احراز هویت تحویل کارآمد با ناشناس ماندن و عدم قابلیت ردیابی کاربر برای رایانش ابری سیار

ولی الله وحیدی نژاد

دانشجوی کارشناسی ارشد مهندسی نرم افزار گرایش نرم افزار ، دانشگاه پیام نور واحد تهران ، ایران

vahidi.best90@yahoo.com

مریم اسکندر پور

فارغ التحصیل کارشناسی ارشد مهندسی فناوری اطلاعات گرایش سیستمهای چند رسانه ای ، دانشگاه پیام نور واحد عسلویه ، ایران

mohandes.eskandarpour@gmail.com

چکیده

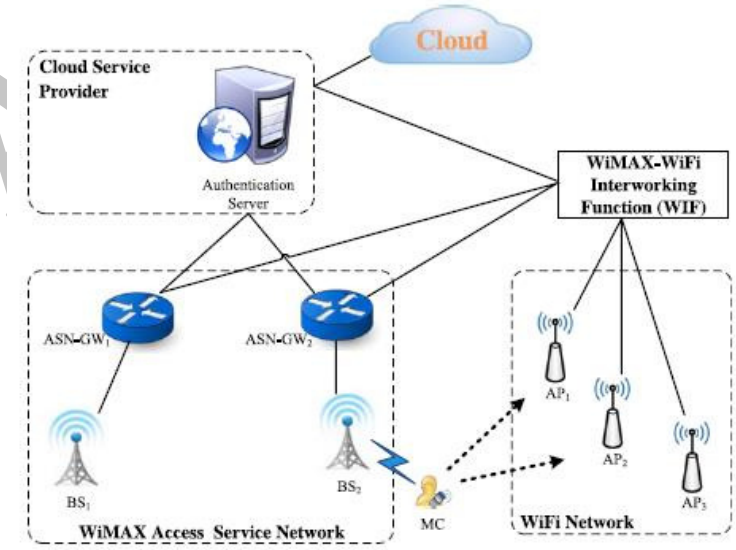
تکنولوژی های ارتباطی وایرلس گوناگونی جهت حجم گسترده ای از تجهیزات تولید و اعمال شده اند. این توانایی رایانش ابری با مداخله ی تحرک، و رایانش ابری سیار (MCC)، برگرفته از روند الگوی رایانش تولید آتی ست. دراین مقاله، ما به بیان موضوع چالش های تکنولوژی MCC – ایمنی و حریم خصوصی فرآیند تحویل- پرداخته ایم. ما یک طرح جدید از تحویل احراز هویت را برای هماهنگی شبکه های ابری سیار پیشنهاد داده ایم، که ناشناس ماندن و عدم قابلیت ردیابی کاربر را توسعه می بخشد. مکانیسم پیشنهادی ما، در مقایسه با پروتکل های پیشین، خصوصیت درک عمومی، ایمنی قوی و کارآمدی را به همراه دارد.

کلید واژه ها: محاسبات ابری سیار، احرازهویت تحویل، امنیت، کارایی

۱. مقدمه

با رشد سرعت تکنولوژی های متفاوت وایرلس، همچون LTE، CDMA، وایمکس و وای فای، رایانش ابری برای ابزار رایانش متصل به سیم، محدودیتی نخواهد داشت. تلفن های هوشمند یا تبلت ها مکررا" از ابزار رایانش بهره می برند. با توزیع ساختار رایانش ابری، و کاربرد ابزار سیار جهت دستیابی ابری، الگوی بعدی تولید رایانش، بیان خواهد شد. این الگو به رایانش ابری سیار (MCC) شناخته شده است. ابزار کاربری، با این الگو به رومینگ تکنولوژی های متجانس ارتباطی نیاز خواهند داشت. هرچندکه، به دلیل سیاست های امنیتی گسترده میان شبکه های متفاوت، مفاهیم ایمنی به حل مجدد یک تحویل عمودی نیاز خواهند داشت، که القای خطرات ایمنی و نتایج موثری کمی را به همراه خواهد داشت. رومینگ پشتیبان و ایمنی تحویل در MCC چالشی برای هر شبکه ی در دسترس می باشند، این شبکه ها ممکن است دارای سیارهای متفاوت، کیفیت خدمات (QoS) و تجهیزات ایمن باشند. علاوه براین، زمان حقیقی کاربردهای ابری، مثل ویدئو کنفرانس و جریان های رسانه ای، دارای تجهیزات رسانه ای دقیق می باشند. برای غلبه بر این اجرا و و توسعه ی ایمنی خدمات در سیارات، طراحی یک پروتکل تحویل کارآمد ضروری می باشد.

احراز هویت یک مدل مهم در پروتکل تحویل می باشد. همان طور که در شکل ۱ نشان داده شده است، عدم توجه به تکنولوژی اعمال شده در MCC ، یک نوع سناریوی متجانس احرازهویت تحویل ابری را با چهار نهاد به همراه دارد: سفارش دهنده های سیار (MCs)، نقاط در دسترس (APs) یا ایستگاه های اولیه (BSs) ، روترهای دروازه (GWs) و سرورهای احرازهویت (AS)، که در خدمات توسعه یافته ی ابری جای می گیرند. پیش از ورود به شبکه، یک MC باید برای AS ثبت شود. پس از تضمین دخول از سوی AS، MC جهت دسترسی به شبکه از طریق GW به یک AP (یا یک BS) متصل می شود. یک MC از یک AP (یا یک BS) به یک AP جدید (یا یک BS) با دامنه ای از یک شبکه ی وایرلس–که به تحویل افقی ارجاع داده می شود- حرکت می کند. متقابلا" ، یک تحویل MC درمیان شبکه های وایرلس متجانس در دسترس –که به تحویل افقی ارجاع داده می شود- انجام می شود. پس از انتقال رومینگ های MC به یک AP جدید (یا یک BS)، احراز هویت تحویل باید در یک AP جدید (یا یک BS) ایجاد شود. AP (یا یک BS) یک MC قانونی را احراز هویت خواهد کرد و هر درخواست دیگر توسط کاربران غیرقانونی را باز می گرداند. درهمان زمان، آنها یک کلید جلسه میان این CMهای احراز هویت شده و AP (یا یک BS) را با هدف توسعه ی اعتماد و تداخل ارتباطات جلسه، برقرار می کنند.



شکل ۱. معماری یک الگوی MCC با یک شبکه دسترسی یکپارچه برای وایمکس و وای فای

دراین تحقیق، تداخل شبکه های متجانس وای فای و وایمکس را مورد توجه قرار داده ایم، شبکه های وایمکس از طریق تابع تعامل وای فای (WIF) ارتباط می یابند، که این تعامل توسط انجمن وایمکس برای رومینگ پشتیبان تعریف شده است. WIF نقش مهمی در ارتباط شبکه های وای فای و وایمکس ایفا می کند، و برای دسترسی عملکرد شبکه های وایمکس، توانایی لازم را دارد. در شکل ۱ کنترل دسترسی احراز هویت، با توجه به خدمات دستیابی شبکه-دروازه (ASN-GW) یا AP نشان داده شده است. یک ASN-GW چندین BS را کنترل می کند و پیام های احراز هویت را بین MC و AS جای گرفته در خدمات توسعه یافته ی ابری (CSP)، شارژ می کند. با توجه به ایمنی لازم، فرض می کنیم که پروتکل انتقال ایمن، برای حفظ ارتباطات صحیح و تثبیت ارتباط با شبکه، درهمه ی موارد بیان شده بکار می رود.

دراین جا دو موضوع کاربردی مبتنی بر طراحی پروتکل تحویل احراز هویت در MCC بیان شده است:

*اول، ایمنی و حریم خصوصی دورابطه ی مهم برای فرآیند تحویل احراز هویت می باشند. برای حریم خصوصی، سفارش دهنده های سیار ممکن است حفظ هویت خود را ترجیح دهند و موقعیت خود را مخفی نگه دارند. از آنجا که پروتکل های رومینگ ممکن است هویت وموقعیت کاربر در فاز احراز هویت کاربری را در معرض نمایش گذارند، این موضوع در شبکه های وایرلس بسیار برجسته است. حریم خصوصی هویت وقتی برای MC نمایان می شود که او درخواست احراز هویت ارسال کند. بنابراین، یک طرح سخت و ارائه دهنده ی حریم خصوصی دراین مورد ضروری ست. از سوی دیگر، حریم خصوصی موقعیت وقتی برای AP یا SB نشان داده می شود که MC برای آنها در دسترس باشد، زیرا هر فرد هجوم آورنده می تواند بر ریشه ی حرکات MC اثر گذارد. بنابراین، باید به ناشناس بودن و عدم قابلیت ردیابی کاربر در پروتکل تحویل، توجه بیشتری شود.

*دوم، کارآمدی نیز برای توجه بیشتر به خدمات احراز هویت تحویل مورد نیاز است. این بخش برای تضمین ادامه ی خدمات و QOS اهمیت زیادی دارد، این خدمات به معنا تاخیر و از بین رفتن بسته ی کمتر درهنگامی ست که یک MC به شبکه ی دیگر تحویل داده می شود. ازآنجا که نه MC ها و نه AP ها به طور کلی با قبلیت قدرت و پردازش محدود نمی شوند، یک پروتکل تحویل احراز هویت کارآمد باید ضرورت یابد. علاوه براین، یک پروتکل باید توانایی حفظ ارتباط ثابت میان MC ها و AP ها را داشته باشد.

۱.۱. کارهای مرتبط

دراین جا برای هدف دستیابی به احراز هویت تحویل کارآمد در یک شبکه ی متجانس، چندین پروتکل احراز هویت بیان شده است. هرچندکه، بیشتر این پروتکل ها در نهایت به چندین شکل خاموش می شوند، ما این مورد را به جنبه های زیر تقسیم کرده ایم:

*تبادل با AS درطول احرازهویت یا نیاز به شرکت دادن بخش های سوم، مثل AP/BS خانه؛

*نمی توان یک مکانیسم حفظ حریم خصوصی را توسعه بخشید حتی اگر آنها مجموعه ای از عیب های امنیتی باشند؛

*هزینه ی بالای احرازهویت و کارآمدی کم، که نمی تواند تجهیزات تحویل را بدست آورد؛ و

*طرح پیچیده ای از طرح های نتیجه شده در ضعف های جهانی.

وون و همکاران یک تست مبتنی بر USIM احراز هویت را برای تحویل UMTS-WLAN ارائه کرده اند. اجرای کامل احراز هویت و سرعت احراز هویت مجدد در زمان پردازش، تحلیل و مقایسه می شود. هرچندکه، دراین جا هیچ توصیف جزیی مبنی بر سرعت احراز هویت و احراز هویت تحویل بیان نشده است. اجرای مبتنی بر سرعت احرازهویت مجدد، به تجهیزات کاربردی

تاخیری نیازی ندارد. در منبع (۶)، مولفان یک طرح احراز هویت اولیه را برای شبکه های متداخل وای فای و وایمکس ارائه کرده اند. این طرح هنگامی که کاربر درابتدا وارد شبکه می شود، MSK تولید می کند، و آن را به شبکه ی مورد نظر انتقال می دهد. با طرح احراز هویت اولیه، فرآیند تحویل با مکان احراز هویت ساده می شود و فقط به جریان پیام ها میان MC و AP/BS مورد هدف –بدون توجه به AS- نیاز دارد. درمنبع (۷)، سان و همکاران نیز یک طرح احرازهویت اولیه ی مبتنی بر طرح های ایمن و کارآمد تحویل، برای شبکه های متجانس وای فای و وایمکس، ارائه داده اند. تطبیق کلید مجدد در این طرح، زمان فرآیند را کاهش می دهد و از تکرار تحویل میان دو BS پیشگیری می کند. با اینحال، تحلیل های اولیه نشان می دهند که هردو طرح ممکن است هنگام از دست دادن MSK یا انتقال MC به AP/BS مورد نظر، زمان زیادی را سپری کنند. در منبع (۹)، مولفان یک احراز هویت AKA را در شبکه های 3G-WLAN پیشنهاد داده اند، که هزینه ی احرازهویت را با کاربرد یک هویت مشترک سیار بین المللی، کاهش می دهد. متاسفانه، تحلیل های ایمنی انجام شده نشان می دهد که کاربران در هجوم پتانسیل کاربرد سوم، آسیب پذیر می باشند.

پنج پروتکل سریع و ایمن احراز هویت مجدد برای مشترکان 3GPP جهت اجرای تحویل میان سیستم های وایمکس و WLAN پیشنهاد شده است، که بسیار سودمند می باشند. دراینجا، «کلید کاربرد مجدد» بدین معناست که، درحالی که کاربر شبکه را مجددا" مشاهده می کند، کلیدی در یک شبکه، برای احرازهویت مجدد ذخیره شده است، بنابراین این عمل فرآیند تولید مجدد را سرعت می بخشد و هزینه ی احراز هویت را کاهش می دهد. اگرچه، این طرح می تواند با اجرای کلید کاربرد مجدد بدست آید، و تاخیر در احراز هویت مجدد نیز با پروتکل های استاندارد 3GPP جاری مقایسه می شوند، و می توانند چند خصوصیت ایمنی را بهبود بخشند، این مورد تنها ارتباطات تک هاپ میان MC و AP/BS را پشتیبانی می کند و زمان پردازش احراز هویت مجدد را با توجه به کاربرد زمان حقیقی مورد نیاز، ناتوان می سازد. این طرح با موارد ارائه شده در سرعت احراز هویت، برای شبکه های متداخل WLAN –وایمکس فرض می شود. با تطبیق مفاهیم احرازهویت و روش احراز هویت اولیه، می توان از تاخیر طولانی پیشگیری کرد. هرچندکه، به دلیل اینکه AS جایگاه نرمالی در AP/BS دارد، ممکن است سیستم اجرایی ارتباط کمی میان AP/BS و AS ایجاد کند.

اخیرا" ، طرح احراز هویت تحویل ایمن و سریع براساس بلیطی برای شبکه های متجانس وایمکس و وای فای، در منبع (۱۴) پیشنهاد شده است. MC و AP/BS مورد نظر می تواند احرازهویت را تکمیل کرده و کلید جلسه را با یک بلیط معتبر تولید شده در AP/BS های قبلی و بدون تعامل با AS، استنتاج کند. محل احراز هویت مشخصا" تاخیر احرازهویت تحویل را کاهش می بخشد. باین حال، این امر حفظ حریم خصوصی را بهبود نمی بخشد و کاهش ضعف را به دنبال خواهد داشت.

متاسفانه همه ی طرح های ذکر شده در بالا هیچ معیارحفظ حریم خصوصی ندارند و برای شبکه های مختلف، عمومیت ندارند. در منبع (۱۵) یک پروتکل احراز هویت جهانی با قدرت عدم شناخت کاربر، برای شبکه های ارتباطی وایرلس، توسط یانگ و همکاران پیشنهاد شده است. این پروتکل براساس شاخص های گروهی ست و تنها به سه پیام نقض میان رومینگ MC و یک AP/BS خارجی حین تحویل نیاز دارد. با اینکه این پروتکل می تواند ناشناس بودن کاربر را تضمین کند و مکانیسم عملکرد اورا توسعه می بخشد، بازهم در عدم قابلیت ردیابی کاربری با خطا روبه رو می شود، و ممکن است درهنگامی که تعداد کاربران زیاد است، با اتلاف زمان و مصرف نیرو همراه باشد. کائو وهمکاران یک ID یکپارچه ی مبتنی بر رمزنگاری طرح احراز هویت تحویل، بدون کاربرد شبکه های متجانس در دسترس، پیشنهاد داده اند. احراز هویت تحویل میان یک MC و AP مورد نظر، بدون دخالت شخص سوم اجرا می شود. اگرچه مولفان ادعا دارند که طرح آنها ناشناس ماندن کاربری را به همراه دارد، اما هویت MC بازهم ممکن است در معرض مهاجمان قرار گیرد، زیرا هویت حقیقی هنگامی نمایان می شود که MC برای AP مورد نظر، درخواست احرازهویت تحویل داشته باشد. بنابراین، این طرح نمی تواند ناشناس ماندن و عدم قابلیت ردیابی کاربری را به همراه داشته باشد. اخیرا"، لیو و

همکاران پروتکلی با زمان محدود در احرازهویت شخص ناشناس را برای شبکه های رومینگ پیشنهاد داده اند. این پروتکل همانند پروتکل منبع (۱۵) براساس شاخص گروهی و جایگیری زمان اطلاعات در این شاخص،می باشد. بدین ترتیب، کاربران می توانند در ماهیت و تعلقات لغو شده را رده بندی کنند. دراین پروتکل نیز عدم قابلیت ردیابی کاربر را عملی نمی کند.

۱.۲. تخصیصات ما

بنا بر تحلیل های انجام شده در بالا، کاربران تمایلی به پذیرش ابزاری را ندارند که در توسعه ی ایمنی و تضمین کارآمدی ، همیشه باخطا مواجه می شوند. بنابراین، توسعه ی یک احرازهویت تحویل عملی با کارآمدی و طرح حریم خصوصی کاربری، موضوع برجسته ای در مفهوم MCC می باشد. دراین تحقیق، مزیت احراز هویت در منحنی الگوریتم (۲۲) آورده شده است، بدین ترتیب ما احراز هویت تحویل کارآمد جدیدی را با ناشناس ماندن و عدم قابلیت ردیابی کاربری، برای MCC پیشنهاد می دهیم. طرح پیشنهادی ما می تواند از کارهای پیشین برجسته تر باشد، این طرح در جنبه های زیر خلاصه می شود:

۱-بدون شخص سوم: به استثناء MC و AP/BS ، دراین جا هیچ شرکت کننده ی اضافه ای از شخص سوم، درطول احرازهویت تحویل –مثل AS یا AP/BS خانه- وجود ندارد.

۲-طراحی ساده: ما تنها به یک پروتکل احرازهویت تحویل برای سناریوی شبکه های مختلف متجانس نیاز داریم.

۳-عمومیت: این پروتکل در این دید کلی می باشد که پروتکل مشابه می تواند به تناسب برای شبکه های متجانس متفاوت بکار رود.

۴-ناشناس ماندن و عدم قابلیت ردیابی کاربر: پروتکل ما برای رضایت از تجهیزات جامعه ی مدرن، از ناشناس ماندن و عدم قابلیت ردیابی کاربر حمایت می کند.

۵-امنیت و کارآمدی قوی: پروتکل ما براساس یک ایمنی پرقدرت، در مقایسه با طرح های موجود، برای اجرای احراز هویت بسیار مناسب می باشد.

بخش های باقی مانده از این تحقیق بدین صورت سازمان یافته اند. بخش ۲ تجهیزات ایمن را مورد بحث قرار می دهد و منحنی بیضی گروه را معرفی می کند. بخش ۳ طرح ما را بیان کرده و بخش ۴ ایمنی و اجرای طرح را مورد تحلیل قرار می دهد. این مقاله در بخش ۵ جمع بندی می شود.

۲. مقدمات و تجهیزات ایمنی

۲.۱. تجهیزات ایمنی

یک طرح ایمن و احراز هویت تحویل کاربر ناشناس در MCC باید تجهیزات زیر را دنبال کند:

۱-احرازهویت متقابل: رومینگ MC و AP مورد نظر هردو با AS احرازهویت می شوند.

۲-امتیاز الحاقی: MC ها برای احراز هویت AP باید با AS پیگیری شوند، چراکه AP به پیشگیری از فریب های پتانسیل و دیگر هجوم ها می پردازد.

۳-کلید تثبیت: MC ، AP مورد نظر و AS همگی یک رمز عمومی را به اشتراک می گذارند.

۴-کلیت داده ها: داده ی انتقال یافته در شبکه نمی تواند معمولی باشد، تکرار شود و عیب های به تاخیر اندازد. استراق سمع نیز برای دستیابی به متن مرتبط انعطاف پذیر است.

۵-ناشناس ماندن کاربر: به جزء AS ، MC نیز برای اشخاصی که AP را مشاهده می کنند، ناشناس می باشد.

۶-عدم قابلیت ردیابی کاربر: به جزء AS ، هیچ کدام توانایی شناخت فعالیت های MC را ندارند.

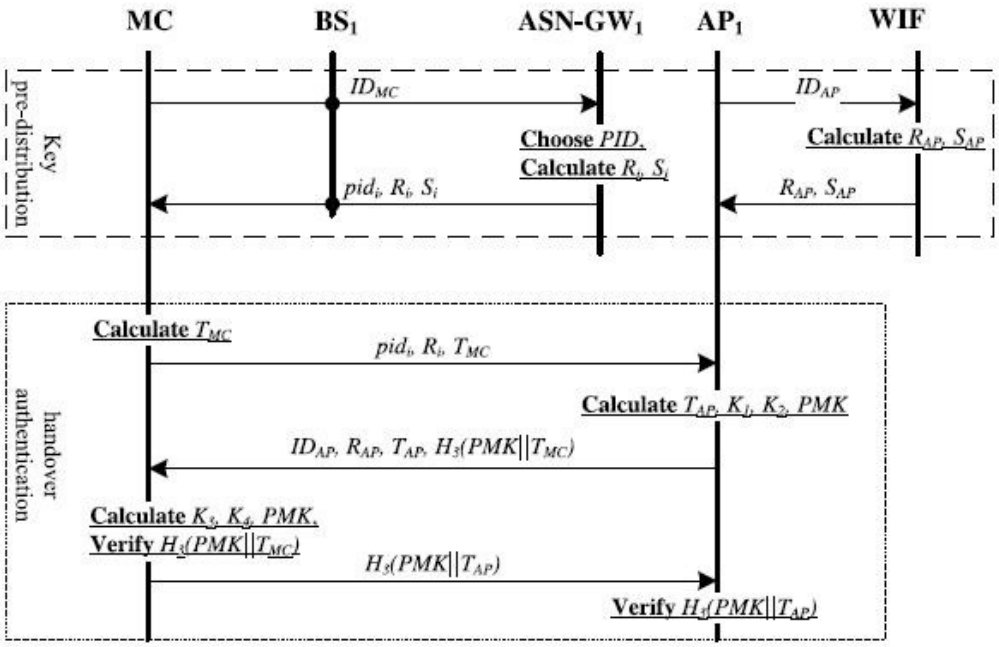
۷-رموز پیشین و پسین: یک دشمن نمی تواند از یک کلید جلسه ی در معرض خطر برای دستیابی به کلیدهای پیشینی که هر موقعیت آتی را محاسبه می کنند یا بکار می برند، استفاده کند.

۸-مقاومت هجوم: امنیت طرح تحت هجوم های مختلف، در معرض خطر قرار نخواهد گرفت.

همه ی این تجهیزات در طراحی طرح ما مورد توجه می باشند.

۳. طرح پیشنهادی

دراین بخش، ما جزییات طرح احرازهویت تحویل عمودی پیشنهادی خود را توصیف کرده ایم. این طرح همان طور که در شکل ۲ نشان داده شده است، شامل دو فاز، به نام های فاز کلید پیش توزیع و فاز احرازهویت تحویل می باشد. پیش از توصیف، کار را با گسترش اولیه شروع خواهیم کرد. نشان گذاری بکار رفته در این طرح نیز در جدول ۱ تعریف شده اند.



شکل ۲. احراز هویت تحویل وایمکس به وای فای

جدول ۱. نمادهایی در طرح

Notation	Description
q	A k-bit prime
F_q	A prime finite field
E/F_q	An elliptic curve E over F_q
G	$G = \{(x, y) : x, y \in E/F_q\} \cup \{\Theta\}$
P	Generator for the group G
T_{exp}	Expiration time
ID_x	Identity of entity x
$H_0()$	A secure hash function $H_0 : G \rightarrow \mathbb{Z}_q^*$
$H_1()$	A secure hash function $H_1 : \{0, 1\}^* \times G \rightarrow \mathbb{Z}_q^*$
$H_2()$	A secure hash function $H_2 : \{0, 1\}^* \times \{0, 1\}^* \times G \times G \rightarrow \{0, 1\}^k$
$H_3()$	A secure hash function $H_3 : \{0, 1\}^k \times G \rightarrow \{0, 1\}^k$
PK_x	Public key of entity x
(R_x, S_x)	Entity x's private long-term key

۳.۱. فاز گسترش اولیه

هدف این فاز مقداردهی اولیه ی سیستم، و آماده سازی برای تحویل و احراز هویت آینده می باشد.

مقداردهی اولیه ی سیستم: فرض می کنیم که AS فرآیند مقداردهی اولیه ی سیستم را برای شبکه های وایمکس و وای فای انجام خواهد داد. کار این فرآیند به شرح زیر می باشد:

(۱)چهار تابع ایمنی هش H۰، H۱، H۲ و H۳ را انتخاب کنید(تعریف هرکدام از این توابع در جدول ۱ آورده شده است).

(۲)یک بیت Kاول q را انتخاب کرده و تابع چند تایی زیر را تعیین کنید؛

{Fq,E/Fq,G,P}

(۳)دو عدد تصادفی را به ترتیب زیر انتخاب کنید،

r 1, r2 ϵ{0,1}*→Z*q

کلید عمومی r۱P ،r۲P را محاسبه کرده و مفهوم ایمنی (r۲P ، r۱) و (r۱P ،r۲) را برای ASN-GW و FIW را توزیع دهید. سپس به محاسبه ی کلید رمز s=H۰ (r۱ ،r۲P) بپردازید، و SP را همانند یک پارامتر سیستم توزیع دهید.

(۴) {H۳، H۲، H۱، H۰، Ps ،r۲P ،r۱P ، PG ،E/qF ،qF} رابه صورت پارامترهای سیستم منتشر کنید و کلید رمز {r۲، r۱} را حفظ کنید.

۳.۲. فاز احرازهویت تحویل عمودی

یک MC یک تحویل عمودی را هنگامی اجرا می کند که خواستار تغییر شبکه های در دسترس خود با توسعه ی شبکه های متجانس متفاوت باشد. با این حال، یک فرآیند پیش توزیع کلیدی درهمان لحظه با MC مقداردهی اولیه می شود. همان طور که در شکل ۲ نشان داده شده است، پیش از تحویل عمودی از وایمکس به وای فای، فاز کلیدی پیش توزیع وجود دارد.توصیفات جزیی احراز هویت تحویل به صورت زیر است.

*فاز کلیدی پیش توزیع: دراین فاز، همان طور که در شکل ۲ نشان داده است، هر AP پسین جهت جریان BS، پیش از احرازهویت تحویل، شاخص های IDAP رابه WIF ارسال می کند. سپس WIF یک عدد تصادفی از $r' \epsilon Z^*_q$ را انتخاب کرده و مقدار زیر را محاسبه می کند؛

$S=H_0 (r_2 r_1 P), R_{AP}=r'P, h_{AP}= H_1 (ID_{AP} || R_{AP}), S_{AP} = r'+h_{AP}S$

درپایان، WIF کلید چندتایی رمز درازمدت خود را جهت کاربرد پروتکل انتقال ایمن، به AP ارسال می کند. به طور مشابه، وقتی یک MC پیام درخواست به ASN-GW ارسال می کند، درابتدا باید اعتبار آن بررسی شود. اگر معتبر باشد، ASN-GW خانواده ای از آی دی های نامشابه را بر می گزیند. برای هرکدام از آنها عددی تصادفی انتخاب شده و مقادیر بالا محاسبه می شود. بدین ترتیب، MC می تواند برای دستیابی به شاخص حریم خصوصی و جایگاه آن در فاز احرازهویت تحویل، تغییر پایداری در آی دی داشته باشد.

*فاز احرازهویت تحویل: احرازهویت میان MC و AP/BS جدید باشد در این فاز انجام شود. کلید کارشناسی دوبه دو میان آنها به اشتراک گذاشته می شود و می تواند به طور مستقیم احرازهویت تحویل تولید کند. دراین جا، پیام های تبادل یافته میان تبادلات پروتکل احراز هویت تحویل ما بیان شده است.

(1) $MC \rightarrow AP_1: pid_i, R_i, T_{MC}$

پس از تکمیل کلید پیش توزیع قبلی، CM آمادگی احرازهویت دست به دست را خواهد داشت. یک رومینگ CM برای رده ی وای فای، از آی دی های بلااستفاده ی dip_iبهره می برد. بدین ترتیب با انتخاب یک مقدار تصادفی و محاسبه ی مقادیر بالا خواهیم داشت؛

(2) $AP_1 \rightarrow MC: ID_{AP}, R_{AP}, T_{AP}, H_3 (PMK||T_{MC})$

بدین ترتیب پیام های رسیده با انتخاب مقادیر تصادفی به محاسبه ی معادله ی بالا می پردازند. سپس کلید عمومی MC محاسبه شده، و کلیدهای به اشتراک گذاشته شده ی K_1 و K_2 و کلید جلسه ی PMK به صورت زیر نشان داده می شوند.

$$PK_{MC} = R_i + H_1(pid_i \parallel R_i)sP$$
$$K_1 = S_{AP}T_{MC} + bPK_{MC}, \qquad K_2 = bT_{MC}$$
$$PMK = H_2(pid_i \| ID_{AP} \| K_1 \parallel K_2)$$
$$(3)\ \underline{MC \rightarrow AP_1 : H_3(PMK \parallel T_{AP})}$$

پس از دریافت پیام از AP۱، MC درابتدا کلید عمومی خود را محاسبه می کند، رموز K۳ و K۴ را به اشتراک می گذارد و رموز به اشتراک گذاشته شده را برای تولید کلید جلسه ی PMK بکار می برد. سپس MC صحت H۳(PMK||T_{MC}) را تایید کرده و درصورت موفقیت آن را به مرحله ی بعد توزیع می کند. دراین مرحله، AP_1 با MC احرازهویت موفقیت آمیز خواهد داشت. به طور مشابه، با هدف احراز هویت AP، MC نیز برای تایید، H۳ (PMK||T_{AP}) را به PA_1 ارسال می کند.

$$PK_{AP} = R_{AP} + H_1(ID_{AP} \parallel R_{AP})sP$$
$$K_3 = S_i T_{AP} + aPK_{AP}, \qquad K_4 = aT_{AP}$$
$$PMK = H_2(pid_i \| ID_{AP} \| K_3 \parallel K_4).$$

درپایان، AP_1 دریافت می شود و $H3(PMK||T_{MC})$ را بررسی می کند. درصورتی که مقدار $H3 (PMK||T_{AP})$ صحیح باشد،MC با AP_1 به طور موفق، احرازهویت می شود. این عمل، احراز هویت را کامل می کند. و PMK جهت ارتباطات ایمن و جایگزین، یک کلید جلسه به اشتراک گذاشته شده میان MC و AP_1 خواهد بود.

۴. تحلیل ایمنی و اجرای ارزیابی

۴.۱. تحلیل ایمنی

ما ایمنی طرح پیشنهادی خود را با توجه به ایمنی تجهیزات بیان شده در بخش ۲ تحلیل می کنیم.

احرازهویت متقابل و کلید تثبیت: بنا بر وجود توافق صحیح میان AS، ASN-GW ، BS، WIF و AP در شبکه های متجانس وایمکس و وای فای، ما تنها احرازهویت متقابل میان CM و AP موجود در طرح پیشنهادی را مورد بحث قرار داده ایم. احراز هویت متقابل میان MC و AP_1 براساس تشخیص و مشکل CDH انجام می شود. MC و AP_1 مقادیر هش را از دیگر رمزهای به اشتراک گذاشته شده بررسی می کنند، این مقادیر در زیر نشان داده شده اند:

$$\begin{aligned} K_1 &= S_{AP}T_{MC} + bPK_{MC} \\ &= S_{AP}aP + b(R_i + H_1(pid_i \parallel R_i)sP) \\ &= S_{AP}aP + S_ibP \\ &= S_ibP + a(S_{AP}P) \\ &= S_iT_{AP} + aPK_{AP} \\ &= K_3 \end{aligned}$$

$$K_2 = bT_{MC} = baP = aT_{AP} = K_4.$$

بنابراین، کلید جلسه ی به اشتراک گذاشته شده ی PMK برای MC و AP_1 می تواند به صورت زیر محاسبه شود:

$$\begin{aligned} PMK &= H_2(pid_i \| ID_{AP} \| K_1 \parallel K_2) \\ &= H_2(pid_i \| ID_{AP} \| K_3 \parallel K_4). \end{aligned}$$

نتیجتا"، تنها تثبیت MC یاAP_1 می تواند مقادیر هش معتبری را برای دستیابی به احرازهویت متقابل تولید کند، و کلید جلسه ی PMK را ثبت کند.

امتیاز الحاقی: پس از موفقیت کلید پیش توزیع، ASN-GW و امتیاز الحاقی WIF برای MC و AP های آتی با کلید رمز درازمدت همراه می باشند. یک MC (یا AP) درصورتی می تواند یک احرازهویت تحویل را کامل کند که کلیدهای رموز درازمدت با یک ASN-GW (یا WIF) به صورت صحیح تولید می شوند. دشمنی که دانش کلیدهای رموز درازمدت MC و AP را ندارد، نمی تواند درخواست کد احرازهویت را ثبت کند.

یکپارچگی داده ها: براساس آنچه که در بالا بر کلیدها توافق شده است، کلیدهای رموز درازمدت جهت تثبیت صحت متقابل میان MC و AP ایجاد شده اند. جلسات تازمانی می توانند با کلیدهای رموز درازمدت حفظ شوند که احراز هویت متقابل تکمیل شود. پس از احراز هویت متقابل، MC و AP می توانند از کلید جلسه ی به اشتراک گذاشته شده ی PMK چشم پوشی کنند. درنتیجه، بنا بر کلیدهای رمز درازمدت و کلید جلسه ی PMK ، داده های انتقال یافته در شبکه نمی توانند برای دشمن سودمند باشند.

ناشناس ماندن و عدم قابلیت ردیابی کاربر: در طرح ما، هر MC خانواده ای از آی دی ها را دریافت می کند و پیش از جایگاه احرازهویت تحویل، آن را با کلید های رمز درازمدت تطبیق می سازد. این آی دی ها، به جای تشخیص حقیقی MC ، با هدف حفظ حریم شخصی، در فاز احرازهویت تحویل بکار می روند. بنا براین، تنها ASN-GW دارای دانش ارتباط میان یک آی دی و تشخیص حقیقی می باشد. درکنار این موارد، ازآنجا که هیچ ارتباطی میان آی دی ها وجود ندارد- به جز ASN-GW و MC - APها نیز توانایی تشخیص MC یا ارتباط میان دو جلسه مقداردهی شده با MC مشابه را نخواهند داشت.

رمز پسین و پیشین: رمز پسین و پیشین بدین معناست که اگر یک کلید رمز دراز مدت در هر نقطه از زمان در معرض خطر قرار گیرد، اثر ایمن نخواهد داشت. ما در طرح خود کلید تبادل دیفی-هلمن را در یک روش احراز هویت اجرا کرده ایم. پارامترهای معمولی دیفی-هلمن بکار رفته در ساختار یک کلید جلسه، به صورت تصادفی و با MC و APمستقل انتخاب شده اند. بنابراین، با مقایسه ی کلیدهای رمز درازمدت یا کلیدهای جلسه، دشمن نمی تواند تاریخ جلسات را پوشش دهد، به عبارت دیگر، پروتکل پیشنهادی ما می تواند رمز پسین و پیشین را بدست آورد.

مقاومت هجوم: طرح ما می تواند دربرابر انواع هجوم مقاوم باشد. برای استراق سمع، داده های انتقال یافته در ارتباط تثبیت شده ی جدید در محیط وایرلس می توانند توسط هجوم کننده تسخیر شوند، بدین ترتیب هجوم کننده ها نمی توانند به محتوای بسته دست یابند، زیرا محتوای بسته با رمز گذاری PMK حفظ شده است. پاسخ هجوم کننده نیز در طرح ما انعطاف پذیر است، زیرا مقادیر تصادفی در هر پیام تبادل یافته افزوده می شوند، و این پیام ها ازطریق کلیدهای رموز درازمدت توسط MC و AP تایید می شوند. تالیف MC و AP برای دریافت اطلاعات، تنها با تثبیت کاربرانی که می توانند اعتبار کلید رمز درازمدت را با ASN-GW و WIF استنتاج کنند، پیشگیری می شود.

۴.۲. ارزیابی اجرایی

دراین بخش، اجرای طرح خود رااز چندین جنبه –شامل عملکرد و اجرا- تحلیل کرده و آن را با طرح های دیگر مقایسه خواهیم کرد. همان طور که در جدول ۲ نشان داده شده است، مقایسه ی عملکرد و اجرا شامل بخش اعداد، کلیت، کاربر ناشناس، عدم قابلیت ردیابی، ارتباطات اضافه، و محاسبات اضافه، می باشد.

ارتباطات اضافه، زمان تحویل در احرازهویت و روش کلید توزیع را بیان می کند. دراین جا، فرض می کنیم که هزینه ی ارتباطات میان MC و AP/BS ، مقدار α، و هزینه ی میان ASN-GW/ WIF و AP/BS ، مقدار β، و هزینه ی میان AP/BS و سرور AAA، مقدار Υ می باشد. محاسبه ی اضافه تاخیر پردازش عملکرد رمزگذاری در هر مورد را نشان می دهد. ما تنها هزینه ی کاربردها را به صورت (T_E، T_D، T_S، T_H، T_M) فهرست کرده ایم، که درآن زمان برای یک MC کاربردی به صورت T_M، زمان کاربرد هش به صورت T_H، زمان رمزگذاری/ رمزنگاری به صورت T_S، زمان تابع استنتاج کلید به صورت T_D و زمان منحنی چندکاربردی به صورت T_E، معنا شده است.

جدول ۲. مقایسه عملکرد بین پروتکل های مختلف تحویل

Protocols	No. P	Univ.	Ano./Unt.	Commun.	Comput.
Shidhani [11]	5	No	No/No	$10\alpha + 4\beta + 4\gamma$	(10, 6, 8, 14, 0)
Huang [3]	3	No	No/No	$5\alpha + 2\beta$	(8, 0, 4, 6, 0)
Fu [14]	3	No	No/No	$4\alpha + 2\beta$	(8, 2, 4, 8, 0)
Cao [16]	2	Yes	No/No	3α	(0, 8, 2, 1, 2)
Yang [15]	2	Yes	Yes/No	3α	(0, 0, 6, 3, 2)
Our scheme	2	Yes	Yes/Yes	3α	(0, 8, 0, 0, 2)

در جدول ۲ می توان مشاهده کرد که طرح ما همه ی تجهیزات عملکرد و اجرا را دارا می باشد و از دیگر طرح ها موثرتر می باشد. به طور ویژه، محاسبه ی اضافه در مقایسه با طرح های موجود، دارای یک مزیت کامل می باشد، زیرا طرح ما برای تکمیل احراز هویت تحویل بدون رمزنگاری یا رمزگشایی، تنها به دو کاربرد ECSM نیاز دارد. به طور کلی، طرح ما بهتر از سایر طرح های پیشنهاد شده درک می شود.

۵. جمع بندی

دراین تحقیق، ما پروتکلی برای دستیابی به احرازهویت تحویل کارآمد جهت الگوی محاسبه ی رایانش ابری، پیشنهاد داده ایم. این پروتکل مزایایی دارد که می توان آنها کلی بودن، امنیت قوی، و کارآمد بودن، خلاصه کنیم. ایمنی و تحلیل اجرایی نشان می دهد که طرح پیشنهاد شده ناشناس ماندن کاربر و عدم قابلیت ردیابی با بهترین اجرا رابه همراه دارد. با این مزایا، ما بر توسعه پذیری پیشنهادات جدید در MCC اعتقاد داریم.

منابع

[1] J.K. Liu, M.H. Au, W. Susilo, K. Liang, R. Lu, B. Srinivasan, Secure sharing and searching for real-time video data in mobile cloud, IEEE Network 29 (2015) 46–50.
[2] W.F.N.W. Group, et al. Wimax forum network architecture—stage 3: Detailed protocols and procedures—release 1, version 1.2, in: WiMAX Forum, January.
[3] K.-L. Huang, K.-H. Chi, J.-T. Wang, C.-C. Tseng, A fast authentication scheme for wimax–wlan vertical handover, Wirel. Pers. Commun. 71 (2013) 555–575.
[4] J.W. Floroiu, R. Ruppelt, D. Sisalem, J. Voglimacci, Seamless handover in terrestrial radio access networks: a case study, IEEE Commun. Mag. 41 (2003) 110–116.
[5] H. Kwon, K.-y. Cheon, K. Roh, A. Park, Usim based authentication test-bed for UMTS-WLAN handover, in: Proceedings of IEEE Infocom.
[6] H. Liming, K.X. Miao, A pre-authentication architecture in WiFi&WiMAX integrated system, in: Communications and Networking in China, 2009. ChinaCOM 2009, Fourth International Conference on, IEEE, pp. 1–5.
[7] H.-M. Sun, S.-M. Chen, Y.-H. Chen, H.-J. Chung, I.-H. Lin, Secure and efficient handover schemes for heterogeneous networks, in: Asia–Pacific Services Computing Conference, 2008, APSCC'08, IEEE, pp. 205–210.
[8] Y. Zhang, N. Ansari, H. Tsunoda, Wireless telemedicine services over integrated IEEE 802.11/Wlan and IEEE 802.16/WiMAX networks, IEEE Wirel. Commun. 17 (2010) 30–36.
[9] C. Ntantogian, C. Xenakis, One-pass eap-aka authentication in 3G-WLAN integrated networks, Wirel. Pers. Commun. 48 (2009) 569–584.
[10] J.Y. Kim, S.U. Shin, et al., Authentication mechanism for fast handoff in CDMA2000-wibro interworking, Sci. China Ser. F: Inform. Sci. 53 (2010) 137–146.
[11] A.A. Al Shidhani, V.C. Leung, Fast and secure reauthentications for 3GPP subscribers during WiMAX–WLAN handovers, IEEE Trans. Depend. Secure Comput. 8 (2011) 699–713.
[12] Q. Han, Y. Zhang, X. Chen, H. Li, J. Quan, Efficient and robust identity-based handoff authentication in wireless networks, in: Proc. 6th Int. Conf. Network and System Security, Springer, 2012, pp. 180–191.
[13] Y. Zhang, X. Chen, H. Li, J. Cao, Identity-based construction for secure and efficient handoff authentication schemes in wireless networks, Secur. Commun. Netw. 5 (2012) 1121–1130.
[14] A. Fu, G. Zhang, Z. Zhu, Y. Zhang, Fast and secure handover authentication scheme based on ticket for WiMAX and WiFi heterogeneous networks, Wirel. Pers. Commun. 79 (2014) 1277–1299.
[15] G. Yang, Q. Huang, D.S. Wong, X. Deng, Universal authentication protocols for anonymous wireless communications, IEEE Trans. Wirel. Commun. 9 (2010) 168–174.
[16] J. Cao, M. Ma, H. Li, An uniform handover authentication between e-utran and non-3GPP access networks, IEEE Trans. Wirel. Commun. 11 (2012) 3644–3650.
[17] Y. Zhai, X. Mao, Y. Wang, J. Yuan, Y. Ren, A DHT-based fast handover management scheme for mobile identifier/locator separation networks, Sci. China Inf. Sci. 56 (2013) 1–15.
[18] Y. Cao, C. Xu, J. Guan, H. Zhang, QoS-driven sctp-based multimedia delivery over heterogeneous wireless networks, Sci. China Inf. Sci. 57 (2014) 1–10.
[19] J.K. Liu, C. Chu, S.S.M. Chow, X. Huang, M.H. Au, J. Zhou, Time-bound anonymous authentication for roaming networks, IEEE Trans. Inform. Forensics Secur. 10 (2015) 178–189.
[20] M.J. Sharma, V.C. Leung, Improved IP multimedia subsystem authentication mechanism for 3G-WLAN networks, Int. J. Secur. Netw. 6 (2011) 90–100.