده مجدد نیست. نقطه دسترسی با دیدن درخواست احراز هویت، ابتدا شناسه مهاجم را ثبت کرده و قسمتی از پیام دریافت‌شده ($\{MAC_{NAP}, U_{ID}, N_U\}K_{U,OAP}$) را رمزگشایی می‌کند و با مشاهده آدرس فیزیکی نقطه اتصال جدید (MAC_{NAP}) متوجه درخواست کاربر برای ارتباط با نقطه اتصال جدید شده و بخش دوم پیام دریافت‌شده را به‌سمت سرویس‌دهنده ارسال می‌کند.

$OAP \mapsto S : Auth\_Rq_S , V_{ID} , H(U_{ID}, K_{U,S}) , \{U_{ID}, MAC_{NAP}, Rand_{NAP}\}K_{U,S}$

سرویس‌دهنده نیز نخست شناسه مهاجم (V_{ID}) را ثبت نموده و برای بازکردن پیام به‌دنبال کلید مشترک با شناسه مهاجم می‌گردد، اما کلید مشترکی نمی‌یابد. بنابراین پیام را از بین می‌برد. به این ترتیب حمله جایگذاری و تکرار برای این پروتکل امکان‌پذیر نیست.

1- Nonce
2- RAND

۴-۱-۴- حمله کشف کلید[3]

در پروتکل پیشنهادی حتی درصورت عدم استفاده از کلیدهای با طول کم‌تر از ۱۲۸ بیت از سوی نقطه اتصال و کشف کلید کاربر و نقطه اتصال قبلی ($K_{U,OAP}$) توسط مهاجم، باز هم امکان نفوذ وجود ندارد. فرآیند این حمله به‌شرح زیر امکان‌پذیر است:

$U \mapsto OAP : U_{ID}, \{MAC_{NAP}, U_{ID}, N_U\}K_{U,OAP}$ ،
$H(U_{ID}, K_{U,S}),\ \{U_{ID}, MAC_{NAP}, Rand_{NAP}\}K_{U,S}$ ،
$Auth\_Rq_S$

اگر مهاجم بسته $\{MAC_{NAP}, U_{ID}, N_U\}K_{U,OAP}$ را رمزگشایی نماید، تنها اطلاعاتی که می‌تواند به‌دست آورد، رشته تصادفی، شناسه کاربر و آدرس فیزیکی نقطه اتصال جدید است و برای طرح‌ریزی حمله، لزوما نیاز به کلید ۱۲۸ بیتی کاربر دارد که در اختیار ندارد، بنابراین این حمله نیز محتمل نیست.

۴-۱-۵- حمله مرد میانی[4]

این حمله درصورت استفاده از کلیدهای نامتقارن محتمل است به‌گونه‌ای که در مرحله مذاکره بین دو موجودیت رخ می‌دهد. با به‌کارگیری رمزنگاری متقارن می‌توان از این نوع حمله جلوگیری کرد زیرا در این نوع رمزنگاری نیازی به مذاکره درباره پارامترهای رمزنگاری وجود ندارد و کلید مشترک بین دو موجودیت از قبل وجود دارد. بنابراین در پروتکل پیشنهادی به‌علت استفاده از رمزنگاری متقارن، این حمله نیز محتمل نیست.

۴-۲- ارزیابی محاسباتی

ارتباطات امن و کارا با سربار محاسباتی و ارتباطی پایین در شبکه‌های بی‌سیم همواره یکی از زمینه‌های اصلی پژوهشی است. هزینه‌های محاسبات و ارتباطات مرتبط با رمزنگاری در پروتکل پیشنهادی با استفاده استانداردهای مربوطه [۳۷]، محاسبه شده است.

در پروتکل پیشنهادی از الگوریتم رمزنگاری متقارن AES و توابع درهم‌ساز SHA-1 استفاده شده است. استفاده از این ترکیب، ضمن افزایش پیچیدگی رمزنگاری، نسبت به روش‌های رمزنگاری نامتقارن که از توابع کلید عمومی و گواهی‌های دیجیتال استفاده می‌کنند هزینه کم‌تری دارد [۳۸ و ۳۹]. خانواده پروتکل‌های EAP مبتنی بر TLS به جهت دارابودن امنیت بالا [۸ و ۱۰و ۱۱ و ۱۳و ۱۴و ۱۶]، طی سالیان متمادی

3- Known key
4- Man In The Middle

در تجهیزات شبکه شرکت‌های بزرگی نظیر سیسکو، اینتل، نوکیا و مایکروسافت به‌صورت گسترده مورد استفاده قرار می‌گیرند. لذا به‌منظور ارزیابی سربار محاسباتی پروتکل پیشنهادی، مقایسه با خانواده پروتکل‌های EAP مبتنی بر TLS صورت گرفته است. در این پروتکل‌ها از الگوریتم‌های رمزنگاری نامتقارن و گواهی‌های دیجیتال استفاده می‌شود.

نتایج حاصله از این مقایسه در جدول (۱) آورده شده است. باتوجه به استانداردها، کد شناسایی برابر ۳۲ بیت، اندازه عدد تصادفی ۶۴ بیت، الگوریتم رمزنگاری AES با طول کلید ۱۲۸بیت، تابع درهم‌ساز SHA-1، ۱۶۰ بیت، اندازه امضای دیجیتالی برای الگوریتم DSA، ۳۲۰ بیت، اندازه کلید برای الگوریتم کلید عمومی RSA، ۱۰۲۴ بیت و اندازه گواهی دیجیتال نیز ۱۰۲۴ بیت درنظر گرفته شده است [۳۷].

جدول (۱). هزینه محاسبات و ارتباطات پروتکل پیشنهادی

بخش مربوطه	گره مربوطه	پروتکل های TLSمبتنی بر	پروتکل پیشنهادی
رمزگذاری کلید عمومی	گره سیار	۱	۰
	نقطه اتصال	۱	۰
	سرویس دهنده	۲	۰
رمزگشایی کلید عمومی	گره سیار	۱	۰
	نقطه اتصال	۱	۰
	سرویس دهنده	۱	۰
رمزگذاری متقارن	گره سیار	۰	۲
	نقطه اتصال	۰	۱
	سرویس دهنده	۰	۲
رمزگشایی متقارن	گره سیار	۰	۱
	نقطه اتصال	۰	۲
	سرویس دهنده	۰	۲
صحت سنجی امضای نقطه اتصال[1]	گره سیار	۱	۰
	نقطه اتصال	۱	۰
	سرویس دهنده	۰	۰
تابع درهم ساز		۲	۲
هزینه ارتباطات		حداقل ۷۰۰۰ بیت	۱۶۰۰ بیت

همان‌گونه‌که در جدول (۱) مشاهده می‌شود سربار محاسباتی و ارتباطی پروتکل پیشنهادی فقط ۱۶۰۰ بیت است درصورتی‌که در پروتکل‌های EAP مبتنی بر TLS این مقدار، حداقل ۷۰۰۰ بیت است. بنابراین هزینه تبادلات پیام در فرآیند احراز هویت در پروتکل پیشنهادی فقط ۱۸ درصد پروتکل‌های EAP مبتنی بر TLS است. علت این کاهش نیز این است که در پروتکل پیشنهادی از الگوریتم کلید خصوصی و تابع درهم‌ساز به‌جای الگوریتم کلید عمومی و گواهی دیجیتال استفاده شده و لذا محاسبات سنگین و هزینه‌های حمل و نقل بالای کلید عمومی و سربار گواهی دیجیتال را ندارد. بنابراین کارآیی بهتری در مقایسه با پروتکل‌های EAP مبتنی بر TLS دارد.

1- Signature Verification Access Point

۴-۳- نتایج شبیه‌سازی

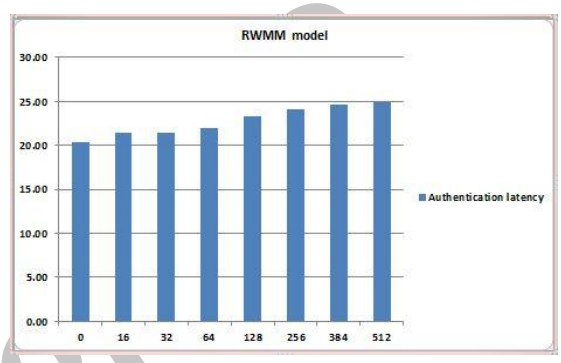
به‌منظور ارزیابی زمان احراز هویت، با استفاده از نرم‌افزار شبیه‌ساز NS2 [۴۰]، پروتکل پیشنهادی در یک محیط عملیاتی در سناریوهای حرکتی مختلف مورد ارزیابی قرار گرفت. در این فرآیند، چهار مدل تحرک برای گره‌ها شامل ۱. مدل حرکت تصادفی کراندار (BRMM[2])، ۲. مدل حرکت براونی گره‌های سیار (BMMM[3])، ۳. مدل حرکت سیار امتدادگرای نامنظم (RDMM[4]) و ۴. مدل حرکت سیار نامنظم ایستگاه‌های هوایی (RWMM[5]) درنظر گرفته شده است.

برای این منظور برای هر آزمایش ۲۰ شبیه‌سازی به انجام رسیده است. واحد زمان به‌صورت ثانیه‌ای افزایش یافته و بیشینه تغییر زاویه‌ای ۱۸۰ درجه درنظر گرفته شده است. همچنین حداکثر شتاب، ۲ متر بر مجذور ثانیه درنظر گرفته شده است. باتوجه به این‌که گره سیار بی‌سیم می‌تواند ساکن یا در حال حرکت باشد، سرعت آن بین صفر تا ۲۰ متر بر ثانیه متغیر درنظر گرفته شده است. البته در مدل RWMM ایستایی بین حرکت‌ها برابر یک ثانیه است. در سناریوی شبیه‌سازی، ۹ نقطه اتصال (احراز هویت‌کننده) و یک سرویس‌دهنده درنظر گرفته شده‌اند. نقاط اتصال، فراهم‌کننده ارتباط بی‌سیم با پروتکل 802.11 با نرخ انتقال داده ۵۴ Mbps هستند. مشخصات و شرایط سناریوی شبیه سازی در جدول (۲) آورده شده است. بدیهی است که تاخیر سربار فرآیند احراز هویت باتوجه به افزایش ترافیک شبکه بالا می‌رود. لازم به توضیح است که تاخیر احراز هویت در شرایطی که ترافیک شبکه از ۵۱۲ KBps بیش‌تر شود تغییر چندانی نداشته و ثابت می‌ماند. به این ترتیب در بدترین حالت، تاخیر سربار احراز هویت، در پروتکل پیشنهادشده برابر ۲۵ میلی‌ثانیه است. این به‌دلیل آن است که در پروتکل پیشنهادی فقط در مراحلی که لازم بوده است رمزنگاری صورت می‌پذیرد، همچنین، سربار مخابراتی کمی نیز مورد نیاز است. نتایج حاصل از شبیه‌سازی در شکل‌های (۶-۳) آورده شده است. همچنین، در شکل (۷) نتایج مقایسه زمان احراز هویت در پروتکل پیشنهادشده، پروتکل EAP-TLS و پروتکل توزیع کلید پیش‌گستر[6] آورده شده است.

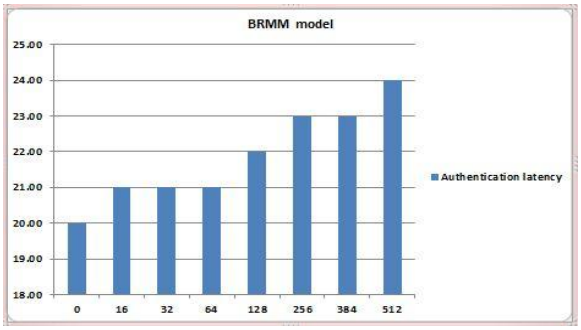
2- Bounded Random Mobility Model
3- Brownian Motion Mobility Model
4 Random Direction Mobility Model
5- Random Waypoint Mobility Model
6- Proactive Key Distribution

جدول (۲). مشخصات سناریوی شبیه سازی پروتکل پیشنهادی

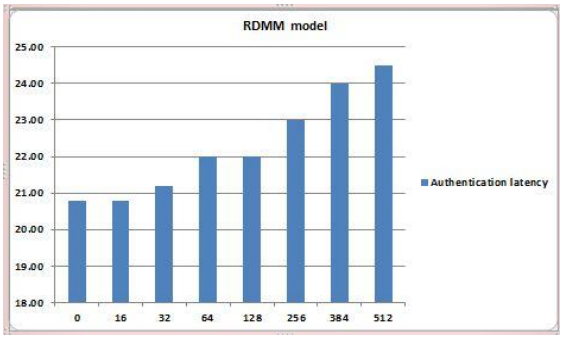
حداکثر سرعت اولیه (m/s)	حداقل سرعت اولیه (m/s)	حداکثر شتاب (m/s2)	سرعت انتقال (KB/s)	شعاع رادیویی (m/s)	تاخیر تغییر کانال (ms)	تاخیر سرپا نگه داشتن (ms)	گستره (m2)
۲۰,۰۰	۰,۰۰	۱,۰۰	۸,۰۰	۷۰,۰۰	۵,۰۰	۰,۱۰	۶۲۵۰۰,۰۰
۲۰,۰۰	۰,۰۰	۱,۵۰	۸,۰۰	۱۰۰,۰۰	۵,۰۰	۰,۱۵	۶۲۵۰۰,۰۰
۲۰,۰۰	۰,۰۰	۲,۰۰	۱۲,۰۰	۷۰,۰۰	۵,۰۰	۰,۱۰	۶۲۵۰۰,۰۰
۲۰,۰۰	۰,۰۰	۲,۰۰	۱۶,۰۰	۱۰۰,۰۰	۵,۰۰	۰,۱۵	۶۲۵۰۰,۰۰



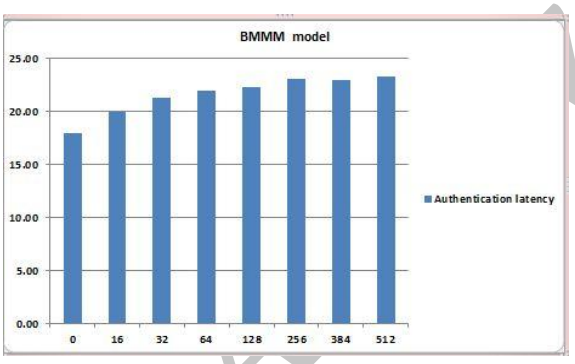
شکل (۳). زمان تاخیر احراز هویت پروتکل پیشنهادی در مدل حرکت سیار نامنظم ایستگاه‌های هوایی (RWMM)



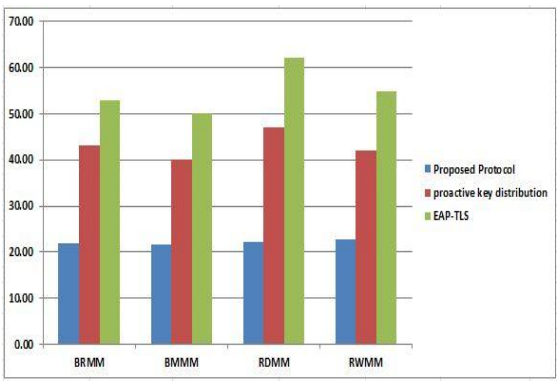
شکل (۴). زمان تاخیر احراز هویت پروتکل پیشنهادی در مدل تصادفی کرانه‌دار نامنظم (BRMM)



شکل (۵). زمان تاخیر احراز هویت پروتکل پیشنهادی در مدل حرکت سیار امتدادگرای نامنظم (RDMM)



شکل (۶). زمان تاخیر احراز هویت پروتکل پیشنهادی در مدل حرکت براونی گره‌های سیار (BMMM)



شکل (۷). مقایسه زمان تاخیر احراز هویت پروتکل در همه مدل‌ها

۶- نتیجه‌گیری

این پژوهش با تاکید بر احراز هویت به‌عنوان اصلی‌ترین عامل مرتبط با امنیت به مقوله جابه‌جایی‌های گسترده کاربران در شبکه‌های بی‌سیم مبتنی بر استاندارد 802.1X پرداخته است. دستگاه بی‌سیم دائماً در حال تغییر موضع در مناطق تحت پوشش و خارج‌شدن به مناطقی است که احراز هویت‌کنندگان جدیدی وجود دارند و بنابراین نیاز به احراز هویت مجدد وجود دارد. در این پژوهش، یک پروتکل احراز هویت مجدد بر روی لایه MAC پیشنهاد شده که مبتنی بر استانداردهای IETF است. پروتکل پیشنهادشده ضمن امن‌بودن، باتوجه به هزینه محاسباتی

و ارتباطی پایین، تاخیر زمانی کمی در فرآیند احراز هویت ایجاد می‌کند. این پروتکل برای کاربردهای بلادرنگ مانند ارتباطات تصویری و ویدئو کنفرانس مناسب می‌باشد.

از آنجاکه عملکرد پروتکل پیشنهادی، درون دامنه‌ای است، به‌منظور توسعه این پروتکل، پیشنهاد می‌شود پژوهش‌های آتی به‌منظور توسعه و ارائه پروتکل‌های مشابه با عملکرد بین دامنه‌ای انجام پذیرد.

۷- مراجع

[1] A. Uzelac and Ed, "Voice over IP (VoIP) SIP Peering Use Cases," Internet Engineering Task Force (IETF), 2011.

[2] T. T. Kwon, M. Gerla, and S. Das, "Mobility Management for VOIP Service: Mobile IP vs. SIP, IEEE Wireless," Commun. Magazine, pp. 66-75, Oct. 2002.

[3] B. Aboba and J. Wood, "Authentication Authorization and Accounting (AAA) Transport Profile," Internet Engineering Task Force (IETF), 12-Feb-2016.

[4] G. Giaretta, et al, "Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6," Internet Engineering Task Force (IETF), September 2009.

[5] R. Housley, et al, "Guidance for Authentication, Authorization and Accounting (AAA) Key Management," Internet Engineering Task Force (IETF), July 2007.

[6] J. Vollbrecht, et al, "AAA Authorization Framework," Internet Engineering Task Force (IETF), August 2000.

[7] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, Internet Engineering Task Force (IETF), June 2004.

[8] B. Aboba and D. Simon, "PPP EAP-TLS Authentication Protocol RFC-2716," Internet Engineering Task Force (IETF), October 1999 .

[9] B. Aboba, H. Levkowetz, D. Simon, and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework," Internet Engineering Task Force (IETF), 2008.

[10] D. Simon, B. Aboba, and R. Hurst, "The EAP-TLS Authentication Protocol RFC5216," Internet Engineering Task Force (IETF), March 2008.

[11] P. Funk and B. Wilson, "Extensible Authentication Protocol, Tunneled Transport Layer Security (EAP-TTLSv0) RFC5281," Internet Engineering Task Force (IETF), Aug. 2008.

[12] A. Palekar, et al., "Protected EAP Protocol (PEAP)," Work in Progress, Internet Engineering Task Force (IETF), July 2004.

[13] S. Convery, D. Miller, and S. Sundaralingam, "Cisco Systems, Cisco SAFE: WLAN Security in Depth," White Paper, 2011.

[14] Interlink Networks, "EAP Methods for Wireless Authentication," April 2003.

[15] H. Haverinen and J. Slowey, "Extensible Authentication Protocol Method for Global System for Mobile, Internet Engineering Task Force (IETF), RFC 4186," May 2006.

[16] N. Cam-Winget, D. McGrew, J. Salowey, and H. Zhou, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)," Internet Engineering Task Force (IETF), RFC 4851, May 2007.

[17] J. W. Hui, A. Ahuja, K. Kondaka, W. Hong, and I. "Cisco Technology, Scalable replay counters for network security," 2012.

[18] L. Gavin, "An attack on the Needham-Schroeder Public-key Authentication Protocol," Information Processing Letters, vol. 56, pp. 131-133, 14 August 1995.

[19] L. D. Manik and S Navkar, "on the security of SSL/TLS-enabled applications," Informatics, pp. 68–81, January 2014.

[20] I. Cervesato, et al., "Breaking and fixing public-key Kerberos," Information and Computation, pp. 402–424, April 2008.

[21] M. S. Daithi, "Law in the last mile: sharing Internet access through WIFI," SCRIPT-ed, vol. 6, 2009.

[22] R. V. Hale, "Wi-Fi liability: potential legal risks in accessing and operating wireless Internet," Santa Clara Computer and High Technology Law Journal vol. 21, 2005.

[23] M. Hines, "Worried about Wi-Fi security?," CNET News, January 2005 .

[24] H. Xia and J. Brustoloni, "Virtual prepaid tokens for Wi-Fi hotspot access," presented at the Local Computer Networks, 29th Annual IEEE International Conference on, pp. 232–239, 2004.

[25] O. Delgado-Mohatar, A. Fúster-Sabater, and J. M. Sierra, "A light-weight authentication scheme for wireless sensor networks," Ad Hoc Netw., vol. 9, no. 5, pp. 727–735, Jul. 2011.

[26] J. Salowey, L. Dondeti, V. Narayanan, and M. Nakhjiri, "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK), RFC5295," Internet Engineering Task Force (IETF), 2008.

[27] S. Khan and A.-S. K. Pathan, "Wireless Networks and Security: Issues, Challenges and Research Trends," Springer Science & Business Media, 2013.

[28] H. Hwang, G. Jung, K. Sohn, and S. Park, "A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP," International Conference on Presented at the Information Science and Security (ICISS), pp. 164–170, 2008.

[29] D. Stanley, B. Aboba, and J. Walker, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, RFC4017," Internet Engineering Task Force (IETF), March 2005.

[30] D. Simon, et al., "The EAP-TLS Authentication Protocol," Microsoft Corporation, March 2008.

[31] Z. Cao, H. Bing, and Z. Glen, "EAP Extensions for the EAP Re-authentication Protocol (ERP), Internet Engineering Task Force (IETF) RFC6696," July 2012.

[32] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), Internet Engineering Task Force (IETF) RFC4187," 2006.

[33] V. Narayanan, T. Clancy, M. Nakhjiri, and L. Dondeti, "Handover Key Management and Re-Authentication Problem Statement," Internet Engineering Task Force (IETF) RFC 5169, 2011.

[34] A. Mishra, M. H. Shin, N. J. Petroni, T. Clancy, and W. Arbaugh, "Proactive Key Distribution Using Neighbor Graphs," IEEE Wireless Communications, pp. 26–36, 2004.

[35] S. Pack and Y. Choi, "Pre-authenticated Fast Handoff in a Public Wireless LAN based on IEEE 802.1x model," Proceedings of the IFIP TC6/WG6.8 Working Conference on Personal Wireless Communications, pp. 175–182, October 2002.

[36] V. Narayanan and L. Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)," Internet Engineering Task Force (IETF) RFC5296, 2008.

[37] R. Housley, "Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm," NIST, August 2009.

[38] A. Menezes, J. V. Oorschot, P. C. Vanstone, and A. Scott "Handbook of Applied Cryptography, CRC Press," 2008, ISBN 0849385237.

[39] M. Stevens, P. Karpman, and T. Peyrin, "The SHAppening: Freestart Collisions for SHA-1," 2015.

[40] Network Simulator 2, www.isi.edu/nsnam/ns/

Journal Of Electronical & Cyber Defence
Vol. 3, No. 4, 2016, Serial No.12

Secure and Fast Re-authentication Protocol to Support Extensive Movement of Users in IEEE 802.1X Wireless Networks

A. Mohammadi*, N. Modiri

*Imam Hossein University

(Received: 18/10/2015, Accepted: 12/01/2016)

ABSTRACT

Tradeoffs between security and performance are the most important issue in wireless networks. An authentication protocol is a type of cryptographic protocol with the purpose of authenticating entities. Latest standards for re-authentication protocols have published by Internet Engineering Task Force (IETF). In this research, after reviewing some protocols in this scope, a security protocol is proposed. The proposed protocol is based on IETF standards. Fundament of RFC 6696 is exploited to develop the proposed protocol. It offers serious advantages over the existing IEEE 802.1X standard protocols, including: symmetric cryptosystem, challenge–response and hash chaining.

Keywords: Wireless Networks, Wireless Networks Security, 802.1X Networks, EAP Protocol, Authentication.

* Corresponding Author Email: mohammadi@ihu.ac.ir