Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 12, Number 4, Winter 2023, pp. 12-22
Received: 04/08/2022, Revised: 08/02/2023, Accepted: 02/16/2024

A Location Aware Lightweight Mutual Authentication for Internet of Things

Ali Mazandarani[1], Mohammad Taghi Kheirabadi [2*] and Amin Bazzazi[3]
1- Faculty of Engineering, Islamic Azad University, Gorgan Branch, Gorgan, Iran.
2*- Faculty of Engineering, Islamic Azad University, Gorgan Branch, Gorgan, Iran.
3- Faculty of Engineering, Islamic Azad University, Gorgan Branch, Gorgan, Iran.
[1]mazandarani.110@gmail.com, [2*]mt.kheirabadi@iau.ac.ir, and [3]amin.bazzazi@iau.ac.ir

Corresponding author's address: Mohammad Taghi Kheirabadi, Faculty of Engineering, Islamic Azad University, Gorgan Branch, Gorgan, Iran.

Abstract- Nowadays, The Combination of Information Technology and Communication, artificial intelligence, Internet of Things (IoT), blockchain, and other new technologies has led to the emergence of the Fourth Industrial Revolution, which has brought about profound changes in human life. The Internet of Things has evolved from equipping devices around humans with sensors, actuators, advanced chips, and intelligent algorithms that connect to the Internet and communicate with other devices or humans independently. Due to independence of smart devices in the IoT, security is one of the most important issues in the IoT debate. IoT security mechanisms should not only address traditional security attacks, but should also provide secure connections for both machine-to-human and machine-to-machine communication. Authentication of Devices is one of the most important issues in IoT Security. Therefore, in this paper, a location-aware mutual authentication protocol is proposed for IoT systems. In this protocol, entities can authenticate each other and attain a shared secret session key. In the production of this key, the information of the devices, their location and the type of devices in terms of being fixed or mobile have been used. .Then, this key is used to authenticate devices before sending information over wireless channels.

To prove the correctness and lightness of the proposed protocol, Experiments were performed and the results show that adding the location parameter to the authentication protocol has increased the security strength of the protocol and communication and computing costs have not increased significantly.

Keywords- Authentication, Security, Internet of Things, Lightweight Protocol.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: www.jscit.ac.ir
شناسگر اشیاء دیجیتالی (DOI) :
جلد ۱۲، شماره ۴، زمستان ۱۴۰۲، صفحه ۱۲-۲۲
دریافت: ۱۴۰۱/۰۱/۱۹ بازنگری: ۱۴۰۲/۰۵/۱۱ پذیرش:۱۴۰۲/۱۱/۲۷

یک پروتکل احراز هویت سبک وزن آگاه از مکان برای اینترنت اشیاء

علی مازندرانی [۱]، محمدتقی خیرآبادی*[۲]، امین بزازی[۳]
۱- دانشکده فنی مهندسی، دانشگاه آزاد اسلامی واحد گرگان، گرگان، ایران.
*۲- دانشکده فنی مهندسی، دانشگاه آزاد اسلامی واحد گرگان، گرگان، ایران.
۳- دانشکده فنی مهندسی، دانشگاه آزاد اسلامی واحد گرگان، گرگان، ایران.
[1]mazandarani.110@gmail.com, [2*] mt.kheirabadi@iau.ac.ir, [3]amin.bazzazi@iau.ac.ir

* نشانی نویسنده مسئول: محمد تقی خیرآبادی، گرگان، خیابان دانشجو، دانشگاه آزاد اسلامی واحد گرگان، دانشکده فنی مهندسی.

چکیده- امروزه، تلفیق فناوری اطلاعات و ارتباطات، هوش مصنوعی، اینترنت اشیاء (IoT)، بلاک‌چین، و دیگر تکنولوژی‌های نوین منجر به ظهور انقلاب صنعتی چهارم شده و تغییرات گسترده و عمیقی در زندگی بشر به‌وجود آورده است. اینترنت اشیاء از تجهیز وسایل پیرامون انسان‌ها به حسگرها، محرک‌ها، تراشه‌های پیشرفته و الگوریتم‌های هوشمند به‌وجود آمده است به‌طوریکه این وسایل به اینترنت نیز متصل بوده و از طریق آن با سایر وسایل یا انسان‌ها بطور مستقل ارتباط برقرار می‌کنند. با توجه به استقلال وسایل هوشمند در اینترنت اشیاء، تامین امنیت یکی از مهمترین مسائل در بحث اینترنت اشیاء می‌باشد. مکانیزم‌های امنیتی در اینترنت اشیاء نه تنها باید حملات امنیتی سنتی را مورد توجه قرار دهند، بلکه بایستی ارتباطات امنی برای هر دو نوع ارتباط ماشین با انسان و ماشین با ماشین را فراهم نمایند. احراز هویت دستگاه‌ها یکی از مهمترین مسائل در بحث امنیت اینترنت اشیاء می‌باشد. از این رو، در این مقاله یک پروتکل احراز هویت متقابل آگاه از مکان برای سیستم‌های اینترنت اشیاء پیشنهاد شد. در این پروتکل، موجودیت‌ها می‌توانند یکدیگر را احراز هویت نموده و به یک کلید جلسه مخفی مشترک دست یابند. در تولید این کلید، از اطلاعات دستگاه‌ها، مکان آن‌ها و نوع دستگاه‌ها از نظر ثابت یا سیار بودن استفاده شده است. از این کلید برای احراز هویت دستگاه‌ها قبل از ارسال اطلاعات بر روی کانال‌های بی‌سیم استفاده می‌شود. جهت اثبات درستی و سبک بودن پروتکل پیشنهادی، آزمایش‌هایی صورت گرفت. نتایج بدست آمده از آزمایش‌ها نشان می‌دهد که افزودن پارامتر موقعیت مکانی به پروتکل احراز هویت منجر به افزایش قدرت امنیتی پروتکل گردیده در حالیکه هزینه‌های ارتباطی و محاسباتی افزایش قابل توجهی نداشته است.

واژه‌های کلیدی: احراز هویت، امنیت، اینترنت اشیاء، پروتکل سبک وزن.

۱- مقدمه

یکی از مهمترین تحولات در انقلاب صنعتی چهارم، بحث هوشمند سازی اشیاء و امکان تعامل اشیاء با یکدیگر و انسان از طریق شبکه اینترنت می‌باشد. استفاده از این تکنولوژی‌ها منجر به تحولات شگرفی در زندگی بشر امروز شده است. اینترنت اشیاء در واقع ترکیبی از فناوری‌های نوین با اینترنت سنتی است که با تجهیز اشیاء فیزیکی به حسگرها، محرک‌ها و تراشه‌های پیشرفته و اینترنت، منجر به هوشمندتر شدن این اشیاء می‌شود. این اشیاء هوشمند از طریق اینترنت، قادر به مبادله داده‌ها میان خود و سایر دستگاه‌ها بدون مداخله انسان می‌باشند[۱]. این تجهیزات هوشمند روز به روز در حال افزایش بوده و بخش بزرگی از زندگی کنونی بشر را تغییر داده و آن را راحت‌تر کرده است [۲]. با توجه به استقلال این اشیاء از انسان، یکی از مهمترین مسائلی که به‌طور بالقوه دستگاه‌های اینترنت اشیاء را تهدید می‌کند، بحث امنیت و حریم خصوصی داده‌های رد و بدل شده از طریق این دستگاه‌ها می‌باشد. زیرا بسیاری از داده‌های مبادله شده بین دستگاه‌ها اطلاعات شخصی و یا امنیتی بوده و عمیقاً با زندگی کاربران و یا سازمان‌ها و نهادها مرتبط می‌باشد[۳]. یکی از جدی ترین تهدیدهای امنیتی برای هر دستگاه رایانه‌ای جعل هویت کاربر مجاز است [۴]. هدف اصلی احراز هویت اطمینان از این موضوع است که دستگاهی که در حال حاضر قصد مبادله اطلاعات با دستگاه دیگر را دارد دارای هویت واقعی است و دستگاه یا شخص دیگری با هویت جعلی اقدام به مبادله اطلاعات ننموده است. لذا احراز هویت کاربر، اولین خط دفاع در برابر جعل هویت کاربران و یک مؤلفه اصلی در هر زیرساخت امنیتی می‌باشد [۵]. طراحی پروتکل‌های احراز هویت قوی و سبک وزن یکی از چالش‌های اصلی در اینترنت اشیاء می‌باشد، زیرا در اینترنت اشیاء، معمولا اشیاء از نظر ظرفیت محاسبه، حافظه و انرژی دارای محدودیت منابع می‌باشند و این مسئله سبب ناکارامد بودن راه‌حل‌های امنیتی موجود سنتی می‌شود چون به منابع نسبتا زیادی نیاز دارند [۶]. احراز هویت متقابل یا دوطرفه یکی از انواع فرآیندهای احراز هویت است که در آن موجودیت‌ها قبل از آغاز ارتباط نهایی به کمک گواهی‌های دیجیتال، یکدیگر را احراز هویت می‌کنند. در این نوع احراز هویت، اتصال تنها زمانی رخ می‌دهد که موجودیت‌ها، گواهی‌های خود را میان یکدیگر مبادله و مورد تایید قرار دهند. از جمله کارهای انجام شده با این نوع احراز هویت می‌توان به پروتکل SEGR اشاره داشت که توسط لای و همکاران [۷] ارائه شده است. لای و همکاران [۸] پروتکل دیگری با نام GLRAM بر پایه احراز هویت متقابل ارائه دادند. سان و همکاران [۹] پروتکل احراز هویت متقابل در سرویس خانگی ارائه دادند. ژو و همکاران [۱۰] پروتکل احراز هویتی دوعاملی به نام Duth ارائه دادند، چانگ و همکاران [۱۱] و داس و همکاران [۱۲] پروتکل‌های امنی برپایه PUF[1] ارائه کرده‌اند. همچنین داس و همکاران [۱۳] پروتکل احراز هویت بر پایه PUF برای دستگاه‌های پوشیدنی[2] ارائه کردند. لی و همکاران [۱۴] پروتکل احراز هویت متقابلی جهت ارتباط میان گره‌های درون شبکه با یکدیگر ارائه دادند. ملکی و همکاران [۱۵] جهت ارتباط اشیاء، پروتکل احراز هویت متقابل ارائه دادند. در سال ۲۰۲۰ پروتکل احراز هویت گروهی و توزیع کلید بر پایه PUF توسط یلدیز و همکاران [۱۶] ارائه شده است. در پروتکل‌های احراز هویت در محیط اینترنت اشیاء باید ویژگی‌های اشیاء از جمله محدودیت در توان پردازشی و فضای ذخیره‌سازی مورد توجه قرار گیرد. اما یکی دیگر از مشخصه‌های اشیاء در اینترنت اشیاء استفاده از موقعیت مکانی اشیاء در احراز هویت است که تحقیقات کمی به آن توجه کرده‌اند. توجه به نوع اشیاء از نظر تحرک و موقعیت مکانی اشیاء می‌تواند منجر به جلوگیری از برخی حملات و نفوذ به اشیاء گردد. با توجه به موارد ذکر شده مهمترین کارهای انجام شده در این مقاله به شرح زیر می‌باشد

- دسته‌بندی اشیاء به گروه‌های سیار و غیرسیار جهت استفاده از اطلاعات مکان اشیاء در احراز هویت.
- ارائه یک پروتکل احراز هویت آگاه از مکان بر اساس نوع اشیاء از نظر سیار یا ثابت بودن.
- ارزیابی پروتکل پیشنهادی از نظر هزینه محاسباتی و ارتباطی و زمان اجرا.

در ادامه این مقاله، در بخش دوم، مروری بر کارهای پیشین صورت خواهد گرفت. بخش سوم به معرفی پروتکل پیشنهادی پرداخته و در بخش چهارم ارزیابی پروتکل پیشنهادی انجام می‌شود. نهایتا در بخش پنجم نتیجه‌گیری و کارهای آتی بیان می‌شود.

۲- پیشینه تحقیق

در سال‌های اخیر تحقیقات بسیاری در مورد پروتکل‌های احراز هویت متقابل وتبادل کلید در اینترنت اشیاء انجام شده است که در این قسمت برخی از این مقالات که عملکرد تقریباً مشابه با روش پیشنهادی دارند، مورد بررسی قرار خواهند گرفت.

در سال ۲۰۱۴، لای و همکاران [۷] برای ارتباط دستگاه‌های 3GPP-WiMAX پروتکلی با نام SEGR پیشنهاد دادند. این پروتکل، به منظور دستیابی به احراز هویت متقابل و توافق کلیدی بین کلیه دستگاه‌های ارتباطی ارائه شد و از نظر برقراری ارتباط در مقایسه با طرح احراز هویت فراگردی[3] سنتی و طرح احراز هویت فراگردی بهینه در کار فو و همکاران [۱۷] عملکرد بهتری دارد همچنین

پیچیدگی محاسبات آن در مقایسه با طرح بدون تجمع کارآمدتر است. از معایب این طرح می‌توان به عدم مطالعه مقاومت در برابر حملات و عدم تحلیل حفظ حریم خصوصی در مقایسه با طرح لای و همکاران [۸] اشاره کرد. همچنین هزینه‌های ذخیره‌سازی نیز در آن در نظر گرفته نشده است.

لای و همکاران [۸] پروتکلی جهت تضمین احراز هویت متقابل موجودیت‌ها به همراه یک توافق نامه مبتنی بر کلید امن پیشنهاد دادند. این پروتکل بر پایه استاندارد 3GPP برای سه دامنه مختلف ارائه شد. نتایج ارزیابی این پروتکل نشان می‌دهد که سربار محاسباتی آن نسبتاً کم بوده و پیچیدگی محاسبات آن نیز بسیار کمتر از طرح‌های کائو و همکاران [۱۸]، لای و همکاران [۱۹] و لای و همکاران [۷] می‌باشد و می‌تواند کیفیت سرویس را برای دستگاه‌های ارتباطی تضمین کند. این پروتکل در مقابل حملات انکار سرویس، مرد میانی و تغییر مسیر مقاوم است. از معایب آن می‌توان به عدم توجه به هزینه‌های ذخیره‌سازی و برخی از مدل‌های حریم خصوصی مانند حریم خصوصی مکان و حریم خصوصی هویت اشاره کرد.

ژو و همکاران [۱۰] بدون افزودن دستگاه سخت‌افزاری اضافی، یک طرح احراز هویت دو عاملی به نام Duth برای دستگاه‌های هوشمند اندرویدی پیشنهاد کردند. این طرح از دو فرآیند اصلی تشکیل شده است. فرایند اول وظیفه استخراج مجموعه‌ای از ویژگی‌ها و ذخیره‌سازی آنها را برای ثبت نام برعهده دارد و در فرایند دوم احراز هویت دو عاملی صورت می‌گیرد. طرح Duth می‌تواند نیازهای کاربر پسند را همراه با یک نرخ عدم پذیرش اشتباه[۴] معقول، برآورده سازد و همزمان یک فرآیند احراز هویت برای دستگاه‌های هوشمند اندرویدی ارائه دهد.

سان و همکاران [۹] پروتکلی به منظور دستیابی به یک فرآیند احراز هویت متقابل در سرویس شبکه خانگی M2M یا ماشین به ماشین[۵] ارائه دادند. در مدل شبکه مورد استفاده آن‌ها، کاربران تلفن همراه، دروازه‌های خانگی و یک سرویس‌دهنده M2M وجود داشت. از مزایای این طرح می‌توان به کارآمدی آن در مقایسه با پروتکل پیشنهادی جیونگ و همکاران [۲۰] از نظر میزان محاسبه و حجم ارتباط اشاره کرد. همچنین مقاومت این طرح در برابر حمله حدس‌زدن، حمله جعل هویت و حمله مجدد مناسب است. از مهمترین معایب این طرح می‌توان به ضعف در مقابل حمله انکار سرویس در مقایسه با طرح PBA [۲۱]، در نظر نگرفتن هزینه‌های ذخیره‌سازی، و عدم تجزیه و تحلیل حفظ حریم خصوصی در مقایسه با طرح GLARM در کار لای و همکاران [۸] اشاره کرد.

داس و همکاران [۱۳] یک پروتکل احراز هویت برپایه PUF برای دستگاه‌های پوشیدنی ارائه دادند. این پروتکل، به دستگاه‌های پوشیدنی و پایانه‌های تلفن همراه که توسط کاربر پوشیده یا حمل می‌شوند، اجازه می‌دهد تا یکدیگر را احراز هویت نموده و یک کلید جلسه محرمانه بین یکدیگر به اشتراک بگذارند تا از آن کلید برای ایمن سازی ارتباطات بین خود استفاده نماید. در این پروتکل برای رسیدن به سطح امنیت بالا و کاهش پیچیدگی از محاسبات رمزنگاری سبک وزن از قبیل توابع درهم‌ساز و عملیات XOR استفاده شده است. در این پروتکل هفده تابع درهم‌ساز جهت رسیدن به یک احراز هویت امن میان دو موجودیت نیاز است که این تعداد محاسبات برای دستگاه‌های اینترنت اشیاء با محدودیت منابع انرژی، محاسباتی و ذخیره‌سازی بسیار بالا بوده و منجر به ناکارآمدی طرح پیشنهادی خواهد شد.

داس و همکاران [۱۲] و چانگ و همکاران [۱۱] نیز پروتکل‌های امنی برپایه PUF ارادە دادند که به‌ترتیب به ۳۱ و ۱۹ تابع درهم‌ساز جهت رسیدن به احراز هویت امن نیاز دارند که این موضوع منجر به بالارفتن هزینه‌های محاسباتی و بالارفتن سطح پیچیدگی در این پروتکل‌ها شده است.

لی و همکاران [۱۴]، یک پروتکل متقابل احراز هویت و تبادل کلید مبتنی بر PUF انتها به انتها ارائه دادند. پروتکل پیشنهادی آنها از PUF و رمزنگاری کلید عمومی بدون گواهی بر روی منحنی بیضوی استفاده می‌کرد. در این پروتکل، هر گره جدید در مرحله ثبت نام با سرویس‌دهنده ارتباط برقرار نموده و کلید عمومی و خصوصی خود را دریافت می‌کرد. بعد از آن، ارتباط با سایر دستگاه‌های درون شبکه، احراز هویت و تبادل پیام بدون مشارکت سرویس‌دهنده صورت می‌گرفت. حذف سرویس‌دهنده در مرحله احراز هویت میان دستگاه‌ها باعث کاهش هزینه ارتباطی پروتکل پیشنهاد شد. از دیگر مزایای پروتکل پیشنهادی می‌توان به نداشتن مشکل در سپردن کلید، امنیت کلید جلسه و محرمانگی آن اشاره کرد.

ملکی و همکاران [۱۵] یک پروتکل احراز هویت چندعاملی متقابل بنام L2MAP برای تجهیزات اینترنت اشیاء پیشنهاد دادند. طرح پیشنهادی آنها به موجودیت‌های اینترنت اشیاء این امکان را می‌دهد تا به صورت متقابل یکدیگر را مورد احراز هویت قرار داده و در مورد یک کلید جلسه مخفی به توافق برسند. این کلید برای ایمن سازی و احراز هویت اطلاعات منتقل شده بر روی کانال‌های وای-فای عمومی استفاده می‌شود. این طرح بر پایه دو مفهوم توابع فیزیکی غیرقابل شبیه‌سازی داخل تجهیزات IOT یعنی PUF و همچنین پارامترهای مبتنی بر کانال استوار است. در این پروتکل، خروجی منحصر به فرد PUF به‌عنوان شناسه مخفی متقابل بین یک جفت

دستگاه استفاده می‌شود که در هر جلسه تغییر می‌کند. علاوه بر این، پروتکل پیشنهادی از ویژگی‌های کانال تصادفی برای ایجاد مقاومت بالا در برابر انواع مختلف حملات بهره می‌برد تا پیچیدگی را کاهش دهد. دلیل سبک بودن طرح پیشنهادی استفاده از تعداد محدودی عملیات ساده XOR بیتی و تابع درهم‌ساز یکطرفه در پیام‌های ارتباطی است که آن را برای محیطهای اینترنت اشیاء با محدودیت منابع مناسب می‌کند. همچنین در این کار، یک طرح نوین برای محرمانگی اطلاعات فیزیکی و یکپارچگی پیام مطرح شده است که پس از احراز هویت اولیه و توافق کلید اجرا می‌شود. تجزیه و تحلیل امنیتی غیر رسمی، ارزیابی امنیتی و برهان‌های ریاضی اثبات می‌کنند که طرح پیشنهادی در برابر حملات احراز هویت مختلف ایمن و محکم بوده و از راه حل‌های موجود بهتر عمل می‌کند، زیرا دارای هزینه‌های ارتباطی و محاسباتی کم است از معایب این پروتکل می‌توان به عدم در نظر گرفتن شبکه‌هایی با گره‌های تجمیعی و همچنین عدم توجه به موقعیت مکانی گره‌ها در درون پروتکل اشاره کرد.

PLGAKD پروتکل سبک وزن احراز هویت گروهی و توزیع کلیدی است که بر پایه PUF بوده و توسط یلدیز و همکاران [۱۶] ارائه شده است. در این پروتکل از PUF، درخت فاکتوریل[۶] و قضیه باقیمانده چینی[۷] استفاده شده است. بکار گیری PUF منجر به تسهیل احراز هویت و توزیع کلید در اعضای گروه شده است و استفاده از درخت فاکتوریل باعث کاهش تعداد کلید ذخیره شده در هر گره و همچنین کاهش تعداد پیام‌های ارتباطی و فضای ذخیره‌سازی شده است.

۳- روش پیشنهادی

پروتکل احراز هویت پیشنهادی در این مقاله، بر پایه پروتکل پیشنهاد شده در کار ملکی و همکاران [۱۵] است. پروتکل پیشنهادی از سه فاز مقدار دهی اولیه، توافق کلید، و تبادل اطلاعات تشکیل شده است که در ادامه به تفضیل شرح داده می‌شود.

۳-۱- مدل شبکه پیشنهادی

شکل ۱ مدل شبکه ارتباطی در این تحقیق را نشان می‌دهد. همانطورکه در شکل مشاهده می‌شود، مدل ارتباطی براساس توپولوژی ستاره بوده و در آن چندین دستگاه سیار و ساکن می‌توانند با واحد ارتباطی ثابت (دروازه/سرویس‌دهنده) به‌صورت مستقیم ارتباط برقرار کنند. فرضیات زیر در این مدل ارتباطی در نظر گرفته شده است:

- دروازه در درون سرویس‌دهنده شبکه قرار دارد و کاربران یا اشیاء می‌توانند به‌طور مستقیم از طریق سرویس‌دهنده عملیات احراز هویت را انجام دهند.
- گره‌های تجمیعی در نظر گرفته نشده اند.



شکل ۱: مدل شبکه پیشنهادی.

- کانال بین دو کاربر دوجانبه نیست.
- دروازه دارای حافظه زیاد و توان محاسباتی بالا بوده و مسئول ذخیره‌سازی مقادیر ورودی مختلف به PUF است که این مقادیر متعلق به اشیاء مختلف در شبکه است.
- شناسه‌های مخفی جلسه (ID_s) از خروجی PUF مشتق شده‌اند.
- دروازه، چالش/پاسخ‌های آغازین برای هر وسیله را ذخیره می‌کند و در ادامه برای هر جلسه احراز هویت، یک چالش/پاسخ تازه تولید و در یک روش امن و همگام سازی شده بروز رسانی می‌شود.
- شناسه‌های مخفی جلسه (IDs) توسط طرفین مخفی نگه داشته می‌شود.
- کلیه گره‌های موجود در شبکه امکان بدست آوردن موقعیت مکانی خود را به کمک GPS دارند.
- اطلاعات GPS دریافتی به صورت دقیق در نظر گرفته شده است و از خطاهای احتمالی آن چشم پوشی شده است.
- وضعیت سیار یا عدم سیار بودن وسیله در سرویس‌دهنده و دستگاه ذخیره می‌شود و چنانچه دستگاه سیار نباشد موقعیت مکانی دقیق آن نیز در سرویس‌دهنده ذخیره می‌شود.

۳-۲- پروتکل پیشنهادی LAL2MAP

پروتکل پیشنهادی LAL2MAP نسخه بهینه شده پروتکل L2MAP [16] می‌باشد که در آن علاوه بر توجه به PUF و اطلاعات کانال، به اطلاعات موقعیت مکانی اشیاء و متحرک یا ثابت بودن آن اشیاء در احراز هویت دستگاه IoT توجه شده است. در این پروتکل از PUF و پارامترهای بر پایه کانال استفاده شده است تا در کنار پیچیدگی،

سادگی در عملیات و مقاومت بالا در برابر انواع مختلف حملات را داشته و وضعیت سیار و یا عدم سیار بودن اشیاء را نیز در نظر می‌گیرد تا برای اشیاء ساکن، امنیت بیشتر بدون سربار محاسباتی قابل توجه نسبت به پروتکل L2MAP ایجاد شود.

۳-۲-۱- پاف (PUF)

توابع غیرقابل تکثیر فیزیکی یا همان PUF، تراشه‌هایی با معماری خاص هستند که دنباله‌ای از بیت‌ها را به‌عنوان ورودی دریافت می‌کنند که اصطلاحا به آن چالش گفته می‌شود. سپس دنباله دیگری از بیت‌ها را به‌عنوان پاسخ در خروجی تولید می‌کنند. به دلیل تنوع در فرآیند تولید، هیچ دو تراشه‌ای قادر به تولید پاسخ یکسان نیستند [۲۲]. این تراشه‌ها به یک چیپ جهت استخراج اثرانگشت یکتا مجهز می‌شوند. به دلیل عدم نیاز به رمزنگاری در PUFها، از آنها بصورت گسترده برای احراز هویت دستگاه‌های با منابع محدود مانند دستگاههای اینترنت اشیاء استفاده می‌شود و استفاده از PUF یک تکنیک محبوب در طراحی احراز هویت دستگاه‌های IoT محسوب می‌شود [۲۳].

۳-۲-۲- استخراج کننده فازی

از آنجایی که کانال‌های بی‌سیم تصادفی و پویا هستند، پارامترهای بر پایه کانال در بازه‌های زمانی متفاوت ممکن است بسیار با هم متفاوت باشند. در حقیقت، مشخصات کانال ممکن است بین فرستنده و گیرنده کمی متفاوت باشد و گاهاً تغییر کند. در نتیجه، مولفه‌ی که بر پایه یک کانال توسط کاربر A استخراج شده همیشه با مولفه‌ی که بر پایه همان کانال توسط کاربر B استخراج شده یکسان نیست. به‌همین دلیل سیستم‌های فازی برای حل مسئله غیرمتقابل بودن از مشخصات کانال بهره می‌گیرند تا از این مزیت برخودار شوند. یک سیستم فازی، یک رشته باینری مانند N از تعدادی فضای متریک SP که متعلق به $\{۰ و ۱\}^n$ است را به‌عنوان ورودی دریافت می‌کند که در آن n یک عدد مثبت است. سپس در خروجی یک رشته تصادفی $\sigma \in \{0, 1\}^l$ (l یک عدد مثبت است) و یک رشته کمک $\tau \in \{0, 1\}^r$ که در آن r یک عدد مثبت است و می‌تواند برابر با l یا n باشد را به‌عنوان خروجی تولید می‌کند. استخراج کننده فازی مورد استفاده بر پایه دو تابع Gen(.) و Rep(.) می‌باشد.

تابع Gen(.): یک تابع احتمال است که رشته‌ی یکنواخت از بیت‌های تصادفی را با توجه به یک ورودی خاص تولید می‌کند. ورودی تابع مولفه کانال استخراج شده توسط کاربر A (فرستنده درخواست احراز هویت) است و با نماد $N_{0.A}$ نمایش داده می‌شود. خروجی‌های تولید شده کلید l - بیتی بر پایه کانال σ_i و پارامتر تولید مجدد τ_i است. از این رو:

$Gen\ (N_{0.A}) = (\ \sigma_i\ ,\ \tau_i\ )$

تابع Rep(.): این تابع رشته یکنواخت از بیت‌های تصادفی را از ورودی بازیابی می‌کند که کمی متفاوت با ورودی اصلی است و اختلاف بیتی آنها با ورودی کمتر یا برابر با مقدار آستانه از پیش تعریف شده t می‌باشد.

$HD\ (N_{0,B}, N_{0,A}) \leq t$

در واقع $N_{0,B}$ و τ_i به‌عنوان ورودی به تابع داده می‌شوند تا کلید برپایه کانال σ_i تولید شود، لذا خواهیم داشت:

$\sigma_i = Rep\ (N_{0,B}\ , \tau_i\ )$

این دو تابع در فرآیند احراز هویت متقابل پیشنهادی جهت ترکیب محرمانگی مقادیر خروجی PUF و تصادفی بودن و پویا بودن کانال‌های بی‌سیم مورد استفاده قرار گرفته‌اند.

۳-۲-۳- فاز اول : مقدار دهی اولیه

در این مرحله، تراشه دستگاه IoT به سرویس‌دهنده متصل می‌شود و سرویس‌دهنده، مجموعه‌ای از چالش‌ها را برای PUF ارسال می‌کند و پاسخ‌های متناظر را دریافت و ذخیره می‌نماید. شناسه مخفی جلسه (ID_s) از مقدار یک خروجی PUF گرفته می‌شود و تنها کاربر IoT و سرویس‌دهنده از آن مطلع خواهند بود. همچنین وضعیت سیار یا عدم سیار بودن دستگاه در محیط در این مرحله مشخص شده و در سرویس‌دهنده ذخیره می‌شود. بدین صورت که اگر دستگاه سیار نباشد موقعیت جغرافیایی دقیق آن در پارامتر L در درون سرویس‌دهنده ذخیره می‌شود و پارامترL در درون دستگاه با مقدار صفر ذخیره می‌شود. همچنین پارامتر دیگری تحت عنوان m که همان وضعیت سیار بودن دستگاه می‌باشد با مقدار صفر در سرویس‌دهنده و دستگاه ذخیره می‌شود. اگر دستگاه سیار باشد پارامتر L و L_0 با مقدار صفر به‌ترتیب در سرویس‌دهنده و دستگاه ذخیره می‌شوند و همچنین پارامتر m نیز با عدد یک مقدار دهی شده و در سرویس‌دهنده و دستگاه ذخیره می‌شود. لازم به ذکر است که پس از مستقر شدن دستگاه IoT، مکان دستگاه توسط حسگر موقعیت مکانی دریافت و براساس آن L_n مقدار دهی می‌شود.

۳-۲-۴- فاز دوم: احراز هویت و توافق کلید

فرآیند احراز هویت و توافق کلید میان دستگاه IoT (کاربر A) و سرویس‌دهنده احراز هویت (کاربر B) در شکل ۲ نمایش داده شده است و به‌صورت زیر می‌باشد:

۱- ابتدا کاربر A، یک مولفه کانال $N_{0,A}$ استخراج کرده و (σ_i, τ_i) را با استفاده از تابع Gen(.) تولید می‌کند. در نتیجه خواهیم داشت: $Gen\ (N_{0,A}) = (\sigma_i, \tau_i)$. در ادامه وضعیت سیار یا عدم سیار بودن دستگاه بررسی شده و چنانچه دستگاه سیار باشد مقدار L_0 با مقدار L_n پر می‌شود. پس از آن پارامتر موقعیت مکانی کاربر از XOR شدن پارامترهای L_0 و L_n بدست می‌آید. در این رابطه چنانچه دستگاه سیار نباشد با توجه به صفر بودن مقدار L_0 خواهیم داشت $L= L_n$ ، و اگر دستگاه سیار باشد با توجه به اینکه $L_0= L_n$ می‌باشد، لذا مقدار L برابر صفر خواهد بود. در ادامه کاربر A همچنین عدد تصادفی R_A را نیز تولید می‌کند. پس از آن پارامتر L با R_A ، XOR می‌شود تا متغیر temp ایجاد شود $temp = L \oplus R_A$. شناسه جلسه مخفی ID_s گرفته شده از PUF به مُهر زمانی TS_A آن لحظه الحاق می‌شود. نتیجه این الحاق درهم‌سازی شده و سپس با temp ، XOR شده تا پیام M_1 تولید شود. $M_1 = h(ID_S\ ||TS_A) \oplus temp$. پیام دوم نیز با XOR کردن عدد تصادفی R_A و τ_i محاسبه می‌شود. در نتیجه داریم : $M_2 = R_A \oplus \tau_i$. سرانجام کاربر A درخواست احراز هویت متشکل از $< M_1 , M_2 , TS_A >$ را از طریق یک کانال عمومی به دروازه می‌فرستد. در اینجا باید متذکر شد که پارامتر تولید مجدد τ_i برای حفاظت و انتقال امن R_A به کاربر B مورد استفاده قرار گرفته است. در این پروتکل، τ_i از یک کانال فیزیکی مشترک میان کاربران قانونی مشتق شده است و این بدان معنا است که این پارامتر به‌صورت عمومی در دسترس نیست و قابل بدست آوردن توسط مهاجمین نیست. از طرف دیگر σ_i توسط فرستنده مخفی نگه داشته می‌شود.

۲- پس از دریافت درخواست احراز هویت توسط کاربر B، اعتبار TS_A به‌وسیله $|TS_A - TS_A^*| \leq \Delta T$ ارزیابی می‌شود که در این رابطه ΔT حداکثر زمان تاخیر انتقال پیام و TS_A^* زمان دریافت پیام است و چنانچه این شرط برقرار نباشد کاربر B اتصال را قطع می‌کند.

۳- در ادامه کاربر B پیام $M_3 = h(ID_s||TS_A)$ را با استفاده از اطلاعات ID_S ذخیره شده و اطلاعات دریافتی TS_A محاسبه کرده و سپس مقادیر $temp = M_1 \oplus M_3$ و $R_A = temp \oplus L$ و $\tau_i = M_2 \oplus R_A$ را به‌ترتیب محاسبه و بعد با استفاده از τ_i، $\sigma_i' = Rep\ (N_{0,B}, \tau_i)$ را تولید می‌کند.

۴- پس از آن، کاربر B ابتدا با توجه به پارامتر موقعیت مکانی کاربر متغیر $temp' = L \oplus R_B$ را به کمک عدد تصادفی R_B تولید می‌کند و سپس پیام $M_4 = h(\ ID_s||TS_A||TS_B||R_A) \oplus temp'$ را با استفاده از عدد تصادفی $temp'$ و مُهر زمانی جاری TS_B تولید می‌کند. علاوه بر این، یک کلید مخفی جلسه SK با استفاده از اطلاعات ذخیره شده و دریافتی به‌صورت $SK = h(ID_s||\sigma_i'||R_A||R_B||TS_A||TS_B)$ مشتق می‌شود. کاربر B در پاسخ کاربر A پیام $< M_4 , M_5 , TS_B >$ را می‌فرستد که در آن $M_5 = h(SK \oplus R_A \oplus R_B)$ می‌باشد.

۵- کاربر A پیام $< M_4 , M_5 , TS_B >$ را دریافت نموده و اعتبار پیام‌ها را به وسیله $|TS_B - TS_B^*| \leq \Delta T$ بررسی می‌کند. چنانچه این شرط برقرار نباشد کاربر A ارتباط را قطع می‌کند.

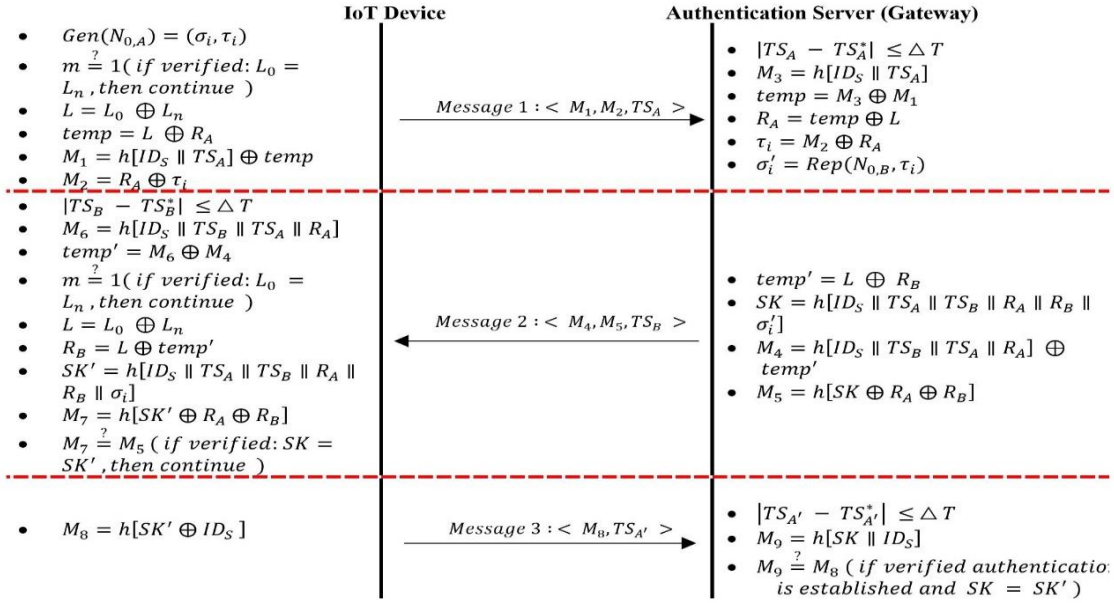
۶- در این مرحله، کاربر A ، TS_B را استخراج کرده و پیام $M_6 = h(\ ID_s||TS_A||R_A||TS_B)$ را تولید می‌کند. $temp'$ با XOR کردن M_6 و M_4 بدست آمده و بعد از آن سیار یا عدم سیار بودن وسیله بررسی می‌شود. چنانچه وسیله سیار باشد مقدار L_0 برابر موقعیت مکانی حال حاضر وسیله (L_n) خواهد شد تا مقدار L برابر صفر باشد و در صورت عدم سیار بودن وسیله با توجه به صفر بودن مقدار L_0، مقدار L برابر موقعیت مکانی حال حاضر وسیله (L_n) خواهد شد. پس از آن مقدار R_B با XOR کردن $temp'$ و L بدست می‌آید که از آن برای بدست آوردن $SK' = h(ID_s||\sigma_i||R_A||R_B||TS_A||TS_B)$ استفاده می‌شود. با استفاده از SK’ ، R_A و R_B کاربر A پیام $M_7 = h(SK'||R_A||R_B)$ را محاسبه می‌کند. اگر $M_7=M_5$، کاربر A کاربر B را تصدیق می‌کند و تایید می‌کند هر دو کاربر قادر به استخراج کلید مخفی جلسه SK=SK’ بوده‌اند.

۷- کاربر A پیام $< M_8 , TS_{A'} >$ را به‌عنوان تایید برای کاربر B می‌فرستد که در آن $M_8 = h(SK'||ID_S)$ بود و $TS_{A'}$ مُهر زمانی جدید است.

۸- سرانجام، کاربر B مقدار $|TS_{A'}^* - TS_{A'} \leq \Delta T|$ را بررسی نموده و پیام $M_9 = h(SK||ID_S)$ را تولید می‌کند. اگر $M_8=M_9$ باشدآنگاه کاربر B نیز تایید می‌کند کاربر A همان کلید مخفی جلسه را تولید کرده است، از این رو کاربر A تصدیق می‌شود. اگر هریک از مراحل فوق با شکست مواجه شود، اتصال بلافاصله لغو می‌شود.

در پایان این مراحل، دستگاه IoT و سرویس‌دهنده احراز هویت یک کلید مخفی جلسه مشترک خواهند داشت که از آن برای ارتباط امن استفاده خواهند نمود.

توابع رمزنگاری درهم‌ساز برای اطمینان از مالکیت یکطرفه پیام‌های مبادله شده و حساسیت بالا به ورودی به کار گرفته شده‌اند. این مسأله سبب جلوگیری از بازیابی اطلاعات مخفی از طریق جمع‌آوری ترافیک توسط مهاجمین می‌شود. فقط مولفه‌های قانونی با ویژگی‌های اشتراکی و پارامترهای یکتا (مخفی) قادر به محاسبه درهم‌سازی یکسان هستند. از این رو استراق سمع کنندگان تا زمانی



شکل ۲: مراحل پروتکل پیشنهادی LAL2MAP.

که همه پارامترهای صحیح را نداشته باشند نمی‌توانند اطلاعات مفیدی از پیام‌های ارسال شده بدست آورند و بدست آوردن همه پارامترهای صحیح نیز بسیار بعید است. این مرحله برای اطمینان از احراز هویت مناسب و مطمئن بسیار مهم است. در نهایت برای محافظت در مقابل حملات مجدد از مُهر زمان۸ و عدد تصادفی (R) استفاده شده است.

۳-۲-۵- فاز سوم: تبادل اطلاعات و محرمانه بودن داده‌ها و صحت پیام

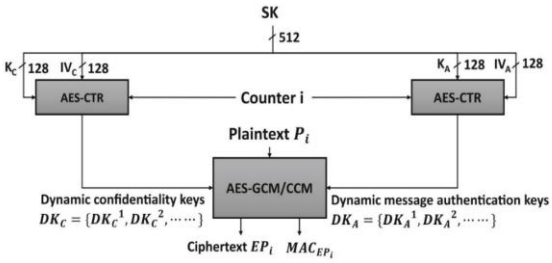
پس از مرحله احراز هویت متقابل و توافق کلید، دستگاه‌های IoT و سرویس‌دهنده هر دو یک کلید رمز جلسه یکسان (SK=SK') دارند که علاوه بر احراز هویت منبع برای اهداف مختلف دیگر مانند محرمانگی داده‌ها و صداقت پیام مورد استفاده قرار می‌گیرد. همانطور که در شکل ۳ مشاهده می‌شود، SK به چهار زیر کلید که هر کدام ۱۲۸ بیتی می‌باشد تقسیم می‌شود که عبارتند از K_C، IV_C، K_A و IV_A.

K_C و IV_C زیرکلیدهای مورد استفاده برای محرمانگی داده هستند که از آن‌ها مجموعه کلیدهای پویای زیر مشتق می‌شود:

$$DK_C = \{DK_C^1, DK_C^2, \dots\}$$

K_A و IV_A زیر کلیدهای احرازهویت منبع هستند که از آن‌ها مجموعه کلیدهای پویای زیر مشتق می‌شود:

$$DK_A = \{DK_A^1, DK_A^2, \dots\}$$



شکل ۳: طرح استخراج کلید کوتاه مدت پیشنهادی از کلید بلند مدت برای محرمانه بودن داده‌ها و صداقت پیام.

به ازای هر پیام i، کلیدهای محرمانگی داده و احراز هویت پیام جدید نیاز است تا به حد امنیت بالایی برسد. تکنیک تولید کلیدپویا پیشنهادی اساساً براساس استاندارد رمزگذاری پیشرفته[۹] با حالت شمارنده[۱۰] است. این حالت، داشتن عملکرد مناسب را تضمین می‌کند. علاوه بر این، می‌توان آن را به‌صورت موازی اعمال کرد. K_C و IV_C به‌ترتیب کلید اولیه محرمانگی داده و بردار اولیه محرمانگی داده هستند. DK_C^i کلید محرمانگی داده iام است که با استفاده از کلید محرمانگی داده آغازین و عنصر iام آرایه آغازین (IV_C^i) تولید می‌شود. جهت بدست آوردن IV_C^i ، مطابق معادله زیر IV_C با شماره (i - 1) بروزرسانی (XOR) می‌شود:

$$IV_C^i = IV_C \oplus (i-1)$$

کلید محرمانگی iام بر اساس معادله زیر تولید می‌شود :

$$DK_C^i = AES_{CTR}(IV_C^i, K_C)$$

به‌طور مشابه، K_A و IV_A به‌ترتیب کلید آغازین احراز هویت پیام و بردار آغازین احراز هویت پیام هستند. یک مجموعه کلید پویا برای احراز هویت به‌صورت $DK_A = \{DK_A^1, DK_A^2, \ldots\}$ با استفاده از همان رویکرد (AES در حالت شمارنده) تولید می‌شود. این بدان معناست که کلید احراز هویت iام با استفاده از K_A و عنصر iام بردار آغازین (IV_A^i) تولید می‌شود که IV_A^i با استفاده از IV_A و شمارنده (i - 1) حاصل می‌شود.

۴- نتایج و بحث

در این بخش به ارزیابی کارایی پروتکل پیشنهادی در مقایسه با پروتکل‌های ارائه شده توسط ملکی و همکاران [۱۵]، داس و همکاران [۱۳]، داس و همکاران [۱۲]، چانگ و همکاران [۱۱] و لی و همکاران [۲۴] پرداخته می‌شود. پارامترهای بررسی شده شامل هزینه ارتباطی، هزینه محاسباتی و زمان‌اجرا می‌باشد. لازم به ذکر است که تمامی این پروتکل‌های از PUF در فرآیند احراز هویت استفاده می‌کنند. ملکی و همکاران [۱۵] در L2MAP دو مفهوم پارامترهای کانال و PUF را جهت افزایش استحکام و کارایی سیستم چند منظوره ترکیب نمودند. الگوریتم پیشنهادی LAL2MAP نسخه بهبود یافته الگوریتم L2MAP می‌باشد و به منظور افزایش استحکام و کارایی سیستم، از ترکیب پارامترهای مشخصات کانال، PUF، و پارامتر موقعیت مکانی و همچنین ثابت یا سیار بودن دستگاهها در فرایند احرازهویت استفاده کرده است.

۴-۱- هزینه ارتباطی

جهت انجام مقایسه، فرض می‌شود مقدار شناسه هویت یا جلسه مخفی برابر ۱۶۰ بیت، عدد تصادفی ۱۶۰ بیت، مُهر زمانی ۳۲ بیت، موقعیت مکانی ۶۴ بیت و درهم‌سازی خلاصه شده ۱۶۰ بیت (استفاده از تابع هش SHA-1 همانند پروتکل پیشنهادی ملکی و همکاران [۱۵] باشد.

پروتکل پیشنهادی توسط داس و همکاران [۱۳] نیاز به ارسال ۳ پیام دارد که حجم آن‌ها به‌ترتیب ۵۱۲ ، ۵۱۲ و ۱۹۲ بیت هستند. در نتیجه هزینه ارتباطی کل ۱۲۱۶ بیت است. در طرح پیشنهاد شده توسط لی و همکاران [۲۴] چهار پیام جهت دستیابی به احراز هویت متقابل نیاز بوده و هزینه ارتباطی کل ۱۸۵۶ بیت است. به‌طور مشابه پروتکل‌های احراز هویت در طرح‌های داس و همکاران [۱۲] و چانگ و همکاران [۱۱] به چهار پیام احتیاج دارند که هزینه ارتباطی آن‌ها به‌ترتیب ۲۷۵۲ بیت و ۲۰۸۰ بیت می‌شود. در پروتکل پیشنهادی L2MAP سه پیام وجود دارد که هزینه ارتباطی آن‌ها عبارت است از:

$$Message\ 1 : < M_1, M_2, TS_A > \rightarrow 160bit + 160bit + 32bit = 352bit$$

$$Message\ 2 : < M_4, M_5, TS_B > \rightarrow 160bit + 160bit + 32bit = 352bit$$

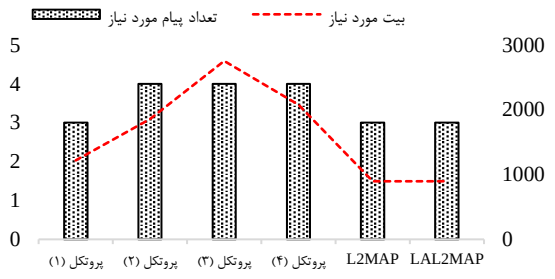
$$Message\ 3 : < M_8, TS_{A'} > \rightarrow 160bit + 32bit = 192bit$$

بنابراین هزینه ارتباطی کل در این پروتکل برابر با ۸۹۶ بیت است که از هزینه ارتباطی در پروتکل ارائه شده توسط داس و همکاران [۱۳] کمتر است.

همانطور که در جدول ۱ مشاهده می‌شود، در پروتکل پیشنهادی LAL2MAP، تعداد پیام‌های ارسالی نسبت به پروتکل L2MAP تغییر نداشته و همان سه پیام ارسال می‌شود. از آنجایی که پروتکل مقدار عدد تصادفی را با پارامتر موقعیت مکانی XOR می‌کند؛ بنابراین همانطور که در شکل ۴ مشاهده می‌شود، میزان حجم پیام نهایی تغییری نخواهد داشت.

جدول ۱: مقایسه هزینه ارتباطی در پروتکل‌ها.

طرح	تعداد پیام مورد نیاز	بیت مورد نیاز
پروتکل ارائه شده در [۱۳]	۳	۱۲۱۶
پروتکل ارائه شده در [۲۴]	۴	۱۸۵۶
پروتکل ارائه شده در [۱۲]	۴	۲۷۵۲
پروتکل ارائه شده در [۱۱]	۴	۲۰۸۰
پروتکل L2MAP [۱۵]	۳	۸۹۶
پروتکل پیشنهادی LAL2MAP	۳	۸۹۶



شکل ۴: مقایسه هزینه ارتباطی در پروتکل‌ها.

۴-۲- هزینه محاسباتی

جهت ارزیابی هزینه‌های محاسباتی پروتکل پیشنهادی ابتدا پارامترهای T_h، T_{XOR}، T_f و T_E را تعریف می‌کنیم که این نمادگذاری به‌ترتیب عبارتند از مدت زمان تابع درهم‌ساز ، مدت زمان عملیات XOR، مدت زمان استخراج کننده فازی و مدت زمان ضرب نقطه‌ای سیستم رمزنگاری منحنی بیضوی[۱۱]. هزینه محاسباتی کل در طرح‌های پیشنهادی عبارتند از:

$Delay_{[۱۳]} = 17T_h + 8T_{XOR} + 1T_f$

$Delay_{[۲۴]} = 21T_h + 3T_E$

$Delay_{[۱۲]} = 31T_h + 4T_E + 1T_f$

$Delay_{[۱۱]} = 19T_h + 7T_{XOR}$

$Delay_{[۱۵]} = 10T_h + 10T_{XOR} + 1T_f$

و هزینه محاسباتی در پروتکل پیشنهادی برابر است با :

$Delay_{[LAL2MAP]} = 10T_h + 16T_{XOR} + 1T_f$

و از آنجایی که مدت زمان مورد نیاز برای عملیات XOR بسیار کمتر از عملیات درهم‌ساز بوده و ناچیز محسوب می‌شود، می‌توان نتیجه گرفت که پروتکل پیشنهادی کماکان با وجود در نظر گرفتن موقعیت مکانی در دستگاه‌های ساکن، هم تراز پروتکل L2MAP و بهتر از طرح‌های موجود در سایر پروتکل‌های مورد بررسی است. جدول ۲ خلاصه هزینه محاسبات را از نظر تاخیر نمایش می‌دهد.

جدول ۲: زمان تاخیر محاسباتی در پروتکل‌ها.

طرح	تاخیر محاسباتی
پروتکل ارائه شده در [۱۳]	$17T_h + 8T_{XOR} + 1T_f$
پروتکل ارائه شده در [۲۴]	$21T_h + 3T_E$
پروتکل ارائه شده در [۱۲]	$31T_h + 4T_E + 1T_f$
پروتکل ارائه شده در [۱۱]	$19T_h + 7T_{XOR}$
پروتکل L2MAP [۱۵]	$10T_h + 10T_{XOR} + 1T_f$
پروتکل پیشنهادی	$10T_h + 16T_{XOR} + 1T_f$

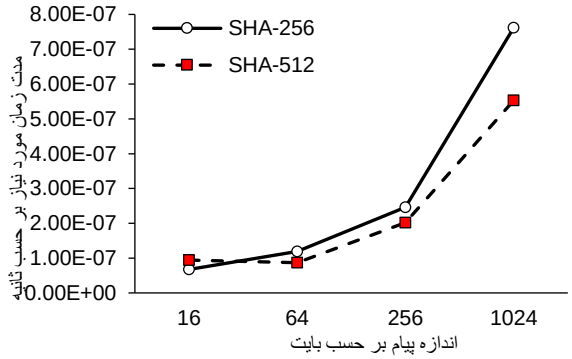
۴-۳- زمان اجرا

جهت ارزیابی زمان اجرای پروتکل احراز هویت پیشنهادی، طرح تولید کلید پویا و پروسه محرمانه بودن داده‌ها و صداقت پیام از برنامه OpenSSL استفاده شده است. این برنامه یکی از مهمترین و کارآمدترین کتابخانه‌های رمزنگاری است که جعبه ابزاری قوی و کامل در سطح تجاری برای امنیت لایه حمل و نقل (TLS) و پروتکل‌های امن لایه سوکت (SSL) دارد. سخت افزار مورد استفاده برای OpenSSL، پردازنده Intel Core i3 M330 و مقدار حافظه ۴ گیگابایت بوده است.

جدول ۳ و شکل ۵ مدت زمان لازم جهت اجرای توابع درهم‌ساز با اندازه‌های مختلف پیام را نشان می‌دهد. جهت نمایش کارایی پروتکل پیشنهادی، زمان مورد نیاز برای توابع درهم‌ساز SHA-256 و SHA-512 محاسبه و نمایش داده شده است. در پیام‌ها با سایزهای متفاوت (در واحد بایت)، واضح است که SHA-512 زمان کمتری نیاز دارد و طبیعتاً کارآمدتر است و در مقابل آن SHA-256 فقط برای پیام‌هایی با سایز کوچک (۱۶ بایت) کارآمد است.

جدول ۳: مدت زمان اجرای توابع درهم‌ساز SHA-256 و SHA-512 برحسب ثانیه.

تاخیر محاسباتی	SHA-256	SHA-512
۱۶ بایت	6.75×10^{-8}	9.44×10^{-8}
۶۴ بایت	1.19×10^{-7}	8.68×10^{-8}
۲۵۶ بایت	2.46×10^{-7}	2.02×10^{-7}
۱۰۲۴ بایت	7.62×10^{-7}	5.53×10^{-7}

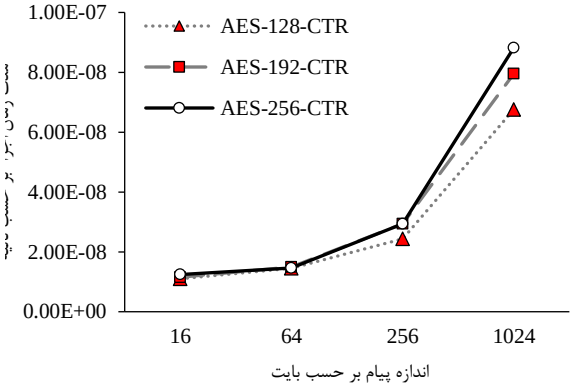


شکل ۵: نمودار مدت زمان اجرای تابع درهم‌ساز SHA با اندازه پیام‌های مختلف.

همچنین برای ارزیابی کارایی عملیات استخراج کلید در روش پیشنهادی، تجزیه و تحلیل زمان اجرای AES OpenSSL با حالت شمارنده (CTR) انجام شد. همانطور که در شکل ۶ مشاهده می‌شود، نتایج این تجزیه و تحلیل نشان می‌دهد که با افزایش طول پیام، تاخیر نیز افزایش می‌یابد. به عبارت دیگر، با افزایش طول کلید مخفی، سطح امنیت افزایش یافته ولی تأخیر نیز بیشتر می‌شود.
در نهایت برای مقایسه دو حالت CCM و GCM در عملیات احراز هویت/ رمزگذاری از AES OpenSSL استفاده شد که علاوه بر تایید منبع احراز هویت، از محرمانه بودن داده و یکپارچگی پیام اطمینان

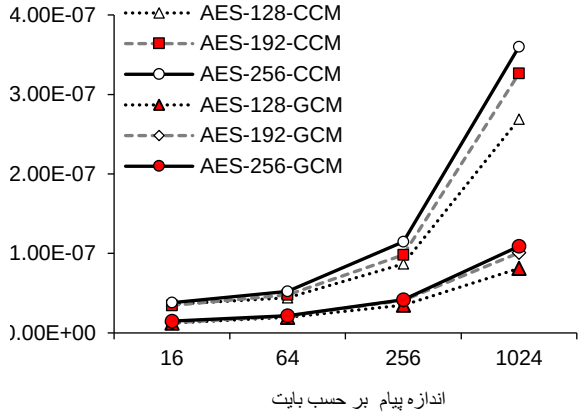
حاصل می‌کند. لازم به ذکر است برخلاف حالت CTR، حالت‌های CCM (شمارنده با CBC-MAC) و GCM (حالت Galois/Counter) از محرمانه بودن داده و یکپارچگی پیام پشتیبانی می‌کنند و این موضوع منجر به ترجیح این دو حالت به حالت CTR می‌شود. جدول ۴ مقادیر عددی زمان اجرا برای حالت‌های مختلف عملیات رمزنگاری به وسیله پیاده‌سازی AES OpenSSL را نمایش می‌دهد.

نتایج مقایسه عملکرد حالتهای GCM و CCM برای کلیدهای متقارن AES با اندازه پیامهای مختلف در شکل ۷ مشاهده می‌شود.



شکل ۶: نمودار مدت زمان اجرای تابع درهم‌ساز AES با اندازه پیام‌های مختلف.

این نتایج ثابت می‌کند که حالت GCM برای کلیدهای متقارن AES با اندازه‌های مختلف پیام به زمان اجرای کمتری نیاز دارد و از حالت CCM بسیار کارآمدتر است. بنابراین برای کاربردهای اینترنت اشیاء مناسب‌تر بوده و استفاده از آن توصیه می‌شود. لازم به ذکر است، هرچه اندازه پیام افزایش می‌یابد، مدت زمان لازم برای عملیات رمزنگاری و احزار هویت پیام نیز افزایش می‌یابد و از آنجایی که افزایش مقدار بایت نیاز به زمان بیشتر برای پردازش (رمزنگاری) دارد این موضوع منطقی به نظر می‌رسد.



شکل ۷: نمودار مدت زمان اجرا و اندازه پیام برای حالت عملیات CCM و GCM.

۱- نتیجه گیری

در این مقاله، یک پروتکل احراز هویت متقابل سبک وزن چند عاملی آگاه از مکان برای سیستم‌های IoT بنام LAL2MAP پیشنهاد شد که نسخه بهبود یافته پروتکل L2MAP می‌باشد. در پروتکل پیشنهادی علاوه بر PUF و مشخصات کانال، از پارامتر موقعیت مکانی و سیار یا ثابت بودن دستگاه‌ها جهت بالا بردن امنیت و مقاومت در برابر حملات استفاده شده است. نتایج ارزیابی‌ها نشان می‌دهد که کارایی پروتکل پیشنهادی از نظر هزینه محاسباتی و ارتباطی نسبت به پروتکل‌های مشابه بهبود داشته است. همچنین در مقایسه با پروتکل پایهL2MAP ، پروتکل پیشنهادی ضمن حفظ هزینه‌های محاسباتی و ارتباطی یکسان، باعث افزایش امنیت و مقاومت در مقابل حملات کانال جانبی نیز شده است. به عبارت دیگر، پروتکل پیشنهادی با حفظ سبک وزن بودن باعث بهبود استحکام و مقاومت نسبت به L2MAP شده است.

جدول ۴: مدت زمان اجرای حالت‌های مختلف رمزنگاری برحسب ثانیه.

نوع	۱۶ بایت	۶۴ بایت	۲۵۶ بایت	۱۰۲۴ بایت
AES-128-CTR	1.10×10^{-8}	1.45×10^{-8}	2.44×10^{-8}	6.76×10^{-8}
AES-192-CTR	1.15×10^{-8}	1.49×10^{-8}	2.94×10^{-8}	7.95×10^{-8}
AES-256-CTR	1.24×10^{-8}	1.46×10^{-8}	2.94×10^{-8}	8.82×10^{-8}
AES-128-CCM	3.60×10^{-8}	4.40×10^{-8}	8.67×10^{-8}	2.69×10^{-7}
AES-192-CCM	3.46×10^{-8}	4.80×10^{-8}	9.83×10^{-8}	3.26×10^{-7}
AES-256-CCM	3.81×10^{-8}	5.22×10^{-8}	1.15×10^{-7}	3.60×10^{-7}
AES-128-GCM	1.25×10^{-8}	1.95×10^{-8}	3.50×10^{-8}	8.12×10^{-8}
AES-192-GCM	1.28×10^{-8}	2.10×10^{-8}	4.08×10^{-8}	1.01×10^{-7}
AES-256-GCM	1.49×10^{-8}	2.18×10^{-8}	4.19×10^{-8}	1.09×10^{-7}

به‌عنوان کارهای آینده، می‌توان مدل حرکتی اشیاء سیار را مورد بررسی قرار داده و براساس آن، برای اشیاء سیار نیز اقدامات امنیتی متناسبی اتخاذ نمود. همچنین می‌توان راه حلی نیز برای دستگاه‌های فاقد GPS در نظرگرفت تا با روشهای دیگر، موقعیت مکانی خود را جهت استفاده از این پروتکل بدست آورند. بعلاوه، می‌توان در مواردی که دستگاه‌ها با سرویس‌دهنده فاصله دارند و فضای تحت پوشش وسیع است از شبکه‌های با گره‌های تجمیعی استفاده نمود.

مراجع

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

[2] C. D. Pham and T. K. Dang, "A lightweight authentication protocol for D2D-enabled IoT systems with privacy," *Pervasive and Mobile Computing*, vol. 74, p. 101399, 2021.

[3] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the Internet of Things in a quantum world," *IEEE Communications Magazine*, vol. 55, no. 2, pp. 116-120, 2017.

[4] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: A systematic literature review," *Information and Software Technology*, vol. 94, pp. 30-37, 2018.

[5] R. Madhusudhan and R. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review," *Journal of Network and Computer Applications*, vol. 35, no. 4, pp. 1235-1248, 2012.

[6] S. Sicari, A. Rizzardi, L. Grieco, G. Piro, and A. Coen-Porisini, "A policy enforcement framework for Internet of Things applications in the smart health," *Smart Health*, vol. 3, pp. 39-74, 2017.

[7] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "SEGR: A secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks," in *2014 IEEE International Conference on Communications (ICC)*, 2014: IEEE, pp. 1011-1016.

[8] C. Lai, R. Lu, D. Zheng, H. Li, and X. S. Shen, "GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications," *Computer Networks*, vol. 99, pp. 66-81, 2016.

[9] X. Sun, S. Men, C. Zhao, and Z. Zhou, "A security authentication scheme in machine-to-machine home network service," *Security and Communication Networks*, vol. 8, no. 16, pp. 2678-2686, 2015.

[10] H. Zhu, X. Lin, Y. Zhang, and R. Lu, "Duth: a user-friendly dual-factor authentication for Android smartphone devices," *Security and Communication Networks*, vol. 8, no. 7, pp. 1213-1222, 2015.

[11] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Transactions on wireless communications*, vol. 15, no. 1, pp. 357-366, 2015.

[12] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 16, pp. 3670-3687, 2016.

[13] A. K. Das, M. Wazid, N. Kumar, M. K. Khan, K.-K. R. Choo, and Y. Park, "Design of secure and lightweight authentication protocol for wearable devices environment," *IEEE journal of biomedical and health informatics*, vol. 22, no. 4, pp. 1310-1322, 2017.

[14] S. Li, T. Zhang, B. Yu, and K. He, "A provably secure and practical PUF-based end-to-end mutual authentication and key exchange protocol for IoT," *IEEE Sensors Journal*, vol. 21, no. 4, pp. 5487-5501, 2020.

[15] R. Melki, H. N. Noura, and A. Chehab, "Lightweight multi-factor mutual authentication protocol for IoT devices," *International Journal of Information Security*, vol. 19, no. 6, pp. 679-694, 2020.

[16] H. Yıldız, "A PUF-based lightweight group authentication and key distribution protocol," 2020.

[17] A. Fu, S. Lan, B. Huang, Z. Zhu, and Y. Zhang, "A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks," *IEEE Communications Letters*, vol. 16, no. 11, pp. 1744-1747, 2012.

[18] J. Cao, M. Ma, and H. Li, "A group-based authentication and key agreement for MTC in LTE networks," in *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012: IEEE, pp. 1017-1022.

[19] C. Lai, H. Li, R. Lu, and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," *Computer Networks*, vol. 57, no. 17, pp. 3492-3510, 2013.

[20] J. Jeong, M. Y. Chung, and H. Choo, "Integrated OTP-based user authentication scheme using smart cards in home networks," in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, 2008: IEEE, pp. 294-294.

[21] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, "PBA: Prediction-based authentication for vehicle-to-vehicle communications," *IEEE transactions on dependable and secure computing*, vol. 13, no. 1, pp. 71-83, 2015.

[22] A. Babaei and G. Schiele, "Physical unclonable functions in the internet of things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, p. 3208, 2019.

[23] C. Mesaritakis *et al.*, "Physical unclonable function based on a multi-mode optical waveguide," *Scientific reports*, vol. 8, no. 1, pp. 1-12, 2018.

[24] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194-204, 2018.

پاورقی:

[1] Physical Unclonable Function

[2] Wearable devices

[3] Rooming

[4] False Rejection Ratio

[5] Machine-to-Machine

[6] Factorial Tree

[7] Chinese Reminder Theorem (CRT)

[8] Timestamp (TS)

[9] Advanced Encryption System (AES)

[10] Counter Mode (CTR)

[11] Elliptic Curve Cryptosystem