Journal of Electronical & Cyber Defence
Vol. 9, No. 2, 2021, Serial No. 34

A New framework for Enhancing the Security of Military Internet of Things Using the Hybrid Classical-Quantum Cryptography

S. N. Doustimotlagh

* Sharif University of Technology

(Received: 11/07/2020, Accepted: 11/01/2021)

ABSTRACT

One of the properties of quantum cryptographic algorithms is to break the security of some systems which are based on classical cryptographic algorithms. However, systems based on quantum cryptographic algorithms are immune from such a risk. Another useful feature of quantum cryptographic algorithms is the change of information (quantum states) exchanged in a telecommunication channel, which in turn can serve for identifying leaked information (such as eavesdropping), unsafe channel or a seemingly secure channel. Besides, the quantum secret sharing algorithm, as a branch of quantum cryptographic algorithms, has many applications in the IoT network because of its characteristics, like the possibility of a safe and secure distribution of shares among the shareholders by the issuer of shares; a fact that is absent in the classical secret sharing algorithm. On the other hand, one of the most important applications of the Internet of Things (IoT) is the military Internet of Things (MIoT). Due to the fact that the Io network directly affects the battle scenes, it is more important compared to civilian applications. Thus, the security issues related to different parts of the MIoT network are of great importance. On this account, we present a new design using a combination of the classical cryptographic algorithm (specifically using the new digital signature scheme) and the quantum secret sharing algorithm to enhance the security of the MIoT network, in which the considered security requirements such as authentication, authenticity, undeniability, data integrity, confidentiality, data freshness, anonymity, unrelatedness, etc., are more than the security requirements in similar researches. The presented framework is also secure against all types of attacks (including repeat attacks, denial of service attacks, identity attack attacks, eavesdropping attacks, middle man attacks, message manipulation attacks, traffic analysis attacks, message forgery attacks, identity disclosure attacks, etc.), suggesting more efficiency with respect to other previous works in this field.

Keywords: Military Internet of Things, Digital Signature, Quantum Secret Sharing, Classic Cryptography, Quantum Cryptography

* Corresponding Author Email: doustimotlagh@chmail.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۲، تابستان ۱۴۰۰، ص ۴۹-۲۹

علمی – پژوهشی

سازوکاری جدید برای ارتقا امنیت شبکه اینترنت اشیا نظامی با استفاده از رمزنگاری کوانتومی و کلاسیک

سید نصیب‌اله دوستی مطلق[1*]

۱- استادیار دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی؛ پژوهشکده آماد، فناوری دفاعی و پدافند غیرعامل

(دریافت: ۱۳۹۹/۰۴/۲۱، پذیرش: ۱۳۹۹/۱۰/۲۲)

چکیده

یکی از خاصیت‌های الگوریتم‌های رمزنگاری کوانتومی، شکستن امنیت برخی سامانه‌های مبتنی بر الگوریتم‌های رمزنگاری کلاسیک است؛ اما امنیت سامانه‌های مبتنی بر الگوریتم‌های رمزنگاری کوانتومی از مخاطره ذکر شده در امان هستند. ویژگی مفید دیگرِ الگوریتم‌های رمزنگاری کوانتومی، تغییر اطلاعات (حالت‌های کوانتومی) مبادله شده در یک کانال مخابراتی است که خود نوعی راهکار برای تشخیص اطلاعات لو رفته (به‌عنوان‌مثال استراق سمع)، کانال غیر امن و یا کانال به‌ظاهر امن است. همچنین الگوریتم تسهیم راز کوانتومی که از شاخه‌های الگوریتم‌های رمزنگاری کوانتومی است در شبکه اینترنت اشیاء (ا.ا)، کاربردهای فراوانی دارد چنانکه با استفاده از الگوریتم تسهیم راز کوانتومی امکان توزیع امن سهم‌ها به سهام‌داران از طرف ایجادکننده سهام ممکن می‌شود؛ حال‌آنکه این امکان در الگوریتم تسهیم راز کلاسیک وجود ندارد. از طرفی یکی از کاربردهای مهم شبکه اینترنت اشیاء (ا.ا)، اینترنت اشیاء نظامی (ا.ا.ن) است. باتوجه به اینکه شبکه ا.ا.ن مستقیماً بر روی صحنه‌های نبرد تأثیر می‌گذارد، لذا در مقایسه با کاربردهای غیرنظامی، دارای اهمیت بالاتری است. از این‌رو، مسائل امنیتی مرتبط با بخش‌های مختلف شبکه ا.ا.ن بسیار حیاتی هستند. بر این اساس در این کار طرحی جدید با استفاده از ترکیب الگوریتم رمزنگاری کلاسیک (به‌طور خاص استفاده از طرح امضای دیجیتال جدید معرفی‌شده در این کار) و الگوریتم تسهیم راز کوانتومی برای ارتقاء امنیت شبکه ا.ا.ن ارائه داده‌ایم که در آن نیازمندی‌های امنیتی چون احراز اصالت، مجاز شناسی، انکارناپذیری، یکپارچگی داده، محرمانگی، تازه بودن داده، گمنامی، ارتباط ناپذیری و ... بررسی‌شده که در مقایسه با پژوهش‌های مشابه نیازمندی‌های امنیتی بیشتری را تأمین کرده است. این طرح همچنین در برابر انواع حمله‌های مطرح (همچون حمله تکرار، حمله منع خدمت، حمله جعل هویت، حمله شنود، حمله مرد میانی، حمله دست‌کاری پیام، حمله تحلیل ترافیک، حمله جعل پیام، حمله آشکارسازی هویت و غیره) مقاوم بوده که نسبت به پژوهش‌های قبلی در این زمینه از کارایی بالاتری برخوردار است.

کلید واژه‌ها: شبکه اینترنت اشیاء نظامی، امضای دیجیتال، تسهیم راز کوانتومی، رمزنگاری کلاسیک، رمزنگاری کوانتومی

۱- مقدمه

اینترنت اشیاء مفهومی است که مجموعه‌ای از هرکسی، هر چیزی، هر خدمتی و هر شبکه‌ای را در هر زمان و مکان به هم مرتبط می‌کند. اینترنت اشیاء امروزه به حوزه‌های مختلفی مانند نظامی، سلامت هوشمند، خانه‌های هوشمند، صنعت، مدیریت هوشمند سفر و دیگر حوزه‌ها وارد شده است. اینترنت اشیاء با ورود به این حوزه‌ها باعث افزایش کارایی و کاهش هزینه در انجام کارها شده است.

از طرفی واضح است حوزه نظامی حوزه‌ای دارای اهمیت است که از این امر مستثنی نبوده و ورود اینترنت اشیاء به آن تحول‌ها و پیشرفت‌های شگرفی را به وجود آورده است. اینترنت اشیاء خدمات و برنامه‌های کاربردی مناسبی را به حوزه نظامی وارد می‌کند و استفاده از آن می‌تواند باعث بهبود کارایی، و کاهش هزینه‌ها و خطرات شود. حوزه لجستیکی که مهم‌ترین بخش اینترنت اشیاء محسوب می‌شود، نقش مهمی در توسعه، امنیت و کارایی حوزه نظامی دارد. علاوه بر این مورد، برنامه‌های کاربردی اینترنت اشیاء، می‌توانند ارزش فوق‌العاده‌ای را برای شناسایی نظامی، نظارت بر محیط، جنگ بدون سرنشین و غیره فراهم کنند. همچنین اینترنت اشیاء می‌تواند جمع‌آوری و تحلیل اطلاعات نظامی را با استفاده از دستگاه‌های مدرن بهبود ببخشد [۱].

* رایانامه نویسنده مسئول: doustimotlagh@chmail.ir

ناشر: دانشگاه جامع امام حسین (ع)

اینترنت اشیاء هنوز به‌طور کامل پیشرفت نکرده و در بسیاری از مسائل مانند تأمین امنیت و حریم خصوصی دچار مشکل است. اکثر کارهایی که در حوزه نظامی اینترنت اشیاء توسعه و ارائه شده است، به‌صورت نمونه‌های کوچک و ایده‌هایی برای حوزه لجستیک نظامی هستند. این حوزه برای پیشرفت بیشتر نیاز به تحقیقات سازمان‌یافته‌تر و بیشتر در حوزه‌های بزرگ‌تر نظامی دارد تا ارتقای کامل در کاربردهای نظامی اینترنت اشیاء صورت بگیرد.

جنگ‌های مدرن عمدتاً مبتنی بر اطلاعات هستند و جنگ متمرکز شبکه‌ای (NCW[1]) نقش مهمی را در جنگ‌های استراتژیک مدرن دارد. در بستر جنگ متمرکز، به اشتراک‌گذاری اطلاعات بسیار حساس و مهم است. جنگ متمرکز شبکه‌ای می‌تواند تمام نیروها و سامانه‌های سلاح را در کل میدان جنگ متصل کند تا یک شبکه اطلاعاتی را ایجاد کند که باعث به اشتراک‌گذاری اطلاعات در زمان حاضر و به‌صورت بی‌درنگ می‌شود. این عمل زمان تصمیم‌گیری و زمان ارسال فرمان را کاهش می‌دهد و بهره‌وری عملیات مشترک را افزایش می‌دهد. ایده کلیدی جنگ متمرکز شبکه‌ای این است که استفاده از سلاح‌های به‌کارگرفته‌شده در میدان جنگ به‌صورت گروهی کارایی آن‌ها را نسبت به استفاده تکی افزایش می‌دهد و این مربوط به فناوری کلیدی اینترنت اشیاء است که آن‌ها را از طریق اینترنت به یکدیگر مرتبط می‌کند. این سلاح‌ها با اشتراک‌گذاری اطلاعات خود می‌توانند یک سامانه یک‌پارچه نظامی ایجاد کنند که کارایی بیشتری نسبت به حالت قبلی و عدم اشتراک اطلاعات میان آن‌ها دارد و توانایی عملیات سامانه را به‌صورت مؤثر بهبود می‌بخشد. با توسعه سریع ارتباطات؛ فناوری‌های شبکه و نرم‌افزار، فناوری‌های جدید نظامی (مانند فناوری شناسایی حس، فناوری ترکیب اطلاعات، فناوری شبکه مخابراتی، فناوری محاسبات پیشرفته، فناوری تصمیم‌گیری فرماندهی و فناوری امنیت اطلاعات) قابل‌دسترس و عملی می‌شوند. این فناوری‌ها تأثیر مهمی در پردازش اطلاعات، معماری سامانه و ویژگی‌های اینترنت اشیاء نظامی دارند.

شبکه اینترنت اشیاء نظامی که از آن با عنوان MIoT[2] نام‌برده می‌شود، به‌دلیل نیاز اطلاعاتی حوزه نظامی و توسعه فناوری اطلاعات بسیار ضروری است. اینترنت اشیاء نظامی معمولاً به‌عنوان یک سامانه اطلاعاتی در نظر گرفته می‌شود که می‌تواند ویژگی‌های فیزیکی و اطلاعات افراد نظامی، تجهیزات و اشیاء نظامی را با استفاده از وسیله سنجشِ اطلاعاتِ مختلف به‌دست آورد و سپس تمام عناصر عملیاتی، عناصر پشتیبانی و عناصر محیطی را به‌عنوان یک مرکز کلی با یک پروتکل ارتباطی استاندارد برای پردازش، کنترل و کاربرد هوشمندانه به یکدیگر مرتبط کند. سه مورد از کارهای مهم اینترنت اشیاء نظامی در حوزه اطلاعاتی عبارت‌اند از:

- اینترنت اشیاء نظامی می‌تواند زیرساخت‌های فیزیکی نظامی و زیرساخت‌های اطلاعاتی را به‌صورت عمیق به هم مرتبط کند و بر قابلیت اتصال اشیاء نظامی بر یکدیگر تأکید دارد. به‌عنوان‌مثال، می‌توان با جمع‌آوری اطلاعات از دستگاه‌های مختلف مانند رادارها، حس‌گرها، زیردریایی‌ها و افزاره‌های RFID[3] از شرایط نظامی و محل قرارگیری اسلحه‌های دشمن و اسلحه‌های خودی یک استراتژی مناسب برای حمله یا دفاع طراحی کرد.
- اینترنت اشیاء نظامی همچنین می‌تواند امور دفاعی نظامی را به‌طور دقیق‌تر و به‌صورت پویا پیاده‌سازی و اداره کند. با بهره‌گیری از اطلاعات منابع نظامی می‌تواند بهره‌وری عملیات نظامی را افزایش می‌دهد. با انجام عملیات و تعیین استراتژی‌ها با کمک اینترنت اشیاء نظامی دیگر نیاز به جمع‌آوری اطلاعات از طریق نیروی انسانی وجود ندارد. با پیاده‌سازی عملیات و طراحی استراتژی به‌صورت نوین کارایی اسلحه‌ها و ابزارهای نظامی از طریق ارتباط با یکدیگر افزایش می‌یابد. همچنین سرعت تبادل و به‌روز بودن استراتژی باعث می‌شود اطلاعاتِ لحظه‌ای در اختیار تمام نیروها و دستگاه‌های خودی قرار بگیرد.
- اینترنت اشیاء نظامی می‌تواند در لجستیک نظامی، حمایت‌های اسلحه‌ها، نظارت بر محیط برای حمایت از تمام قابلیت سامانه (مبتنی بر اطلاعات)، استفاده شود. به‌عنوان‌مثال، اطلاعات جمع‌آوری‌شده توسط دستگاه‌های اینترنت اشیاء نظامی از شرایط محیطی، شرایط اسلحه‌ها و نیروهای خودی می‌توانند امکان نظارت بهتر بر محیط جنگ و همچنین ارسال نیروهای پشتیبانی برای جایگزینی اسلحه‌ها و نیروهای تلف‌شده را در برداشته باشد.

یکی از حوزه‌هایی که این‌روزها، گسترش فناوری‌های مرتبط با شبکه اینترنت اشیاء در حوزه نظامی روی آن تمرکز کرده است، حوزه مربوط به‌کاربردهای سامانه‌های C4ISR[4] و سامانه کنترل آتش است. این گسترش از یک نگرش غالب در حوزه نظامی منشأ می‌گیرد که در ابتدای امر شبکه‌ها و حس‌گرها به‌عنوان ابزاری برای جمع‌آوری و به اشتراک‌گذاری داده‌ها در میدان جنگ در نظر گرفته می‌شوند تا بتوانند فرمان‌ها و کنترل تأثیرگذارتری از دارایی‌های نظامی داشته باشند. فناوری‌های

[1] Network Centric Warfare
[2] Military Internet of Things
[3] Radio Frequency Identification
[4] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

شبکه اینترنت اشیاء در بعضی از کاربردها برای مدیریت لجستیک، شبیه‌سازی و آموزش مطابقت داده شده‌اند. بااین‌وجود، استفاده و گسترش اینترنت اشیاء، در حوزه نظامی محدود بوده و از یکپارچه‌سازی نسبتاً ضعیفی برخوردار است که هم‌اکنون جامعه علمی جهان در حال تقویت آن است (پژوهش‌های مختلفی هرسال در این حوزه انجام می‌گیرد). برای این‌که بتوان داده‌های نظامی را از نیروهای نظامی مربوطه جمع‌آوری کرد، تعداد بسیار زیادی (در حد میلیون) حس‌گر بر روی ابعاد بزرگی از بسترهای مرتبط با نیروهای نظامی پیاده‌سازی و گسترش داده شده‌اند. با استفاده از مراکز عملیات مرکزی که وظیفه جمع‌آوری داده‌ها از بسترهای مربوطه را بر عهده دارند، فرماندهان ارشد می‌توانند به آگاهی از موقعیت جامعی از وضعیت و شرایط میدان نبرد دست پیدا کنند. همچنین، به‌عنوان‌مثال، جنگنده‌ها نیز به داده‌های مربوط به نواحی عملیاتی خود دسترسی پیدا می‌کنند. داده اولویت‌بندی شده از طریق لینک داده تاکتیکی[1] در اختیار خلبان‌های جنگی قرار می‌گیرد. سپس این داده اولویت‌بندی شده با اطلاعات خلبان‌ها که از طریق حس‌گرها به‌دست‌آمده‌اند، تجمیع می‌گردد. بدین‌صورت خلبان می‌تواند تمامی تهدیدهای ممکن و اهداف را در صفحه‌های موجود در کابین خود مشاهده کند. سامانه‌های کاملاً خودکار در حوزه نظامی در بحث‌های کنترل آتش مورد استفاده قرار می‌گیرند. سامانه‌های کاملاً خودکار از اطلاعات مربوط به حسگرهای مختلف بهره می‌برند تا سریع‌تر واکنش نشان داده و دقت لازم برای نشانه‌گیری جنگ‌افزارها را تأمین کنند. در ادامه به نقش رمزنگاری در امنیت می‌پردازیم.

۱-۱- نگاهی بر نقش رمزنگاری (کلاسیک، کوانتومی و پساکوانتومی) در برآورده کردن نیازمندی‌های امنیتی

با توجه به شرایط کنونی کشور عزیزمان ایران پرداختن به بحث امنیت حائز اهمیت دوچندانی در مقایسه با گذشته شده است. با توجه به اینکه حوزه امنیت شبکه اینترنت اشیاء نظامی در کشور کم‌تر موردتوجه واقع شده است و از طرف دیگر اهمیتی که بحث امنیت در اینترنت اشیاء نظامی دارد، سعی کرده‌ایم که به موضوع امنیت اینترنت اشیاء بپردازیم و طرحی را برای ارتقا امنیت شبکه اینترنت اشیاء نظامی با استفاده ترکیبی از رمزنگاری کلاسیک و رمزنگاری کوانتومی ارائه بدهیم. در ادامه، در رابطه با اهمیت علم محاسبات کوانتومی (و به‌طور خاص تسهیم راز کوانتومی که از زیرشاخه‌های الگوریتم‌های رمزنگاری کوانتومی است) در برآورده کردن نیازمندی‌های امنیتی (به‌خصوص در شبکه اینترنت اشیاء نظامی) صحبت خواهد شد.

[1] Tactical Data Links

کامپیوترهای کوانتومی که برای اولین بار در سال ۱۹۸۲ توسط برنده جایزه نوبل فیزیک ریچارد فاینمن مطرح شدند [۲]، با استفاده از ویژگی‌های کوانتومی عناصر تشکیل‌دهنده‌شان (برخلاف کامپیوترهای کلاسیک) امکان پردازش مقادیر زیاد اطلاعات را در زمان بسیار کم‌تری در مقایسه با رایانه‌های کلاسیک دارند. امروزه دانشگاه‌ها، مراکز تحقیقاتی و شرکت‌های بسیاری در سراسر جهان در حال تلاش برای ساخت اولین کامپیوتر کوانتومی حقیقی مقیاس‌پذیر هستند. چراکه با توجه به قدرت محاسباتی نهفته در محاسبات کوانتومی (در مقایسه با کامپیوترهای امروزیِ کلاسیک) کامپیوترهای کوانتومی نامزد اصلی جانشینی ابزار محاسبات کنونی ما هستند. اگرچه راه رسیدن به کامپیوتری بزرگ مقیاس و فراگیر شدن استفاده از آن طولانی به‌نظر می‌رسد، ولی، دست‌یابی و به‌کارگیری کامپیوترهای کوچک مقیاس در راستای محاسبات سریع برای شبیه‌سازی سامانه‌های زیستی و افزایش سرعت جست‌وجو در فضای وب در آینده نزدیک قابل پیش‌بینی است. بنابراین، ضروری است با پایه‌های محاسبات کوانتومی آشنا شویم تا امکان کار با ماشین‌های کوانتومی که به‌زودی از راه خواهند رسید را داشته باشیم.

الگوریتم‌های کوانتومی بر مبنای محاسبات کوانتومی طراحی می‌شوند. یکی از مخاطراتی که توسط الگوریتم‌های کوانتومی به جهان اعمال می‌شود، استفاده از آن‌ها به‌منظور تحلیل الگوریتم های رمزنگاری کلاسیک است. به‌عنوان‌مثال، الگوریتم کوانتومی شور با حل مسائلی همچون مسئله لگاریتم گسسته و مسئله تجزیه عددی بزرگ به عوامل اول خود، قابلیت به‌دست‌آوردن کلید در برخی از الگوریتم‌های رمزنگاری کلاسیک را دارا است. با توجه به وجود چنین الگوریتم‌های کوانتومی‌ای نیاز به اولیه‌های رمزنگاری وجود دارد تا بتوان جایگزین اولیه‌های رمزنگاری فعلی (به‌عنوان‌مثال، سامانه‌های رمزنگاری کلید عمومی مبتنی بر سختی حل مسئله لگاریتم گسسته) شوند. در راستای همین موضوع، الگوریتم‌های توزیع کلید و تسهیم راز کوانتومی از جمله طرح‌هایی هستند که به‌عنوان جایگزینی برای طرح‌های فعلی مطرح می‌شوند. اینجایگزین‌ها در برابر مخاطرات اعمالی از سوی خود الگوریتم‌های کوانتومی امن هستند؛ بنابراین، شایسته است تا به بررسی آن‌ها بپردازیم تا بتوانیم راهکارهای موردنیاز را برای مقابله با خطرات الگوریتم‌های کوانتومی ارائه دهیم.

تسهیم راز کلاسیک که از زیرشاخه‌های رمزنگاری کلاسیک است با توجه به ویژگی‌های خاص خود در بسیاری از طرح‌های امنیتی در دنیای امروز کاربرد دارد. برای بهبود طرح کلاسیک تسهیم راز و حل مشکل توزیع امن سهم‌ها در این طرح می‌توان از طرح‌های تسهیم راز کوانتومی که از زیرشاخه‌های رمزنگاری

کوانتومی است استفاده کرد. رمزنگاری کوانتومی در برابر مخاطرات الگوریتم‌های کوانتومی مقاوم است و اگر نیازمندی‌های امنیتی سامانه‌ای مبتنی بر رمزنگاری کوانتومی ارضا شود می‌توان از امن بودن آن سامانه مطمئن بود. وجود ویژگی‌های خاص مکانیک کوانتومی و الگوریتم پیتر شور، سبب شد که استفاده از مکانیک کوانتومی و محاسبات کوانتومی در رمزنگاری موردتوجه قرار بگیرند. رمزنگاری کوانتومی حوزه‌ای بسیار گسترده و میان‌رشته‌ای است (همان‌طور که رمزنگاری کلاسیک چنین است) و الگوریتم‌های کوانتومی مختلفی در این زمینه مطرح شده‌اند. به‌طورکلی هدف رمزنگاری کوانتومی انتقال و به اشتراک‌گذاری اطلاعات به‌صورت امن و در چارچوب قوانین مکانیک کوانتومی است. استفاده از رمزنگاری کلاسیک کلید متقارن به‌دلیل نیاز به کانال امن برای ارسال امن کلید در شبکه‌های اینترنت اشیاء نظامی غیرعملی است (البته این موضوع صرفاً به شبکه‌های اینترنت اشیاء نظامی محدود نمی‌شود بلکه این موضوع حقیقتی است که در رابطه با سایر شبکه‌ها همچون شبکه بلاک‌چین، شبکه هوشمند برق و غیره نیز صادق است). همچنین، با ظهور کامپیوترهای کوانتومی و امکان پیاده‌سازی الگوریتم شور که قابلیت تجزیه عدد و حل مسئله لگاریتم گسسته را در زمان خطی دارد، سامانه‌های رمزنگاری کلید عمومی با تهدید مواجه شده‌اند چرا که مبنای درستکار کردن برخی از سامانه‌های رمزنگاری کلید عمومی (منظور از درستکار کردن داشتن امنیت کافی است) سخت بودن حل مسئله‌های تجزیه عدد و لگاریتم گسسته است؛ بنابراین، برای توزیع کلید توسط سامانه‌های رمزنگاری کلید عمومی و سامانه‌های رمزنگاری کلید متقارن با چالش‌هایی روبه‌رو هستیم. می‌توان از طرح‌های تسهیم راز کلاسیک برای توزیع کلید بهره برد، اما در مورد طرح‌های تسهیم راز کلاسیک همان‌طور که ذکر شد چالشی به نام امکان توزیع امن سهم‌ها از ایجادکننده سهام به سهام‌داران وجود دارد. استفاده از کلیدهای از پیش به اشتراک گذاشته شده روشی است که در این موارد پیشنهاد می‌شود؛ اما این‌روش از کارایی و امنیت لازم مخصوصاً در کاربرد اینترنت اشیاء نظامی برخوردار نیست. روشی که در این موارد پیشنهاد می‌شود استفاده از تسهیم راز کوانتومی است.

تسهیم راز کوانتومی امکان توزیع امن کلید را فراهم می‌کند. در این پژوهش از تسهیم راز کوانتومی برای به اشتراک گذاشتن کلید در شبکه اینترنت اشیاء نظامی استفاده کرده‌ایم. قبل از اجرای این تسهیم راز کوانتومی از یک امضای جدید دیجیتالی (زیرشاخه رمزنگاری کلید عمومی کلاسیک) برای محرز شدن اصالت دو طرف درگیر در ارتباط استفاده کرده‌ایم. این استفاده در شروع ارتباط است و برای ادامه آن از کلید به اشتراک گذاشته شده توسط طرح تسهیم راز کوانتومی بین هویت‌ها استفاده کرده‌ایم. حتی اگر زیرساخت موردنیاز برای پیاده‌سازی محاسبات کوانتومی در کشور در آینده نزدیک ایجاد نشود می‌توان از طرح امضای دیجیتال جدید معرفی‌شده در این مقاله برای احراز اصالت و حفظ حریم خصوصی کاربران استفاده کرد. این طرح امضا ویژگی‌های زیادی دارد که در قسمت تحلیل امنیتی طرح جدید آن‌ها را مورد بررسی قرار داده‌ایم.

الگوریتم‌های رمزنگاری کوانتومی حوزه‌ای بسیار گسترده و میان‌رشته‌ای است و الگوریتم‌های کوانتومی مختلفی در این زمینه مطرح شده‌اند. به‌طورکلی هدف رمزنگاری کوانتومی، انتقال و به اشتراک‌گذاری اطلاعات به‌صورت امن و در چارچوب قوانین مکانیک کوانتومی است. دو بخش اصلی این حوزه، ۱- تسهیم راز کوانتومی یا اشتراک‌گذاری کوانتومی رمز[1] و ۲- توزیع کوانتومی کلید[2] هستند.

- **در تسهیم راز کوانتومی (QSS)**: هدف، انتقال یک رمز با استفاده از قوانین مکانیک کوانتومی از یک نفر مانند آلیس به شخص دیگری مانند باب است. این موضوع برای اولین بار توسط بوژک و هیلری[3] در ۱۹۹۸ معرفی شد [۳] و از آن زمان تاکنون پژوهش‌های بسیاری در این زمینه معرفی شده و همچنان حوزه‌ای فعال و مورد پژوهش است.

- **در توزیع کوانتومی کلید (QKD)**: هدف انتقال یک کلید با استفاده از مکانیک کوانتومی به‌صورت امن است. این کلید می‌تواند در پروتکل‌های رمزنگاری به‌کار رود و در واقع پاسخی برای مسئله قدیمی انتقال کلید در رمزنگاری کلاسیک به شمار می‌رود. این دسته از الگوریتم‌های کوانتومی رمزنگاری شامل زیردسته‌های همچون پروتکل $BB84$ [۴] است که همگی دارای کاربرد یکسان هستند و در تعداد پیام‌های تبادلی و سربارهای محاسباتی و مخابراتی تفاوت دارند. لازم به ذکر است که به‌طور معمول طرح‌های توزیع کلید کوانتومی سربار محاسباتی و مخابراتی بالاتری نسبت به طرح‌های تسهیم راز کوانتومی دارند. در اینجا لازم است اشاره کرد که در رابطه با سربار محاسباتی امضا دیجیتال ارائه‌شده در قسمت رمزنگاری کلاسیک باید گفت که این امضا بسیار کارا است. چراکه برای تشکیل این امضا از زوج‌نگار دوخطی استفاده نمی‌شود. همچنین، از ضرب روی منحنی بیضوی نیز بسیار کم استفاده شده است. همین باعث می‌شود طرح امضای جدید ارائه‌شده بسیار کارا باشد. توجه به زمان اجرای عملگرهای رمزنگاری که در جدول (۱) آمده است این موضوع را روشن‌تر می‌کند. چراکه

[1] Quantum Secret Sharing (QSS)
[2] Quantum Key Distribution (QKD)
[3] Buzek & Hillery

در بین همه عملگرهای، رمزنگاری، زمان‌برترین‌ها مواردی است که در این کار اشاره شد.

جدول (۱): زمان اجرای عملگرهای رمزنگاری در سخت‌افزاری با مشخصات بیان‌شده در جدول [۳۹].

INTEL CORE (TM) 2 DUO CPU @ 2.4GHZ	
عملگرهای رمزنگاری	زمان موردنیاز
T_{E-M} (elliptic curve multiplication)	5.4 ms
T_{E-A} (elliptic curve addition)	22.34 μs
T_P (pairing operation)	40.7 ms
T_{MAC} (MAC operation)	16.7 μs
T_{ENC} (encryption operation)	40.7 μs
T_h (hash function operation)	6 μs
T_{M-M} (modular multiplication)	186.2 μs
T_{M-A} (modular addition)	negligible

الگوریتم‌های پساکوانتومی از دیگر الگوریتم‌هایی هستند که در برابر مخاطرات الگوریتم‌های کوانتومی امن هستند. این الگوریتم‌ها چه در زمینه تسهیم راز، چه در سایر اولیه‌های رمزنگاری همانند الگوریتم رمزگذاری، امضای دیجیتال، تابع چکیده ساز و طرح‌های تعهد، ماهیت کلاسیک داشته و تاکنون هیچ راه‌حلی توسط کامپیوترهای کوانتومی برای حل این مسائل ارائه نشده است. هیچ تضمینی وجود ندارد که در چند سال آینده نیز هیچ راه‌حلی برای آن‌ها ارائه نشود. از طرف دیگر پیاده‌سازی این الگوریتم‌ها نیز با چالش‌هایی همراه است. به‌عنوان‌مثال، برای رمزگذاری کد مبنا بزرگ‌ترین چالش موجود حجم کلید است که به‌این‌ترتیب ذخیره‌سازی کلید یا انتقال آن از طریق یک کانال امن را با مشکل مواجه می‌کند. از سوی دیگر مشکل رمزگذاری مشبکه مبنا نیز سربار محاسباتی موجود است که پیاده‌سازی طرح‌های توافق کلید روی مشبکه را با مشکل مواجه می‌کند.

اهمیت تسهیم راز کوانتومی به نحوی است که NIST[1] برای تسهیم راز کوانتومی و کاربرد اصلی آن رمزنگاری آستانه‌ای کوانتومی یک کارگاه در سال قبل میلادی برگزار کرد که جزئیات آن قابل‌پیگیری است. علاوه بر موارد گفته‌شده، ویژگی‌های مثبت موجود در مکانیک کوانتومی همانند درهم‌تنیدگی و برهم‌نهی باعث ایجاد تغییر اطلاعات کیو بیت در هنگام مشاهده شدن و در نتیجه مقاومت در برابر شنود می‌شود. از این ویژگی برای مقابله با حملات خارج از سامانه مثل شنود کلید یا شنود رازها می‌توان استفاده کرد. با کمک این ویژگی می‌توان از خدشه‌دار نشدن اطلاعات هرچند با وجود امن نبودن کانال‌های ارتباطی اطمینان حاصل نمود.

۱-۲- اهمیت و ضرورت پرداختن به شبکه اینترنت اشیاء نظامی برای امنیت ملی

ارزشمند است که اشاره کنیم این پژوهش مستقیماً در راستای ارضای نیازمندی‌های نقشه راه و برنامه عملیاتی اینترنت اشیاء در کشور است. این نقشه راه و برنامه عملیاتی توسط مرکز تحقیقات مخابرات ایران تنظیم شده است. برای مطالعه بیشتر در رابطه با پیش ارائه نقشه راه اینترنت اشیاء کشور به [۵] رجوع شود. ما سعی کرده‌ایم نه تنها در راستای این نقشه راه به برآورده کردن نیازمندی‌های امنیتی اینترنت اشیاء با تمرکز بر کاربرد نظامی آن بپردازیم، بلکه سعی کرده‌ایم با طرح ارائه‌شده الزامات امنیتی بیشتری از آنچه در این نقشه راه اشاره شده است را برآورده کنیم. به‌عنوان مثال، از منظر امنیتی در این نقشه راه صرفاً به مشکلات حریم خصوصی و امنیت اطلاعات در اینترنت اشیاء اشاره شده است. این در حالی است که در طرح پیشنهادی، ما بسیار فراتر از رفع این نیازمندی‌ها رفته‌ایم.

کلپر[2] که ریاست هوش ملی آمریکا را داشت در سال ۲۰۱۶ گفته بود: "در آینده، خدمات و سرویس‌های اطلاعاتی از بستر اینترنت اشیاء به‌منظور تشخیص، نظارت، پیمایش، رهگیری مکانی و هدف‌یابی استفاده خواهند کرد" [۶]. در جلسه‌ای خاص بر روی کاربردهای نظامی شبکه اینترنت اشیاء که توسط موسسه مهندسان برق و الکترونیک[3] در اوایل سال ۲۰۱۸ صورت گرفت به ضرورت و اهمیت ورود اینترنت اشیاء به حوزه نظامی برای افزایش کارایی در میدان جنگ اشاره شد [۷]. سایت پژوهش جهانی[4] دارای گزارشی تحت عنوان "جنگ سایبری آژانس امنیت ملی[5] از قطعات متصل به اینترنت به‌عنوان بستر سلاح‌های جنگی بهره می‌برد" است [۸]. در این گزارش بیان شده است که آژانس امنیت ملی در جنگ سایبری از اینترنت اشیاء به‌عنوان بستری برای سلاح‌های جنگی استفاده می‌نماید. در نتیجه، خانه مردم به میدان جنگ تبدیل خواهد شد [۸]. نکته ذکرشده بسیار اهمیت دارد، چراکه بیان می‌دارد که اینترنت اشیاء در کنار تمامی مزایایی که برای کشور ما دارد و می‌تواند داشته باشد، می‌تواند بستری برای جاسوسی و انتقال اطلاعات خصوصی افراد به سازمان‌ها و کشورهای دشمن باشد. همچنین، این گزارش بیان می‌کند که اعضای پنج چشم که شامل کشورهای انگلیس، آمریکا، کانادا، استرالیا و نیوزیلند هستند، طی تلاشی سخت، در جست‌وجو گسترش تسلیحات دیجیتالی برای ایجاد برتری در

[1] National Institute of Standards and Technology

[2] James Clapper
[3] Institute of Electrical and Electronics Engineers
[4] https://www.globalresearch.ca
[5] National Security Agency

جنگ سایبری هستند. شبکه اینترنت اشیاء در کنار تمام مزیت‌هایی که دارد، می‌تواند به ضرر مخترع اینترنت اشیاء یعنی آمریکا نیز عمل کند. به گزارش پایگاه خبری دِ-هیل[1]: "سطح امنیتی پایین فناوری شبکه اینترنت اشیاء (که بخش زیادی از آن بیرون از مرزهای آمریکا شکل می‌گیرد) پتانسیلی است برای ایجاد تسلیحات سایبری با توانایی تخریب وسیع که آمریکا را هدف قرار داده‌اند. عملکرد اینترنت اشیاء برای مهاجمان بدین‌شکل است که سنگ کوچک آن‌ها را به موشکی تبدیل می‌کند." [۹].

در جلسه چهل و پنجم شورای عالی فضای مجازی که در ۲۷ آذر سال ۱۳۹۶ به ریاست دکتر حسن روحانی تشکیل شد، تصویب شد تا در راستای گسترش سامانه‌های هوشمند و اینترنت اشیاء با رعایت اصول اقتصاد مقاومتی، سند مناسب تهیه و تنظیم گردد [۱۰]. در خبری که در تاریخ ۲۳ دی ماه سال ۱۳۹۶ انتشار یافت ذکر شد که کارگروه اینترنت اشیاء در مرکز ملی فضای مجازی جلسه‌ای تحت عنوان ضرورت هماهنگی ملی در بهره‌گیری از ظرفیت اینترنت اشیاء برگزار کرده است. روابط عمومی مرکز ملی فضای مجازی گزارش داده است که اعمال حاکمیت بر اینترنت اشیاء با تولید سکوی وطنی برای کاربردهای داخلی، مدیریت تجهیزات و اشیاء هوشمند به‌واسطه بسترهای مناسب و ایمن در راستای جلوگیری از خروج وسیع اطلاعات از کشور، جلوگیری از موازی‌کاری در برنامه‌ریزی، جلوگیری از صرف هزینه، از مهم‌ترین نیازمندی‌های هماهنگی و همکاری سازمان‌های گوناگون در سطح کشور است. همچنین، این گزارش اعلام کرده است که نمونه‌هایی از فعالیت‌های صورت‌گرفته در کشور در این حوزه، به‌صورت نامنظم و بدون هماهنگی و برنامه‌ریزی لازم صورت گرفته است [۱۱]. نقشه راه توسعه فناوری اینترنت اشیاء در کشور در راستای ایجاد فضایی منسجم و توسعه‌یافته، ارائه سرویس‌های مختلف، دستیابی به الزامات، قانون و مقررات و سیاست‌گذاری، زیرساخت‌های مورد نیاز و شناسایی ارائه سرویس‌های مختلف دستیابی به اهداف شامل دستیابی به بازار توسعه‌یافته و خدمات متنوع تدوین می‌گردد. ازاین‌رو هدف پروژه تدوین نقشه راه اینترنت اشیاء دستیابی به اهداف پیشنهادی در این سند برای توسعه و پشتیبانی از فناوری اینترنت اشیاء تا افق زمانی ۱۴۰۴ است. به‌طوری‌که نقش وزارت ارتباطات و فناوری اطلاعات در آن در حوزه‌های مختلف مشخص شود. وزارت ارتباطات و فناوری اطلاعات عهده‌دار برنامه‌ریزی، پشتیبانی و توسعه زیرساختار و توانایی‌های ملی مخابراتی و اطلاعاتی کشور، اینترنت اشیاء را به‌عنوان موضوع محوری توسعه فناوری و آینده کسب‌وکارهای مرتبط با فاوا در نظر گرفته است.

[1] https://thehill.com/

مرکز تحقیقات مخابرات ایران، در اولین گام مسئولیت تدوین نقشه راه و ارائه برنامه عملیاتی اینترنت اشیاء در کشور را عهده‌دار شده است [۱۲]. دیدگاه وزارت ارتباطات و فناوری اطلاعات در این خصوص به شرح زیر است [۱۲]: ۱- طراحی و تدوین نقشه راه اینترنت اشیاء کشور. ۲- شناسایی بازیگران تأثیرگذار بر پیاده‌سازی فضای یکپارچه در کشور. ۳- تعیین اقدامات و برنامه‌های عملیاتی وزارت ارتباطات و فناوری اطلاعات برای توسعه اینترنت اشیاء در کشور از جمله: تأمین امنیت و زیرساخت‌های توسعه مورد نیاز برای توسعه اینترنت اشیاء در کشور، تأمین و توسعه تولید ایده، سرویس و محصولات مرتبط برای توسعه اینترنت اشیاء در کشور، تأمین و توسعه الزامات قانونی و حاکمیتی در محدوده وظایف وزارت ارتباطات و فناوری اطلاعات، و تأمین و توسعه بازار جهت ارائه سرویس‌های اینترنت اشیاء در کشور.

شبکه اینترنت اشیاء نظامی بستری است که می‌تواند با توجه به امنیت ضعیفی که دارد درجهت انتقال اطلاعات حیاتی کشور به سازمان‌های معاند، علیه کشور استفاده شود. از طرف دیگر، شبکه اینترنت اشیاء بستری است که درصورتی‌که سرمایه‌گذاری کافی‌ای در این بخش صورت گیرد می‌تواند برای پیشبرد اهداف امنیتی و دفاعی کشور بسیار مفید باشد؛ بنابراین، ضروری است تا به ابعاد مختلف شبکه اینترنت اشیاء از جمله بحث امنیت آن بپردازیم. در اینترنت اشیاء نظامی نیازمندی‌های امنیتی همچون محرمانه ماندن اطلاعات، محرز شدن اصالت فرستنده پیام و محرز شدن اصالت اطلاعات ارسال‌شده از اهمیت بسیار زیادی برخوردار است. بدیهی است که اگر اشتباهی در فرایند برآورده کردن این نیازمندی‌ها و سایر نیازمندی‌های امنیتی رخ دهد خسارت‌های جبران‌ناپذیری به وجود خواهد آمد.

۲- روش تحقیق

نوع پژوهش صورت‌گرفته در این مقاله چندمنظوره از نوع بنیادی- کاربردی- توسعه‌ای که می‌باشد دلیل آن در ادامه آورده شده است. در طول پژوهش صورت‌گرفته در زمان نگارش مقاله سعی بر این شده که به ابعاد مختلف شبکه اینترنت اشیاء نظامی و الگوریتم‌های کوانتومی پرداخته شود. ابتدا مبانی، مفاهیم و اصطلاحات مربوطه مطالعه شده‌اند. سپس پیشینه پژوهش در حوزه امنیت اینترنت اشیاء و الگوریتم‌های کوانتومی مورد بررسی دقیق قرار گرفته‌اند. با توجه به ویژگی‌های تسهیم راز کوانتومی که از زیرشاخه‌های رمزنگاری الگوریتم‌های کوانتومی می‌باشد به پیشینه پژوهش در حوزه تسهیم راز کوانتومی نیز پرداختیم، تا دید کافی برای ارائه طرح جدید احراز اصالت و محرمانگی در شبکه اینترنت اشیاء نظامی داشته باشیم. دلیل امر ذکرشده این

است که یکی از کاربردهای تسهیم راز کوانتومی در برآورده کردن نیاز امنیتی به احراز اصالت و توزیع امن کلید برای برآورده کردن نیاز به محرمانگی است. ما نیز، پس از مطالعه تسهیم راز کوانتومی بر آن شدیم تا از مزایا و ویژگی‌های آن برای طراحی طرحی به‌منظور ارتقا امنیت در شبکه اینترنت اشیاء نظامی استفاده کنیم. تسلط به علم رمزنگاری کلاسیک با تمرکز بر رمزنگاری کلید عمومی نیز از دیگر مراحل آماده‌سازی برای نگارش این مقاله بوده است؛ بنابراین، نوع پژوهش از نوع بنیادی است و با توجه به نوآوری فنی طرح از نوع توسعه‌ای نیز هست. ارزشمند است که اشاره کنیم طرح جدید ارائه‌شده در صورت تأمین زیرساخت‌های پیاده‌سازی الگوریتم‌های کوانتومی طرحی عملی و قابل پیاده‌سازی است؛ همچنین، مستقل از پیاده‌سازی زیرساخت‌های کوانتومی در کشور، می‌توان طرح ارائه‌شده را صرفاً با استفاده از طرح امضای دیجیتال کلاسیک جدید پیاده کرد و از مزایای آن بهره‌مند شد؛ و هرگاه که امکانات کوانتومی لازم در کشور ایجاد شد به سمت اعمال قسمت دوم طرح که استفاده از رمزنگاری کوانتومی است پیش رفت. در نتیجه، طرح معرفی‌شده جنبه‌کاربردی نیز دارد. در نهایت می‌توان گفت که نوع این پژوهش بنیادی-کاربردی- توسعه‌ای می‌باشد.

طرح ارائه‌شده از دو مفهوم رمزنگاری کلید عمومی (کلاسیک) و تسهیم راز کوانتومی استفاده می‌کند و هر قسمت نیازمندی‌های امنیتی خاصی را در شبکه برآورده می‌کند. می‌توان از هر قسمت با توجه به برنامه عملیاتی بهره برد. در این پژوهش منابع کتابخانه‌ای در حوزه الگوریتم‌های کوانتومی (تسهیم راز کوانتومی، توزیع کلید کوانتومی و غیره)، و شبکه اینترنت اشیاء نظامی و ابعاد مختلف آن (معماری، کاربردها، امنیت و غیره) به‌صورت جامع موردمطالعه قرار گرفته است. منظور از منابع کتابخانه‌ای مواردی هست که در ادامه آورده می‌شوند: ۱- کتاب‌ها. ۲- مقاله‌های چاپ‌شده در مجله‌ها و ارائه‌شده در کنفرانس‌ها چه بین‌المللی چه داخلی. ۳- تارنماهای تخصصی و علمی. ۴- اسناد، مدارک و مطالعات علمی مرتبط با موضوع پژوهش. ۵- سایت‌های خبری مرتبط با موضوع پژوهش. برای نگارش این مقاله مطالعه‌ای جامع از منابع کتابخانه‌ای اشاره‌شده صورت‌گرفته است؛ بنابراین، روش انجام این پژوهش روش کتابخانه‌ای است. برای نگاشتن نوآوری این مقاله نیز از روش تحقیق کتابخانه‌ای استفاده شده است. به‌این‌ترتیب که ابتدا مفاهیم کلیدی موردنیاز در الگوریتم‌های کوانتومی و تسهیم راز کوانتومی به‌تفصیل مطالعه شده‌اند. همچنین ابعاد مختلف شبکه اینترنت اشیاء نظامی نیز با روش تحقیق کتابخانه‌ای به‌طور کامل موردمطالعه قرار گرفت. سپس برای بررسی دقیق‌تر و جزئی‌تر الگوریتم‌های کوانتومی و تسهیم راز کوانتومی منابع متعددی مورد جست‌وجو و مطالعه قرار گرفتند تا شناخت جامعی نسبت به ساختار ریاضی الگوریتم‌های کوانتومی و تسهیم راز کوانتومی، کاربردها و ویژگی‌های این الگوریتم‌ها حاصل شود. همچنین، دانش رمزنگاری کوانتومی و رمزنگاری کلاسیک در طول پژوهش حاصل شد. منظور از دانش رمزنگاری کوانتومی و کلاسیک، ریاضیات مربوط به آن‌ها، سازوکار طرح‌های امنیتی مبتنی بر این علوم و غیره است. سپس سازوکاری برای برآورده کردن نیازمندی‌های امنیتی مهم شبکه اینترنت اشیاء نظامی با استفاده از تسهیم راز کوانتومی و احراز اصالت اولیهِ مبتنی بر رمزنگاری کلید عمومی طراحی شد.

مقاله پیش‌رو دارای دو هسته اصلی ۱- الگوریتم‌های کوانتومی و تسهیم راز کوانتومی و ۲- شبکه اینترنت اشیاء نظامی است. مراحل زیر برای نگاشتن مقاله در هر یک از دو هسته اصلی اشاره شده طی شده‌اند.

- در رابطه با الگوریتم‌های کوانتومی و تسهیم راز کوانتومی

۱- آشنایی با مفاهیم اولیه و تعاریف (تسهیم راز کلاسیک و تسهیم راز کوانتومی). ۲- مطالعه جامع الگوریتم‌های کوانتومی اولیه و مهم و مطالعه نمونه‌های اولیه و مهم طرح‌های تسهیم راز کلاسیک و کوانتومی از روی منابع کتابخانه‌ای ذکر شده. ۳- پی‌بردن به ویژگی‌های مثبت و منفی الگوریتم‌های کوانتومی رمزنگاری در مقایسه با الگوریتم‌های کلاسیک رمزنگاری و نحوه کارکرد آن‌ها (به‌عنوان‌مثال، مطالعه ویژگی های مثبت و منفی تسهیم راز کوانتومی در مقایسه با تسهیم راز کلاسیک). ۴- پی‌بردن به ارتباط الگوریتم‌های کوانتومی با بحث امنیت و کاربرد آن‌ها در ارتقا یا نقض امنیت (به‌عنوان‌مثال، مطالعه توانایی‌های منحصربه‌فرد تسهیم راز کوانتومی در برآورده کردن نیازمندی‌های امنیتی مختلف همچون محرمانگی و احراز اصالت (احراز اصالت پیام و احراز اصالت هویت فرستنده پیام))

- در رابطه با شبکه اینترنت اشیاء نظامی

۱- آشنایی با مفاهیم اولیه (معماری شبکه اینترنت اشیاء نظامی، استانداردها و پروتکل‌های ارتباطی شبکه اینترنت اشیاء نظامی، امنیت و نیازمندی‌های امنیتی شبکه اینترنت اشیاء نظامی و کاربردهای شبکه اینترنت اشیاء نظامی). ۲- مطالعه جامع پژوهش‌های صورت‌گرفته در حوزه امنیت این شبکه، لازم به ذکر است که برای طراحی طرح جدید بیش از بیست طرح امنیتی، چاپ‌شده در معتبرترین مجله‌های علمی و ارائه‌شده در مشهورترین کنفرانس‌های جهان در حوزه‌های مختلف (علوم کامپیوتر، علم رمزنگاری، علم ریاضیات کاربردی، مهندسی برق مخابرات و شبکه و مهندسی فناوری اطلاعات و امنیت) که

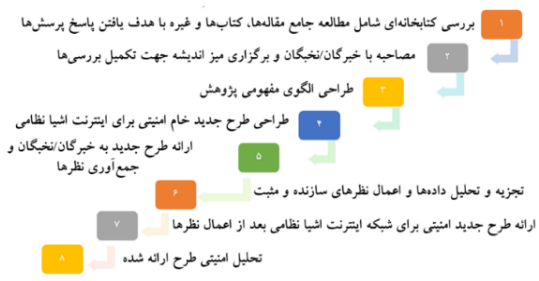
همگی در راستای تأمین امنیت این شبکه بودند، موردمطالعه دقیق قرار گرفتند. این کار بدین سبب صورت گرفت تا دید کلی نسبت به سازوکارهای تأمین امنیت به‌دست آید.

۳- پیدا کردن نقاط ضعف طرح‌های مطالعه شده به‌عنوان‌مثال، برخی طرح‌ها در برابر حمله تکرار آسیب‌پذیر بودند که سعی شده است این آسیب‌پذیری در طرح ارائه شده حل شود. همچنین، برخی طرح‌ها در برابر حمله جعل هویت آسیب‌پذیر بودند که طرح پیشنهادی ما در برابر این حمله مقاوم است (برای اطلاع بیشتر از سایر جنبه‌های برتر طرح ارائه‌شده به بخش تحلیل امنیتی طرح جدید رجوع شود).

۴- تسلط بر ریاضیات حاکم بر طرح‌های مطالعه شده برای برآورده کردن امنیت شبکه اینترنت اشیاء (به‌عنوان‌مثال، تسلط به ریاضیات گسسته، محاسبات پیمانه‌ای، منحنی بیضوی، زوج نگار دوخطی و غیره).

۵- تلاش برای طراحی طرح جدید به‌منظور رفع نیازمندی‌های امنیتی شبکه اینترنت اشیاء نظامی، امن‌تر از کارهای مشابه صورت گرفته (انجام طوفان فکری[1] برای به‌دست‌آوردن طرح های مختلف و تلاش برای اعمال حمله‌های مختلف مطرح در این شبکه‌ها به طرح خام اولیه پیشنهادی و رفع آسیب‌پذیری های طرح جدید و در نهایت به‌دست‌آوردن طرحی اصلاح شده و آماده ارائه). ۶- تحلیل امنیتی طرح جدید با دقت به نیازمندی‌های امنیتی مطرح.

به‌عنوان جمع‌بندی این بخش از مقاله، در ادامه ساختار پژوهش را در شکل (۱) نشان داده شده است.



شکل (۱): ساختار پژوه.

۳- پیشینه تحقیق

تا جایی که اطلاع داریم پژوهشی مشابه در راستای استفاده از الگوریتم رمزنگاری کوانتومی و کلاسیک در برآورده کردن نیازمندی‌های امنیتی شبکه اینترنت اشیاء (چه کاربرد نظامی و چه غیرنظامی) تاکنون صورت نگرفته است. از مقاله‌های اخیر چاپ شده در سال ۲۰۱۹ می‌توان به [۱۳ و ۱۴] اشاره کرد. در [۱۳] مقاومت در برابر حمله شنود و حمله تکرار وجود دارد و احراز اصالت نیز برقرار می‌شود. اما، حریم خصوصی حفظ نمی‌شود. مقاله ذکر شده، از رمزنگاری کلید متقارن و توکن‌های شناسه‌مبنا استفاده کرده است. طرح ارائه‌شده در مقاله [۱۴] در برابر حمله جعل هویت مقاوم است اما، در برابر حمله منع خدمت مقاوم نیست. این مقاله برای حفظ حریم خصوصی از شبه‌شناسه‌ها به‌جای شناسه اصلی استفاده کرده است. در قسمت تحلیل امنیتی طرح ارائه شده (بخش ۴-۷)، طرح خود را با پژوهش‌های مشابه از منظر تأمین نیازمندی‌های امنیتی به‌صورت کامل مقایسه کرده‌ایم. طرح پژوهشی معرفی‌شده در [۱۵] در برابر حمله استراق سمع و در برابر حمله جعل مقاوم نیست چراکه از سازوکار کافی برای احراز اصالت برخوردار نیست. اما، این طرح در برابر حمله تکرار به خاطر حفظ تازگی مقاوم است. این در حالی است که طرح پیشنهادی این مقاله در برابر تمامی حمله‌های ذکرشده مقاوم است. در مقاله‌های [۱۸-۱۶]تازگی حفظ شده است، اما، احراز اصالت در این طرح‌ها برآورده نمی‌شود. در طرح‌های پیشنهادی مقاله‌های [۲۱-۱۹] حریم خصوصی کاربرها به‌صورت کامل حفظ می‌شود. اما، نیاز به محرز شدن اصالت کاربرها بی‌پاسخ مانده است. در مراجع [۴۰-۲۲] حریم خصوصی کاربرها حفظ نمی‌شود. در مراجع [۱۸-۱۶ و ۴۰-۲۲] ارتباط ناپذیری برآورده نمی‌شود. در [۱۵] ارتباط ناپذیری تا حدی برآورده می‌شود اما به‌صورت کامل و مشابه آنچه با استفاده از تعداد زیاد مقادیر تصادفی در طرح ارائه‌شده برآورده می‌شود نیست.

۴- طرح جدید برای ارتقا امنیت شبکه اینترنت اشیاء نظامی با استفاده از رمزنگاری

۴-۱- طرح تسهیم راز کوانتومی با استفاده از حالت های درهم‌تنیده

در بخش ۱-۲ به الگوریتم‌های توزیع کلید کوانتومی اشاره شد. در الگوریتم‌های توزیع کلید کوانتومی برای ارسال امن سهم‌ها از توزیع‌کننده به شرکت‌کننده‌ها، به تبادلات زیاد نیازمندیم که هزینه و وقت زیادی را از ما نسبت به استفاده از تسهیم راز کوانتومی می‌گیرد. با استفاده از حالت‌های درهم‌تنیده کوانتومی می‌توان تسهیم راز و انتقال امن سهم‌ها را به‌صورت توأمان انجام داد تا کارایی طرح افزایش یابد. در این طرح از حالت‌های درهم‌تنیده سه‌تایی GHZ استفاده می‌شود. این طرح توسط هیلاری و همکارانش در سال ۱۹۹۸ ارائه شد [۴۶]. حالت‌های GHZ دارای سه کیوبیت هستند و به‌صورت $|GHZ\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}}$ تعریف می‌شوند. این سه ذره درهم‌تنیده هستند و می‌توان از آن برای تسهیم راز استفاده کرد. حالت $|GHZ\rangle$ را

[1] brain storm

می‌توان بر پایه عملگرهای پاولی X یعنی $|X+\rangle$ و $|X-\rangle$ بسط داد. $|X+\rangle$ و $|X-\rangle$ به‌صورت $|X+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ و $|X-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ تعریف می‌شوند. حال می‌توان حالت $|GHZ\rangle$ را به‌صورت زیر نوشت:

$$|GHZ\rangle = (|X+\rangle \otimes |X+\rangle + |X-\rangle \otimes |X-\rangle)|X+\rangle + (|X+\rangle \otimes |X-\rangle + |X-\rangle \otimes |X+\rangle)|X-\rangle)$$

ایده این طرح این است که اگر بخواهیم طرح تسهیم راز را میان سه نفر اجرا کنیم، کافی است از هر سه نفر بخواهیم اندازه‌گیری خود را در پایه X انجام دهند. در این صورت هر دو نفر می‌توانند به نتیجه اندازه‌گیری نفر سوم برسند، به این صورت که اگر نتیجه اندازه‌گیری آن‌ها یکسان باشد، نتیجه اندازه‌گیری نفر سوم $|X+\rangle$ و در صورت یکسان نبودن، نتیجه اندازه‌گیری نفر سوم $|X-\rangle$ خواهد بود. هم‌چنین می‌توان از پایه‌های پاولی Y نیز استفاده کرد که به‌صورت $|Y+\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$ و $|Y-\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$ تعریف می‌شوند. با در نظر گرفتن این تعریف می‌توان حالت $|GHZ\rangle$ را به‌صورت زیر نوشت:

$$|GHZ\rangle = (|X+\rangle \otimes |Y+\rangle + |X-\rangle \otimes |Y-\rangle)|Y-\rangle + ((|X+\rangle \otimes |Y-\rangle + |X-\rangle \otimes |Y+\rangle)|Y+\rangle)$$

حال اگر نفر اول اندازه‌گیری خود را بر پایه X و دو نفر دوم اندازه‌گیری بر پایه Y انجام دهد، در این صورت اگر نتیجه هر دو مثبت یا منفی باشد، در این صورت نتیجه نفر سوم $|Y-\rangle$ و اگر نتیجه اندازه‌گیری دو نفر یکی مثبت و دیگری منفی باشد، نتیجه اندازه‌گیری نفر سوم $|Y+\rangle$ خواهد بود. نکته‌ای که وجود دارد این است که هر سه نفر یا یک نفر نباید از پایه Y برای اندازه‌گیری خود استفاده کنند، در این صورت نتیجه اندازه‌گیری نفر سوم با داشتن نتیجه‌گیری اندازه‌گیری نفر اول و دوم قابل بازیابی نخواهد بود. به عبارت دیگری برای این‌که بتوان از این‌روش استفاده کرد باید تعداد استفاده‌کنندگان از پایه X برای اندازه‌گیری فرد باشد. برای این‌که این طرح به یک طرح تسهیم راز کوانتومی آستانه‌ای تبدیل کنیم، شخص توزیع‌کننده یک کیوبیت را به‌عنوان راز برای خود نگه می‌دارد و دو کیوبیت را برای دو نفر حاضر در طرح تسهیم راز ارسال می‌کند. حال کافی است دو نفر حاضر با پایه مناسب اندازه‌گیری را انجام دهند و با مقایسه آن با یکدیگر به کیوبیت موجود در نزد توزیع‌کننده یعنی راز برسند. به این ترتیب توانستیم طرح تسهیم راز کوانتومی آستانه‌ای $(2,2)$ ایجاد کنیم که هر دو نفر می‌توانند با داشتن حالت‌های خود حالت توزیع‌کننده یعنی راز را به‌دست آورند. اما باید به این نکته توجه داشت که باید تعداد نفراتی که برای اندازه‌گیری از پایه X استفاده می‌کنند، فرد باشد. در این‌جا در هربار، نفرات شرکت‌کننده در تسهیم راز پایه خود را که برای اندازه‌گیری استفاده کرده‌اند، به‌صورت عمومی به توزیع‌کننده اعلام می‌کنند و توزیع‌کننده با بررسی آن و در صورت فرد بودن دفعات استفاده از پایه X نتیجه را مقبول اعلام می‌کند و در غیر این صورت نتیجه آن دور را مردود اعلام می‌کند و هر سه نفر نتیجه اندازه‌گیری خود را حذف می‌کنند. پس از این‌که این عمل را چندین بار تکرار کردند، در پایان تعدادی از بیت‌های به‌دست‌آمده را به‌صورت عمومی با یکدیگر مقایسه می‌کنند و در صورتی اگر حتی در یک بیت تفاوت داشته باشند، می‌توان گفت شنودگر در حال شنود بوده است و باید طرح GHZ را از نو تکرار کنند. در صورتی که تمامی بیت‌ها یکسان باشند، آن را از رشته‌بیت اصلی این بخش حذف می‌کنند و بقیه رشته‌بیت را به‌عنوان کلید می‌پذیرند و نهادهای حاضر در تسهیم راز می‌توانند راز را به‌دست آورند.

طرح GHZ نسبت به طرح BB84 تعداد تبادلات و هزینه کم‌تری دارد، اما در اینجا ما تنها هزینه استفاده از حالت درهم‌تنیده را می‌دهیم و می‌توانیم کارایی را تا حد زیادی افزایش دهیم. در سال ۲۰۰۱، ژانگ و همکارانش طرحی را ارائه کردند که در آن از حالت‌های کوانتومی درهم‌تنیده به‌عنوان کلید از پیش به اشتراک گذاشته استفاده می‌شود [۴۷] در این طرح توزیع‌کننده از حالت درهم‌تنیده کوانتومی که در بالا اشاره شد به‌عنوان کلید استفاده می‌کند. به این صورت که حالت کوانتومی دلخواه خود را با کیوبیت درهم‌تنیده رمز می‌کند و بر روی کانال عمومی ارسال می‌کند. حال فرد شرکت‌کننده در طرح تسهیم راز یا توزیع کلید، با کیوبیت اولیه دریافتی پیام ارسالی را رمزگشایی می‌کند و به حالت کوانتومی موردنظر توزیع‌کننده دست می‌یابد. به این ترتیب بدون استفاده از تبادلات زیاد و بار اضافه می‌توانیم بیت‌ها را منتقل کنیم. هم‌چنین می‌توان با استفاده از کدگذاری مناسب طرحی را که در بالا اشاره شد برای تسهیم راز کوانتومی آستانه‌ای $(2,3)$ و از آن مهم‌تر برای طرح آستانه‌ای $(k, 2k-1)$ به شرط اول بودن $2k-1$ ایجاد کرد. به‌عنوان جمع‌بندی، مسئله توزیع امن سهم‌ها مسئله مهمی است که برای این منظور می‌توان از طرح‌های توزیع کلید کوانتومی مانند BB84 استفاده کرد. اما، این طرح‌ها کارایی مناسبی در مقایسه با طرح‌های تسهیم راز ندارند. به همین دلیل به طرح تسهیم حالت درهم‌تنیده GHZ اشاره کردیم که نسبت به طرح BB84 علاوه بر این‌که کارایی مناسب‌تری دارد، کار توزیع کلید و تسهیم راز را به‌طور توأمان انجام می‌دهد.

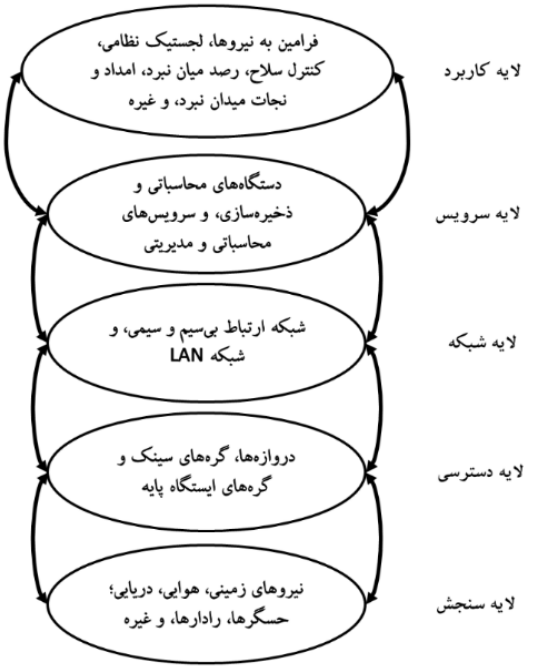
۴-۲- چهارچوب شبکه طرح جدید

ابتدا به معرفی چهارچوب شبکه که شامل ساختار شبکه و مدل امنیتی شبکه است، می‌پردازیم.

۴-۲-۱- ساختار شبکه طرح جدید

معماری شبکه اینترنت اشیاء نظامی را در شکل (۲) نشان داده‌ایم [۱]. ساختار در نظر گرفته‌شده در این مقاله شامل دو قسمت

است. ۱- کاربران موجود در لایه دسترسی (سامانه مورد نظر یک یا چند مدیر گروه دارد. بر حسب میزان امنیت مورد نظر مدیر یا مدیران گروه می‌توانند هویتی که عضو لایه‌های بالای شبکه است فرض شود و یا از همان لایه دسترسی عضوی را به‌عنوان مدیر گروه فرض کرد.). ۲- کاربران موجود در لایه سنجش. ساختاری که برای شبکه مورد بررسی برای اینترنت اشیاء نظامی در این مقاله در نظر می‌گیریم از دو لایه کلی شامل لایه دسترسی و لایه سنجش تشکیل شده است. لایه زیرین مربوط به حس‌گرها و نیروهای زمینی، هوایی، دریایی و غیره است و لایه بالایی نیز از کاربران لایه دسترسی تشکیل شده است. ارتباط بین کاربران لایه سنجش با لایه بالایی خود عموماً به‌صورت بی‌سیم است که همین مسئله ما را بر آن می‌دارد تا به تأمین امنیت فضای بین این دولایه تمرکز کنیم. مدیرگروه مسئول بارگذاری اولیه سامانه و ثبت‌نام کردنِ کاربران معتبر موجود در دولایه مورد بررسی در شبکه است. مسئولیت افشای هویت اصلی کاربران شبکه فقط و فقط با مدیر گروه است. فرض می‌کنیم که مدیر گروه از لحاظ قدرت محاسبه و میزان حافظه به‌اندازه موردنیاز قدرت‌مند می‌باشد. لایه دسترسی از یکسری دروازه و در واقع کاربرانی تشکیل شده است که وظیفهِ جمع‌آوریِ اطلاعاتِ کاربرانِ لایهِ سنجش را دارند. اطلاعات جمع‌آوری شده، پردازش اولیه شده و سپس به لایه‌های بالا برای تصمیم‌گیری‌های نظامی ارسال می‌شوند. در لایه سنجش متناسب با نوع جنگ، نیروهای نظامی شامل نیروهای زمینی، هوایی، و دریایی و همچنین یکسری حسگرها برای جمع‌آوری اطلاعات مختلف وجود دارند.



شکل (۲): معماری شبکه اینترنت اشیاء نظامی

۴-۲-۲- مدل امنیتی شبکه طرح جدید

این شبکه نیازمندی‌های امنیتی زیر را باید ارضا کند.

- احراز اصالت پیام و فرستنده پیام: پیام‌های ارسالی توسط کاربران لایه سنجش باید احراز اصالت بشوند تا از عدم تغییر و یا جعل آن‌ها و همچنین از این‌که توسط یک هویت معتبر در شبکه ارسال شده‌اند اطمینان حاصل کرد. به احراز اصالت پیام، حفظ یکپارچگی پیام نیز گفته می‌شود و به احراز اصالت فرستنده پیام مجازشناسی نیز گفته می‌شود.
- گمنام بودن نیروهای نظامی: در حین استفاده از شبکه اینترنت اشیاء نظامی در کاربردهای امنیتی خاصی به‌دلیل افزایش سطح امنیت نیاز هست تا هویت اصلی فرستنده پیام فاش نشود. این در حالی است که نهادهای بالادستی باید بتوانند در مواقع بروز جرم و خطا به هویت اصلی فرستنده پیام پی ببرند. همچنین در مواقع خاص باید قابلیت مشخص‌کردن دقیق هویت اصلی فرستنده وجود داشته باشد؛ بنابراین، درعین‌حال که هویت اصلی کاربران مخفی می‌ماند، فقط مدیرگروه باید بتواند در مواقع لزوم به هویت اصلی کاربران شبکه برای اعمال مجازات (در مواقع بروز خطای عمد در ارسال اطلاعات) و یا کسب آگاهی از جزئیات دقیق هویت فرستنده پیام (در صورت نیاز امنیتی به این کار) دسترسی پیدا کند.
- ارتباط ناپذیری: دشمن نباید بتواند پیام‌های ارسالی در بازه‌های زمانی مختلف توسط یک کاربر را به یکدیگر ارتباط بدهد.
- انکارناپذیری: نیروهای نظامی داخل شبکه نباید بتوانند در هیچ زمانی پیام‌های ارسال‌شده توسط خودشان را انکار کنند.
- تازگی پیام‌ها: دشمن نباید بتواند پیام‌های ارسالی در بازه‌های زمانی گذشته را دوباره در شبکه تحت هر عنوان و برای ارسال به هر کاربری از شبکه استفاده کند.
- مقاومت در برابر حمله‌های مختلف مطرح: طرح باید در برابر حمله‌های مطرح در شبکه اینترنت اشیاء نظامی مانند: حمله تکرار، حمله جعل امضا، حمله تغییر پیام، حمله منع خدمت و غیره مقاوم باشد.
- محرمانگی: اطلاعات حساس داخل پیام‌های ردوبدل شده نباید به‌صورت متن آشکار ارسال گردد و باید به‌صورت رمز شده ارسال شوند.

قصد داریم با استفاده از تسهیم راز کوانتومی میان لایه سنجش و لایه دسترسی احراز اصالتی دوطرفه انجام دهیم. بدین معنی که هرکدام از دولایه مطرح شده برای لایه دیگر احراز اصالت شود و کلیدی بین آن‌ها به اشتراک گذاشته شود. شبکه‌ای که در نظر می‌گیریم شامل تعدادی دستگاه جمع‌آوری اطلاعات

در لایه سنجش (مانند رادارها، زیردریایی‌ها، افزاره‌های RFID و حس‌گرها) و تعدادی دروازه در لایه دسترسی است. در این طرح از تسهیم راز کوانتومی درهم‌تنیده آستانه‌ای $(2,2)$ برای تبادل کلید امن استفاده می‌شود. این طرح شامل ۴ فاز است که عبارت‌اند از: ۱- فاز آماده‌سازی و احراز اصالت کلاسیک. ۲- فاز تبادل کلید امن با استفاده از تسهیم راز کوانتومی درهم‌تنیده. ۳- فاز انتقال پیام محرمانه. ۴- فاز به‌روزرسانی

۴-۳- فاز اول طرح جدید - فاز آماده‌سازی و احراز اصالت کلاسیک

ابتدا نهادی از گروه مدیران شبکه که می‌تواند هویتی از لایه کاربرد شبکه اینترنت اشیاء نظامی باشد را به‌عنوان مدیرگروه در نظر می‌گیریم. همان‌طور که در بخش ۴-۲-۱ اشاره کردیم مدیرگروه می‌تواند برحسب استانداردهای در نظر گرفته‌شده در طرح هویتی از لایه دسترسی نیز باشد. واضح است که اگر این مدیر از لایه کاربرد انتخاب شود امنیت بیشتری را خواهیم داشت. چرا که هویت‌های موجود در این لایه در واقع همان رهبران جنگ و از نهادهای بالادستی کشور هستند. در این فاز، J یک رشته بیت است که برای هر کدام از کاربران شبکه (در این طرح فرض می‌کنیم که در تمامی لایه‌های شبکه) به‌صورت منحصر به فرد و به‌صورت رشته‌ای از صفر و یک‌ها تعریف می‌شود و در ادامه بیان می‌کنیم که این مقدار در داخل محیط اجرایی امن[1] (TEE) تعبیه‌شده در تمامی کاربران شبکه بارگذاری می‌شود. این محیط اجرایی امن در برابر حملات فیزیکی و نرم‌افزاری بسیار مقاوم هستند. نیروهای نظامی به محتویات داخل TEE دسترسی ندارند. خواننده را برای مطالعه بیشتر در این مورد به [۴۸] ارجاع می‌دهیم. مدیر گروه وظایف زیر را در فاز اول طرح انجام می‌دهد:

- انتخاب Bبه‌عنوان گروه جمعی دوری با مرتبه l (B و l در TEE تمامی نیروهای نظامی بارگذاری می‌شود. مرتبه گروه B، l باید عدد اول بزرگی باشد.)
- مدیر تابع $f:\{0,1\}^{\text{با طول دلخواه}} \to Z_l^*$ را با توجه به l انتخاب می‌کند. $f(.)$ در TEE تمامی نیروهای نظامی بارگذاری می‌شود.
- Y را به‌عنوان مولد گروه B انتخاب می‌کند. Y در TEE تمامی نیروهای نظامی بارگذاری می‌شود.
- مقدار θ را به‌عنوان کلید خصوصی ارتباطات به‌صورت تصادفی از Z_l^* انتخاب می‌کند. θ در TEE تمامی نیروهای نظامی بارگذاری می‌شود.
- کلید عمومی ارتباطات، N را طبق معادله
- $N=\theta Y$ محاسبه می‌کند. N در TEE تمامی نیروهای نظامی بارگذاری می‌شود.
- تابع $s:\{0,1\}^{\text{با طول دلخواه}} \to \{0,1\}^{\text{با طول دلخواه}}$ را انتخاب می‌کند. $s(.)$ در TEE تمامی نیروهای نظامی بارگذاری می‌شود.

فرض می‌کنیم C نمایش یک خم بیضوی روی میدان متناهی اول F_y و y نمایش عدد اول بزرگ باشد. C توسط رابطه $z^2=k^3+qk+w$ تعریف می‌شود. در رابطه فوق $q,w\in F_y$می‌باشند. همچنین رابطه $\partial=4q^3+27w^2\neq 0$ در معادله فوق برقرار است [49].

فرض می‌کنیم Bیک گروه جمعی دوری با مرتبه l باشد. همچنین Y را به‌عنوان مولد گروه B در نظر می‌گیریم. گروه B شامل تمام نقاط روی منحنی بیضوی C به همراه نقطه O در بی‌نهایت است. ضرب اسکالر در منحنی بیضوی Cبه‌صورت (برای u بار) $uY=Y+\cdots+Y$ تعریف می‌شود. لازم به ذکر است که l عدد اول بزرگ است. در فاز اول طرح مرحله‌ای داریم که در آن کاربران اقدام به تولید کلید امضای خود و همچنین اقدام به گمنام‌سازی خود می‌کنند. در زیر نحوه درست کردن امضا و نحوه گمنام‌سازی کاربران را شرح می‌دهیم.

نحوه ایجاد کلید امضای کاربران و نحوه گمنام‌سازی کاربران لایه سنجش شبکه اینترنت اشیاء نظامی: هرکدام از کاربران لایه سنجش شبکه اینترنت اشیاء نظامی در این مرحله اقدام به گمنام‌سازی خود می‌کنند تا حریم خصوصی خود را هم در برابر شنودگران خارج از شبکه و هم در برابر کاربران داخل شبکه که با آن‌ها در ارتباط هستند حفظ کنند. توضیح دادیم که J_i هویت اصلی کاربر i است. برای گمنام‌سازی باید J_i پنهان شود. برای این‌کار این رشته‌ای از صفر و یک‌ها را با مقدار $s(g_iN)$ جمع می‌کنیم. در این رابطه g_i مقداری تصادفی از Z_l^* است که توسط محیط اجرایی امن مربوط به هر کاربر از شبکه انتخاب می‌شود. بنابراین، هویت کاربران تبدیل به هویت جدیدی که طبق رابطه $J_i'=s(g_iN)\oplus J_i$ به‌دست می‌آید می‌شود. در هر بار برقراری پیام یک g_i جدید به‌صورت تصادفی از Z_l^* انتخاب می‌شود. واضح است که با این کار کاربران دارای هویت‌های گمنام جدیدی در هر بار تبادل پیام خواهند شد که امنیت طرح را در برابر حمله آشکارسازی هویت کاربران مقاوم می‌کند. چراکه هر حمله نیازمند زمان و هزینه است و با این کار پیدا کردن J_i سخت‌تر می‌شود. حال باید سازوکاری را طراحی کنیم که به وسیله آن بتوانیم به J_i در واقع بروز خطا، جرم، اشتباه و غیره

[1] Trusted Execution Environment (TEE)

دست یابیم. به‌دلیل اهمیت حریم خصوصی این کار باید توسط مدیر گروه انجام شود. بنابراین، اقدام به طراحی مقدار $k_i = g_i Y$ می‌کنیم. با این مقدار و با کمک J_i' مدیر گروه قادر خواهد بود در مواقع لزوم به J_i دست یابد. جزئیات این اقدام در قسمت تحلیل امنیتی طرح در بخش ۴-۷ آورده شده است. همان‌طور که در شکل (۳) مشاهده می‌شود هویت اصلی کاربر به‌واسطه XOR شدن مخفی شد. دلیل این نحوه محاسبه هویت گمنام در قسمت تحلیل امنیتی شرح داده شده است. سپس مقدار W_i توسط نیروی نظامی iام محاسبه می‌شود. در این مرحله کاربر iام از لایه سنجش شبکه اینترنت اشیاء نظامی مقدار تصادفی v_i را از Z_l^* انتخاب و مقدار $v_i Y$ را به‌دست می‌آورد که آن را W_i می‌نامیم. بنابراین، داریم: $W_i = v_i Y$. این کاربر مقدار خروجی تابع $s(.)$ را به ازای ورودی‌های $s(g_i N) \oplus J_i$، k_i، T_i، W_i و پیام درخواست احراز اصالت (P_i) که از اهمیت خاصی برای حفظ محرمانگی برخوردار نیست را محاسبه می‌کند. یعنی داریم:

$$s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) \bmod l$$

سپس با استفاده از مقادیر g_i، θ و v_i نیروی نظامی iام اقدام به محاسبه a_i در پیمانه l مطابق رابطه زیر می‌کند.

$$a_i \equiv \theta s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) + g_i + v_i \bmod l$$

a_i کلید خصوصی متناظر با هویت گمنام نیروی نظامی iام محسوب می‌شود.

نحوه ایجاد امضای دیجیتال کاربران شبکه اینترنت اشیاء نظامی: هدف از ایجاد امضا تأمین نیاز به احراز اصالت کاربر توسط لایه دسترسی می‌باشد. در این مرحله امضا توسط کاربر موجود در لایه سنجش تولید می‌شود. وارسی طرح امضای جدید شناسه مبنای ارائه‌شده بدون نیاز به زوج نگار دوخطی است. در نتیجه، فرایند وارسی با سربار محاسباتی و مخابراتی پایین‌تری نسبت به امضاهای دیگر، و البته با سطح امنیت بیشتر انجام می‌پذیرد. در رابطه با امنیت این طرح امضا در قسمت تحلیل امنیتی طرح در بخش ۴-۷ صحبت کرده‌ایم. این طرح امضا دارای امنیت بسیار بالایی در برابر بسیاری از حملات مطرح در شبکه‌های توزیع یافته است. نیروی نظامی iام از لایه سنجش مقدار f_i را محاسبه می‌کند که برابر است با $f(s(g_i N) \oplus J_i)$. بنابراین، داریم:

$f_i \equiv f(s(g_i N) \oplus J_i) \bmod l$ سپس مقدار v_i f_i را محاسبه می‌کند و در پیمانه l با مقدار a_iجمع می‌کند. داریم:

$$\mu_i \equiv v_i f_i + \theta s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) + g_i + v_i \bmod l$$
$$\equiv v_i (f_i + 1) + \theta s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) + g_i \bmod l$$

نیروی نظامی iام مقدار $(P_i, T_i, (s(g_i N) \oplus J_i), k_i, W_i, \mu_i)$را که با τ_i نشان می‌دهیم به‌کاربر لایه دسترسی مطابق شکل (۳) ارسال می‌کند. $\tau_i = (P_i, T_i, (s(g_i N) \oplus J_i), k_i, W_i, \mu_i)$

محتویات τ_i را در زیر جمع‌بندی می‌کنیم:

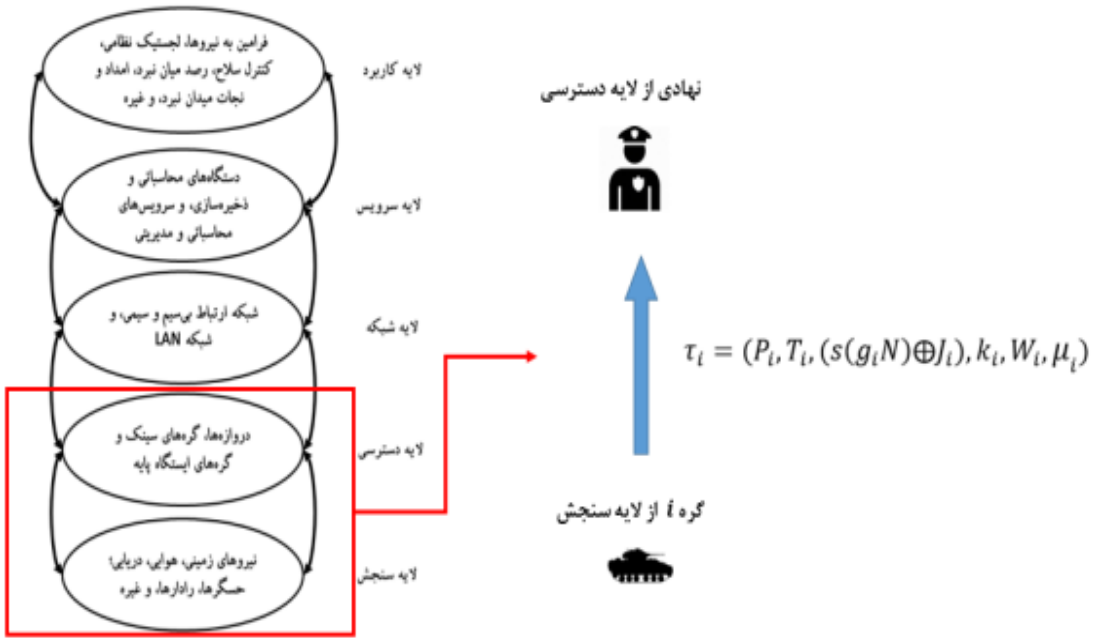
- P_i پیام است. واضح است که پیام P_i از اهمیت امنیتی برخوردار نیست. یعنی لازم نیست که آن را رمزگذاری کنیم. چراکه محتوی آن اطلاعات حساس و امنیتی نیست و هدف از تولید آن صرفاً انجام امضا بر روی آن است تا در طرف مقابل احراز اصالت انجام بپذیرد. بنابراین، این پیام را بدون رمزگذاری ارسال می‌کنیم.
- $s(g_i N) \oplus J_i$ هویت گمنام نیروی نظامی iام شبکه است. که مقدار g_i در عبارت k_i دخیل شده است.
- T_i مهر زمانی است. دلیل استفاده از این پارامتر در قسمت تحلیل امنیتی در بخش ۴-۷ اشاره شده است. محیط اجرایی امن موجود در هر کاربر به‌راحتی می‌توانند مهرهای زمانی مربوطه را تولید کنند. تولید مهر زمانی بسیار راحت است و در مقاله‌های بی‌شماری روش‌های تولید آن ذکر شده است.
- W_i مقدار تصادفی عضوی از گروه جمعی B است. طبق نحوه محاسبه W_i که در زیر مجدداً آورده شده است، W_i تابع مقدار تصادفی v_i عضو Z_l^* است. در واقع، Y مولد گروه جمعی B را به تعداد v_i بار باهم جمع می‌کنیم تا W_i طبق رابطه $W_i = v_i Y$ حاصل شود.
- μ_i امضا شناسه مبنا است. دلیل شناسه مبنا بودن این امضا هم در دل آن و هم در ظاهر آن نهفته است. برای μ_i داریم:

$$\mu_i \equiv v_i f_i + \theta s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) + g_i + v_i \bmod l$$
$$\equiv v_i (f_i + 1) + \theta s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) + g_i \bmod l$$

با جایگذاری f_i در رابطه μ_i داریم:

$$\mu_i \equiv v_i (f(s(g_i N) \oplus \boldsymbol{J_i}) + 1 + \theta s(T_i, W_i, P_i, (s(g_i N) \oplus \boldsymbol{J_i}), k_i) + g_i \bmod l$$

همان‌طور که در رابطه با بعد از جایگذاری‌های لازم مشاهده می‌شود (البته قبل از جایگذاری نیز تا حدی مشخص بود)، این امضا در دل خود شناسه هر کاربر را دارد، که همان J_i است. دلیل این امر نیاز امنیتی به عدم انکار است (همان انکارناپذیری). مجدداً برای توضیحات بیشتر در این مورد به بخش ۴-۷ مراجعه شود.



شکل (۳): ارسال امضای دیجیتال نیروی نظامی برای احراز اصالت به لایه دسترسی شبکه اینترنت اشیاء نظامی.

اطمینان از اصالت کاربران در شبکه اینترنت اشیاء نظامی در مرحله اول تبادل اطلاعات

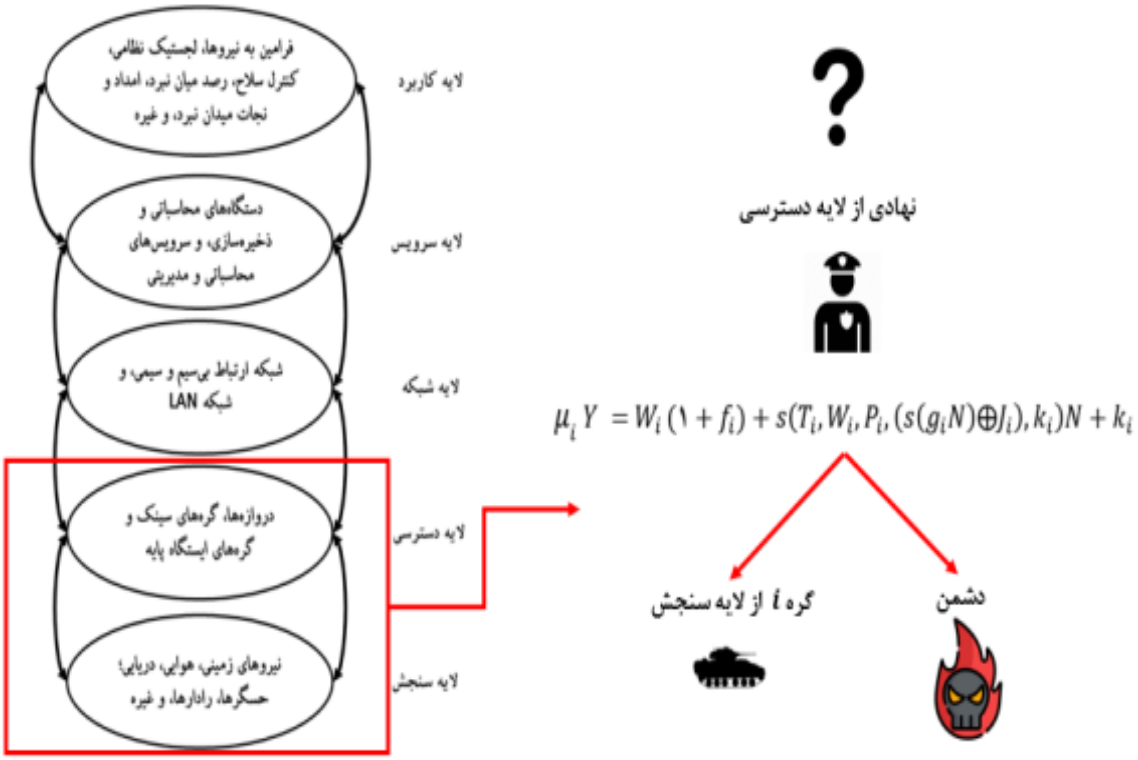
در این مرحله احراز اصالت کلاسیک را شرح می‌دهیم. لازم به ذکر است که این مرحله قبل از احراز اصالت و حفظ محرمانگی توسط تسهیم راز کوانتومی انجام می‌پذیرد. بعد از این‌که عضوی از لایه دسترسی شبکه است پیام

$$\tau_i = (P_i, T_i, (s(g_i N) \oplus J_i), k_i, W_i, \mu_i)$$

را دریافت کرد، برای وارسی این پیام به‌صورت زیر عمل می‌کند: قبل از هر چیز باید از تازگی مهر زمانی T_i اطمینان حاصل کند. سپس معتبر بودن هویت گمنام در بازه زمانی تعیین‌شده را بررسی کند (این بازه از قبل تعریف شده است) و در صورت معتبر بودن، عضو لایه دسترسی مقادیر $P_i, T_i, (s(g_i N) \oplus J_i), k_i, W_i, \mu_i$ را از τ_i دریافتی استخراج می‌کند. با استفاده از این مقادیر f_i را طبق رابطه زیر محاسبه می‌کند: $f_i \equiv f(s(g_i N) \oplus J_i) \bmod l$ و $s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) \bmod l$. حال گیرنده مقادیر زیر را دست دارد: μ_i (دریافت شده است.). W_i (دریافت شده است.). k_i (دریافت شده است.). f_i (با استفاده از مقادیر دریافتی محاسبه شده است.). $s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) \bmod l$ (با استفاده از مقادیر دریافتی محاسبه شده است.). N (کلید عمومی سامانه است.). Y (کلید عمومی سامانه است.). در نتیجه به‌راحتی می‌تواند صحت رابطه‌ای که در ادامه آورده شده را بررسی کند. ابتدا Y را برای μ_i بار با خودش جمع می‌کند. سپس W_i را $f_i + 1$ بار با خودش جمع می‌کند. همچنین N را $s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i)$ بار با خودش جمع می‌کند. در نهایت درستی یا برقراری رابطه زیر را بررسی می‌کند.

$$\mu_i Y = W_i (1 + f_i) + s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) N + k_i$$

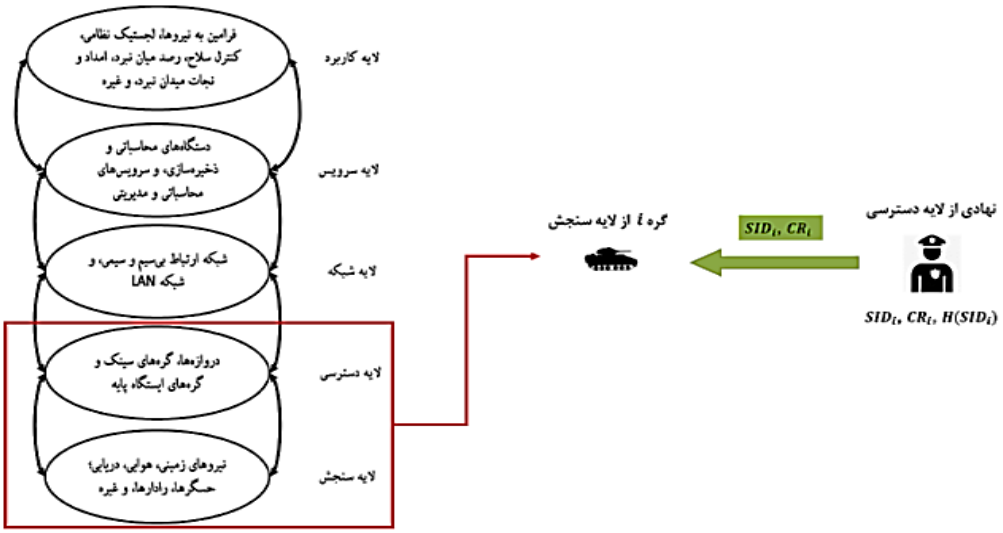
اگر رابطه فوق برقرار بود امضای دریافت شده معتبر می‌باشد و در نتیجه نیروی نظامی iام از لایه سنجش برای کاربر لایه دسترسی احراز اصالت می‌شود. دلیل این امر به اثبات صحت رابطه فوق بر می‌گردد که در قسمت تحلیل امنیتی طرح در بخش ۴-۷ آمده است. همانطور که در شکل (۴) ملاحظه می شود، کاملاً واضح است که تمام مراحل بالا می‌تواند از جانب نیروی نظامی iام نیز با هدف احراز اصالت کاربر لایه دسترسی به طریق مشابه انجام بپذیرد که برای اجتناب از تکرار، از نوشتن دوباره مراحل برای طرف دیگر احراز اصالت با اندیس‌های متفاوت اجتناب کردیم.



شکل (۴): محرز شدن اصالت نیروی نظامی iام از لایه سنجش برای کاربر لایه دسترسی در شبکه اینترنت اشیاء نظامی

۴-۴- فاز دوم طرح جدید - فاز تبادل کلید امن با استفاده از تسهیم راز کوانتومی درهم‌تنیده

لازم به ذکر است، همان‌طور که در بخش مقدمه اشاره شد استفاده طولانی مدت از رمزنگاری کلید عمومی در شبکه‌ای مانند شبکه اینترنت اشیاء نظامی که برآورده کردن نیازمندی‌های امنیتی اهمیت دوچندان دارد، منطقی به نظر نمی‌رسد. چرا که، با پیشرفت روزافزون فناوری‌های کوانتومی احتمال شکستن سامانه‌های مبتنی بر سختی تجزیه عدد و سختی حل مسئله لگاریتم گسسته روزبه‌روز افزایش می‌یابد. بعد از اینکه کاربر امiلایه سنجش با هویت گمنام مربوط به خود به‌واسطه فرآیند احراز اصالت کلاسیک اشاره‌شده در فاز اول، مورد تأیید کاربر لایه دسترسی قرار گرفت، برای ادامه، به طریق زیر عمل می‌کنیم. در این مرحله، همانطور که در شکل (۵) قابل مشاهده است، با استفاده از تسهیم راز کوانتومی حالت‌های درهم‌تنیده معرفی‌شده در بخش ۳-۱، کاربر لایه دسترسی برای ثبت‌نام هر دستگاه از لایه سنجش با استفاده از کانال کوانتومی یک شناسه به‌صورت SID_i و یک گواهی به‌صورت CR_i در اختیار دستگاه لایه سنجش قرار می‌دهد. برای این منظور کاربر لایه دسترسی هر دو مقدار شناسه و گواهی رو به‌صورت مقادیر ۲۵۶ بیتی تصادفی در نظر می‌گیرد و با کنار هم قرار دادن آن‌ها یک مقدار ۵۱۲ بیتی تصادفی ایجاد می‌کند. حال لازم است این مقدار ۵۱۲ بیتی تصادفی را از طریق کانال امن در اختیار دستگاه لایه سنجش قرار دهد. برای این منظور می‌تواند از روش توزیع کلید کوانتومی (به‌عنوان مثال، BB84) یا تسهیم راز کوانتومی درهم‌تنیده آستانه‌ای (2, 2) استفاده کند. همان‌طور که اشاره شد، تسهیم راز کوانتومی درهم‌تنیده آستانه‌ای (2, 2) امکان اشتراک کلید را با رفت‌وبرگشت کم نسبت به طرح توزیع کلید کوانتومی فراهم می‌کند. برای استفاده از طرح تسهیم راز کوانتومی درهم‌تنیده آستانه‌ای (2, 2) لازم است که کاربر لایه دسترسی هر دو قسمت را برای بازیابی راز (مقدار ۵۱۲ بیتی تصادفی مربوط به شناسه و گواهی در کنار هم) برای یک دستگاه مشخص لایه سنجش به‌صورت کوانتومی مطابق با آنچه در قسمت طرح تسهیم راز با استفاده از حالت‌های درهم‌تنیده توضیح داده شد ارسال کند. دستگاه لایه سنجش پس از دریافت پیام با اندازه‌گیری کوانتومی و بازیابی راز به مقدار ۵۱۲ بیتی دست می‌یابد که ۲۵۶ بیت اول را به‌عنوان شناسه خود و ۲۵۶ بیت دوم را به‌عنوان گواهی خود در نظر می‌گیرد. حال کارگزار لایه دسترسی و دستگاه لایه سنجش چکیده گواهی را با استفاده از تابع چکیده‌ساز که اعلام عمومی شده است، محاسبه و در حافظه خود ذخیره می‌کنند.



شکل (۵): احراز اصالت در طرح جدید - فاز دوم - تبادل کلید امن با استفاده از تسهیم راز کوانتومی درهم‌تنیده

به‌این‌ترتیب دستگاه لایه سنجش دارای سه مقدار $H(SID_i)$، SID_i و CR_i خواهد بود که این مقادیر در لایه دسترسی نیز متناظر با هر دستگاه از لایه سنجش موجود هستند. منظور از متناظر با هر دستگاه این است که به ازای دستگاه iام مقدار CR_i و SID_i به‌صورت مشخص در لایه دسترسی ثبت می‌شود و همین‌طور برای کاربر مثلاً kام مقدار CR_k و SID_k به‌صورت مشخص در لایه دسترسی ثبت می‌شود. لازم به ذکر است که برای اینکه شبکه دچار حمله نشود، می‌توان پارامتری تصادفی را در بخش احراز اصالت کلاسیک در نظر گرفت (توسط هر نهاد یک پارامتر تصادفی تولید شود) و در پیام‌های تبادلی این بخش از آن استفاده کرد (در پیام‌های این بخش ضمیمه شود). این کار برای این است که از تغییر هویت نهاد مقابل بعد از احراز اصالت جلوگیری شود.

۴-۵- فاز سوم طرح جدید - فاز انتقال پیام محرمانه

در این مرحله پس از تبادل سه مقدار $H(SID_i)$، SID_i و CR_i نوبت به انتقال پیام امن می‌رسد. قبل از تبادل پیام امن به‌منظور افزایش امنیت یک‌بار دیگر با استفاده از این سه مقدار احراز اصالت انجام می‌گیرد. دلیل این امر است که احتمال دارد بعد از احراز اصالت کلاسیکی که در ابتدا صورت گرفت هویت جعلی جای هویت اصلی را بگیرد و در واقع شاهد حمله در شبکه باشیم. در اینجا دروازه موجود در لایه دسترسی که فرض می‌کنیم کاربر jام است که به اطلاعات هر کدام از دستگاه‌های سنجش نیازمند است (به‌طور مثال دستگاه یا کاربر i ام)، شناسه، چکیده شناسه و گواهی دستگاه موردنظر را مطابق رابطه زیر به‌کار می‌گیرد تا پیام A_1 را تولید کند. در رابطه با عملگر $Enc_{key}(plaintext)$ به این توضیح بسنده می‌کنیم که می‌توان الگوریتم‌های رمزنگاری‌های مختلفی را متناسب با هزینه و امنیتی که دارند انتخاب کرد. منظور از $plaintext$ همان داده‌ای است که می‌خواهیم آن را رمز کنیم و key کلید رمزنگاری ما است. $A_1 = Enc_{CR_i}(H(SID_i), N_1, T_1)$ دروازه لایه دسترسی با توجه به مهر زمانی زمان حاضر که T_1 است، یک مقدار تصادفی N_1، انتخاب می‌کند و مقادیر مهر زمانی، چکیده شناسه و مقدار تصادفی را با گواهی دستگاه به‌صورت $Enc_{CR_i}(H(SID_i), N_1, T_1)$ رمز می‌کند و پیام $M_1 = (A_1, T_1)$ را برای دستگاه لایه سنجش ارسال می‌کند. مقدار تصادفی N_1 برای به‌روزرسانی شناسه و گواهی دستگاه به‌کار می‌رود، در صورتی که این مقدار توسط لایه دسترسی ارسال شود به آن معناست که در پایان فاز احراز اصالت گواهی و شناسه دستگاه به‌روز خواهد شد و در غیر این صورت نیاز به به‌روزرسانی نخواهد بود. این به‌روز رسانی بر اساس نیاز امنیتی هر چند وقت یک‌بار می‌تواند صورت بگیرد. دستگاه موجود در لایه سنجش به محض دریافت پیام M_1، مهر زمانی T_1 را بررسی می‌کند. در صورتی که مهر زمانی T_1 فاصله اندکی با مهر زمانی حاضر داشته باشد، آن را می‌پذیرد و در غیر این صورت آن را رد می‌کند. این فاصله اندک از قبل قابل تعریف است. حال دستگاه با گواهی خود A_1 را رمزگشایی می‌کند و مهر زمانی داخل آن را با مهر زمانی دریافت‌شده مقایسه می‌کند، در صورت برابری پیام را می‌پذیرد و در غیر این صورت آن را رد می‌کند. حال اگر چکیده شناسه SID_i رمزگشایی‌شده با چکیده شناسه دستگاه یکسان باشد، لایه دسترسی برای دستگاه لایه سنجش احراز اصالت می‌شود، زیرا چکیده شناسه دستگاه تنها در اختیار کارگزار اصلی است و این مقدار شناسه از طریق کانال کوانتومی میان آن‌ها توافق شده است و نهاد دیگری از آن آگاه نیست. لازم به ذکر است که اگر شنودی در طول مسیر انجام شود به‌دلیل ویژگی اندازه‌گیری کوانتومی قابل تشخیص خواهد

بود. دستگاه لایه سنجش اطلاعات P_i را با توجه به مأموریت خود از محیط نظامی اطراف جمع‌آوری کرده است و آماده ارسال این اطلاعات به لایه بالای شبکه است. دستگاه لایه سنجش مهر زمانی تازه یعنی T_2، شناسه خود، اطلاعات P_i و مقدار تصادفی را با گواهی خود به‌صورت $A_2 = Enc_{CR_i}(SID_i, P_i, N_1, T_2)$ رمز می‌کند و پیام $M_2 = (A_2, H(SID_i), T_2)$

$$M_2 = \left(Enc_{CR_i}(SID_i, P_i, N_1, T_2), H(SID_i), T_2\right)$$

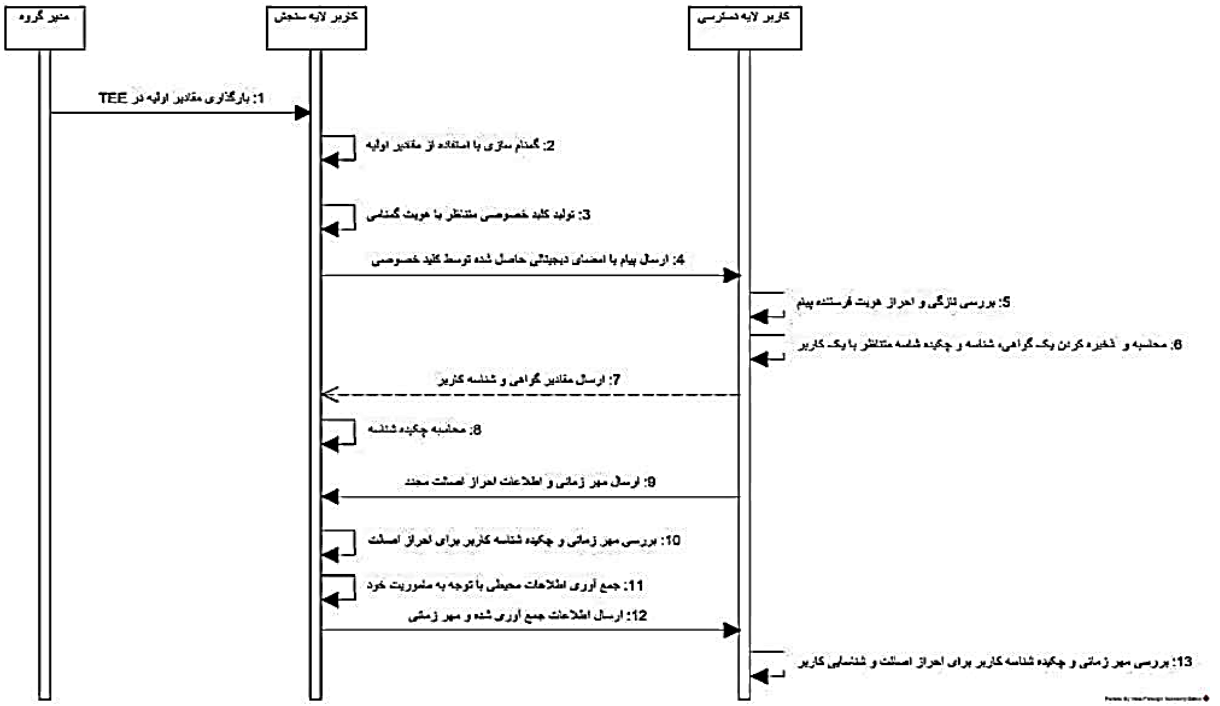
را برای دروازه ارسال می‌کند. دروازه به‌محض دریافت پیام M_2، مهر زمانی T_2 را بررسی می‌کند. در صورتی که مهر زمانی T_2 فاصله اندکی با مهر زمانی حاضر داشته باشد، آن را می‌پذیرد و در غیر صورت آن را رد می‌کند. حال دروازه با توجه به مقدار $H(SID_i)$ متوجه می‌شود که پیام از طرف کدام دستگاه لایه سنجش ارسال شده است و با گواهی متناظر با آن A_2 را رمزگشایی می‌کند. در ادامه دروازه مهر زمانی داخل آن را با مهر زمانی دریافت‌شده مقایسه می‌کند، در صورت برابری پیام را می‌پذیرد و در غیر این صورت آن را رد می‌کند. حال اگر شناسه SID_i رمزگشایی‌شده با شناسه موجود در حافظه لایه دسترسی یکسان باشد، دستگاه لایه سنجش برای دروازه احراز اصالت می‌شود، زیرا شناسه دستگاه تنها در اختیار کارگزار اصلی است و این مقدار شناسه از طریق کانال کوانتومی میان آن‌ها توافق شده است و از طرف دیگر نهاد دیگری از آن آگاه نیست. با تأیید احراز اصالت دستگاه اطلاعات رمزگشایی‌شده P_i تأیید می‌شود و این اطلاعات برای استفاده و تجزیه‌وتحلیل در اختیار لایه‌های بالاتر قرار می‌گیرد.

۴-۶- فاز چهارم طرح جدید - فاز به‌روزرسانی

این فاز در صورتی وجود خواهد داشت که مقدار تصادفی N_1 توسط دروازه ارسال شده باشد. بدین منظور پس از پایان فاز احراز اصالت دستگاه لایه سنجش و دروازه مقادیر شناسه و گواهی را به‌صورت زیر به‌روزرسانی می‌کنند و در حافظه خود ذخیره می‌کنند.

$$SID_i^{new} = H(SID_i \parallel N_1) \text{ و } CR_i^{new} = H(CR_i \parallel N_1)$$

همان‌طور که اشاره شد در این طرح نیاز به کانال امن از بین رفت و ارسال اطلاعات اولیه برای برقراری کلید با استفاده از کانال کوانتومی و تسهیم راز کوانتومی صورت گرفت. بدین‌صورت هزینه استفاده از کانال کوانتومی به شدت کاهش یافت، زیرا در این حالت برای هر دستگاه لایه سنجش فقط یک‌بار از کانال کوانتومی استفاده می‌شود و نیاز به کانال کوانتومی در فاز بعدی که مربوط به احراز اصالت مجدد برای انتقال پیام محرمانه است به‌طور کامل از بین می‌رود. به‌منظور روشن شدن روش پیشنهادی، دیاگرام توالی برای تمامی مراحل روش پیشنهادی در شکل (۶) به تفسیر رسم شده است.



شکل (۶): دیاگرام توالی[1] طرح پیشنهادی.

[1] sequence diagram

۴-۷- تحلیل امنیتی طرح جدید

در این قسمت به تحلیل امنیتی طرح ارائه‌شده در راستای ارضا نیازمندی‌های امنیتی مهم در شبکه اینترنت اشیاء نظامی می‌پردازیم. لازم به ذکر است که در این قسمت اثبات امنیتی در مدل مبتنی بر بازی[1] یا چهارچوب ترکیب جهانی[2] ارائه نشده است. تحلیل امنیتی این قسمت بر مبنای شهود اثبات امنیت در مدل مبتنی بر بازی در اورال تصادفی[3] می‌باشد. در واقع امنیت در قسمت مثلاً حفظ حریم خصوصی بر مبنای سختی مسئله ریاضی است. کاهش[4] که در اثبات امنیتی رسمی ارائه می‌شود بر مبنای سختی حل مسئله است که اثبات می‌شود اگر مهاجمی کارا وجود داشته باشد که بتواند امنیت را نقض کند (مثلاً تمایز قائل شود بین مقدار خروجی سامانه و مقداری تصادفی) در نتیجه مسئله سخت ما که امنیت سامانه مبتنی بر آن است حل خواهد شد. طبق این منطق ریاضی: "عکس نقیض گزاره ارزشی برابر با خود گزاره دارد"، از آن جهت که این مسئله سخت حل نمی‌شود بنابراین، مهاجمی نیز وجود نخواهد داشت؛ بنابراین، امنیت موردنظر اثبات می‌شود. در ادامه به تحلیل امنیتی طرح جدید برای برآورده کردن نیازمندی‌های شبکه اینترنت اشیاء نظامی می‌پردازیم.

- احراز اصالت: احراز اصالت یکی از نیازمندی‌های مهم در شبکه‌های اینترنت اشیاء نظامی است. در اینترنت اشیاء نظامی منبع ارسالی پیام باید یک منبع مجاز باشد، یعنی هویت ارسال‌کننده اطلاعات باید برای دریافت‌کننده به‌صورت صحیح مشخص شود و فرستنده نتواند خود را به‌عنوان نهاد دیگری به دریافت‌کننده نشان بدهد. در طرح معرفی‌شده توسط این پژوهش احراز اصالتی دوطرفه میان لایه سنجش و لایه دسترسی برقرار می‌شود. به‌طوری‌که هر دو نهاد می‌توانند هویت نهاد دیگر را تأیید یا رد کنند. پس در این طرح‌ها امکان حمله جعل و حمله مرد میانی[5] وجود نخواهد داشت و نهادهای دیگر امکان جعل هویت خود و جا زدن به‌عنوان یک نهاد مجاز را نخواهند داشت. پیام‌های ارسالی توسط نیروهای نظامی لایه سنجش در طول ارتباط با لایه دسترسی باید احراز اصالت بشوند تا از اینکه بدون تغییر و توسط فرد معتبر ارسال شده‌اند، مطمئن شد. در طرح احراز اصالت ارائه‌شده، امضای شناسه مبنایی که برای وارسی بدون زوج‌نگار دوخطی است به جهت بررسی اصالت پیام‌های دریافتی مورد استفاده قرار گرفت. زوج نگار دو خطی عملگری زمان‌بر است و عدم استفاده از آن باعث افزایش کارایی می‌شود. در ادامه به بررسی صحت رابطه وارسی امضا می‌پردازیم. صحت رابطه وارسی امضا از طریق زیر به‌دست می‌آید:

$$\mu_i \equiv v_i(f_i+1) + \theta s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) + g_i \bmod l$$

$$\mu_i Y = v_i(f_i+1)Y + \theta s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i)Y + g_i Y$$
$$= v_i f_i Y + v_i Y + \theta Y s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) + g_i Y$$
$$= f_i W_i + W_i + s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) N + k_i$$
$$= W_i (1+f_i) + s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) N + k_i$$

در مقاله‌های [۳۱-۲۳ و ۲۱-۱۹] نیاز به احراز اصالت تأمین نمی‌شود و یا به‌صورت محدود برآورده می‌شود. منظور از واژه به‌صورت محدود این است که امضاهای دیجیتال مورد استفاده به اندازه کافی از تصادفی‌بودن برخوردار نیستند. همچنین، مقادیر مجهول در دست مهاجم برای جعل کردن امضا از تعداد بالایی برخوردار نیست و در نتیجه هزینه حمله جعل هویت (جعل امضا) برای مهاجم کاهش می‌یابد چرا که مجبور به گشتن در فضای گسترده‌ای نیست. در مقاله [۲۲] احراز اصالت برآورده می‌شود، اما حفظ حریم خصوصی به‌صورت کامل و مشابه آنچه در این طرح به‌صورت جامع ارائه شد برآورده نمی‌شود. در مقاله [۱۳] که در سال ۲۰۱۹ چاپ شده است، مقاومت در برابر حمله شنود وجود دارد و احراز اصالت نیز برقرار می‌شود. اما، حریم خصوصی حفظ نمی‌شود.

- مجاز شناسی: مجاز شناسی یکی از نیازهای مهم در شبکه اینترنت اشیاء نظامی است. در شبکه‌های اینترنت اشیاء نظامی نهادهای غیرمجاز نباید امکان ورود به شبکه و دسترسی به اطلاعات را داشته باشند که با طرح احراز اصالت دوطرفه این امکان به‌طور کامل از بین رفته است. لازم به ذکر است مجاز شناسی همان احراز اصالت است منتها در مقاله‌های مختلف داخلی با واژه‌های مختلفی از این مفهوم نام‌برده می‌شود.
- انکارناپذیری: انکارناپذیری به معنی عدم توانایی انکار ارسال پیامی مشخص توسط هویتی مشخص در زمانی مشخص است. با توجه به اینکه هویت واقعی هر نیروی نظامی J_i مطابق آنچه با جزئیات ذکر شد، در امضای آن‌ها دخیل شده است، امکان انکار ارسال درخواست احراز اصالت وجود ندارد. همچنین، با توجه به اینکه قبل از تسهیم راز کوانتومی اصالت طرفین محرز شده است، پیامی که از نیروی نظامی ام i به‌صورت رمزشده به لایه بالاتر به مدیر گروه موجود در لایه دسترسی ارسال می‌شود، غیرقابل انکار توسط آن هویت است چراکه با کلیدی رمز شده است که تنها در اختیار همان کاربر در سطح لایه اول شبکه است. با توجه به اینکه این کلیدی متقارن است و در اختیار کاربر لایه دسترسی هم هست، می‌توان در این مرحله

[1] game based security proofs
[2] Universal Composibility Framework
[3] random oracle
[4] reduction
[5] man in the middle attack

نیز برای به‌دست آوردن انکارناپذیری برای کل شبکه، از امضای جدید کلید عمومی مبنا معرفی‌شده بعد از تسهیم راز کوانتومی استفاده کرد.

- یکپارچگی داده: در اینترنت اشیاء نظامی لازم است که داده‌ها و اطلاعات ارسالی از فرستنده تا گیرنده بدون تغییر ارسال شود، یعنی یک نهاد خرابکار نتواند اطلاعات ارسالی را دچار تغییر کند. در مرحله احراز اصالت کلاسیک به‌دلیل وجود امضا روی پیام (که به‌دلیل هدف ما برای احراز اصالت صرفاً دارای محتوای درخواست احراز اصالت است) امکان تغییر محتوا وجود ندارد. در طرح ما با استفاده از کلید مخفی امکان تغییر اطلاعات وجود نخواهد داشت. زیرا حمله‌کننده برای تغییر اطلاعات نیاز به کلید مخفی به اشتراک گذاشته دارد و هرگونه تغییر در پیام توسط دشمن باعث می‌شود، دروازه به تغییر اطلاعات پی ببرد یا اینکه احراز اصالت را مردود کند. در مقاله های حوزه امنیت معمولاً هدف از احراز اصالت بر دو گونه است. مورد اول محرز شدن اصالت هویت ارسال‌کننده پیام و مورد دوم محرز شدن اصالت پیام دریافتی که در طول مسیر دستخوش تغییر نشده باشد. از مفهوم دوم به یکپارچگی نیز یاد می‌شود. برای مقایسه طرح پیشنهادی با سایر طرح‌ها در مورد یکپارچگی به بخش تحلیل امنیتی احراز اصالت رجوع شود.
- محرمانگی: هدف از محرمانگی ایمن ماندن اطلاعات از شنود توسط نهادهای خراب‌کار و یا دشمن است. در طرح ارائه‌شده ارسال اطلاعات جمع‌آوری‌شده توسط کاربر موجود در لایه سنجش به‌صورت رمز شده $Enc_{CR_i}(SID_i, P_i, N_1, T_2)$ و با کلید مخفی صورت می‌گیرد که محرمانگی اطلاعات را تأمین می‌کند. محرمانگی در اکثر مقاله‌های حوزه امنیت اینترنت اشیاء و اینترنت اشیاء نظامی برآورده شده است.
- تازه بودن داده، جلوگیری از حمله تکرار و حمله منع خدمت: استفاده از مهر زمانی باعث می‌شود که نهادهای خراب‌کار و یا دشمن نتوانند اطلاعات قدیمی را بر روی شبکه ارسال کنند، پس بدین‌صورت تازه بودن داده‌ها فراهم می‌شود و امکان حمله تکرار و حمله منع خدمت‌دهی از بین می‌رود. در حمله تکرار یک نهاد خراب‌کار پیام‌های معتبری را تولید می‌کند یا از ارتباطات قبلی میان نهادهای مجاز پیام‌هایی را به‌دست می‌آورد و برای یکی از نهادها ارسال می‌کند. ازآنجاکه این پیام معتبر است، نهاد موردنظر درگیر پردازش این پیام می‌شود و شروع به برقراری ارتباط با دشمن می‌کند. به این نوع حمله، حمله تکرار گفته می‌شود. اگر تعداد حمله‌های تکرار افزایش یابد، به‌طوری‌که نهاد موردنظر نتواند پاسخگوی ارتباطات دیگر خود شود، اصطلاحاً گفته می‌شود، آن نهاد دچار حمله منع خدمت‌دهی شده است. در طرح ارائه‌شده با استفاده از مهرهای زمانی و مقادیر مخفی امکان این حملات به‌طور کامل از بین رفته است. در مقاله‌های [۴۵-۴۱] تازگی حفظ نشده است و در نتیجه این مقاله‌های در برابر حمله تکرار آسیب‌پذیر هستند. اما، مقاله [۱۵] در برابر حمله تکرار به خاطر حفظ تازگی مقاوم است. اما، این مقاله در برابر حمله جعل مقاوم نیست چراکه از سازوکار کافی برای احراز اصالت برخوردار نیست. همچنین، مقاله [۱۵] در برابر حمله استراق سمع نیز مقاوم نیست. این در حالی است که طرح پیشنهادی در برابر حمله‌های ذکر شده مقاوم است. در [۱۸-۱۶] تازگی حفظ شده است، اما، به‌دلیل احراز اصالت ناکافی این طرح‌ها در برابر حمله جعل آسیب‌پذیر هستند. مقاله [۱۴] که در سال ۲۰۱۹ منتشر شده است، در برابر حمله جعل هویت مقاوم است اما، در برابر حمله منع خدمت مقاوم نیست. مقاله [۱۳] (منتشرشده در سال ۲۰۱۹)، در برابر حمله تکرار مقاوم است، اما همان‌طور که ذکر شد در این مقاله حریم خصوصی حفظ نمی‌شود.
- گمنامی و گمنامی مشروط (حفظ حریم خصوصی): در اینترنت اشیاء نظامی لازم است که شناسه منبع ارسالی پیام یا همان هویت اصلی ارسال‌کننده پیام از دید نهادهای دیگر حفظ شود. در طرح ارائه‌شده هرگز شناسه دستگاه ارسال‌کننده بر روی کانال به‌صورت آزاد ارسال نمی‌شود. در احراز اصالت مرحله اول، کاربران از هویت گمنام استفاده می‌کنند. کاربران هویت اصلی خود J_i را تبدیل به هویت گمنام J_i' کرده و سپس با استفاده از هویت گمنام اقدام به احراز اصالت می‌کنند، همچنین با هویت گمنام، مورد احراز اصالت شدن واقع می‌شوند. در طرح معرفی‌شده هر کاربر در یک بازه زمانی مشخص دارای مقدار g_iY است که این مقدار با J_i' ارتباط دارد. در ادامه دلیل استفاده از g_iY نوشته شده است. با توجه مسئله CDH (مسئله CDH: فرض می‌کنیم Y مولد گروه B و $r, t \in_r Z_l^*$ باشد. ($\in_r$ به معنی انتخاب تصادفی می‌باشد.) نقاط $R = rY \in B$ و $T = tY \in B$ به ازای مقادیر مجهول r و t داده شده‌اند، مسئله CDH محاسبه $rtY \in B$ است که جزو مسائل سخت است.) امکان به‌دست آورن هویت اصلی کاربران J_i برای مهاجم منوط به حل مسئله CDH می‌باشد، چراکه مهاجم به k_i که برابر با g_iY است و همچنین به N که برابر با θY است دسترسی دارد. بنابراین محاسبه θg_iY (که برای به‌دست آوردن J_i از روی J_i' نیاز است) منوط به حل مسئله CDH می‌باشد. در مواقع مورد نیاز باید قابلیت به‌دست آوردن هویت اصلی کاربران از روی هویت گمنام وجود داشته باشد. در طرح احراز اصالت معرفی شده مدیر گروه تنها نهادی است که می‌تواند هویت اصلی کاربران را از روی هویت گمنام آن‌ها J_i' به‌دست آورد. برای این کار مدیر گروه با استفاده از کلید خصوصی سامانه θ و با استفاده از $k_i = g_iY$ مقدار θg_iY و سپس $s(\theta g_iY)$ را محاسبه می‌کند، سپس طبق رابطه زیر به

هویت اصلی کاربر J_i پی می‌برد:

$$J_i' \oplus s(\theta g_i Y) = J_i' \oplus s(g_i(\theta Y)) \\ = J_i' \oplus s(g_i N) = \{J_i \oplus s(g_i N)\} \oplus s(g_i N) = J_i$$

و در مرحله دوم احراز اصالت نیز تنها چکیده شناسه‌های آن‌ها ارسال می‌شود که ارتباطی با هویت اصلی آن‌ها از نظر ریاضی ندارد. ارزشمند است که اشاره کنیم به‌روزرسانی هویت‌های گمنام (J_i' و k_i) بسیار سریع (که با کمک مقادیر تصادفی آن‌ها که برای هر پیام یک مقدار مجزا است صورت می‌گیرد) اتفاق می‌افتد. دلیل این امر استفاده مجدد از مقدار تصادفی داخل آن‌ها در هر بار ارسال پیام است. بنابراین، در طرح ارائه‌شده حریم خصوصی به‌صورت کامل برآورده می‌شود. در مقاله‌های حفظ حریم خصوصی به‌صورت کامل برآورده نمی‌شود. در مراجع [۴۰-۲۲] حریم خصوصی حفظ نمی‌شود. اما، در مقاله‌ها [۲۱-۱۹] حفظ حریم خصوصی به‌صورت کامل برآورده می‌شود. این در حالی است که در هر سه این مقاله‌ها احراز اصالت برآورده نمی‌شود. اما، در طرح پیشنهادی ما احراز اصالت با استفاده از امضا دیجیتال برآورده می‌شود. مقاله [۱۳] (منتشرشده در سال ۲۰۱۹)، در برابر حمله منع خدمت، حمله تکرار و حمله جعل هویت مقاوم است. اما، در این مقاله سازوکاری برای حفظ حریم خصوصی کاربرها در نظر گرفته نشده است.

- ارتباط ناپذیری: در طرحی که در این پژوهش ارائه شده است، هر بار که کاربر بخواهد پیامی را به لایه بالاتر ارسال کند، آن را امضا می‌کند. امضای مورداستفاده در این پژوهش

$$\mu_i \equiv v_i(f_i + 1) + \theta s(T_i, W_i, P_i, (s(g_i N) \oplus J_i), k_i) \\ + g_i \bmod l$$

می‌باشد که در آن، v_i و g_i مقادیر تصادفی هستند. هربار که کاربری بخواهد پیامی ارسال کند، یک مقدار تصادفی v_i از Z_l^* انتخاب می‌کند و همچنین محیط اجرایی امن مربوط به کاربر نیز یک مقدار جدید g_i از Z_l^* انتخاب می‌کند. بنابراین، احتمال موفقیت مهاجم در ربط دادن دو پیام مختلف به یک هویت بسیار ناچیز است. در مراجع [۱۸-۱۵ و ۴۵-۴۱] رتباط ناپذیری برآورده نمی‌شود. البته لازم به ذکر است که در [۱۵] تا حدی توانایی ارتباط‌پذیری برای مهاجم با سختی همراه است ولی مشابه طرح ما از مقادیر تصادفی همچون v_i و g_i در هر بار ارسال پیام استفاده نشده است. مسلماً با استفاده هرباره از این مقادیر توان حمله ارتباط‌پذیری به شدت کاهش می‌یابد. در جدول (۲) طرح پیشنهادی با طرح‌های قبلی مقایسه شده است.

جدول (۲): مقایسه طرح ارائه شده با طرح‌های قبلی.

طرح	حفظ حریم خصوصی	ارتباط ناپذیری	مقاومت در برابر حمله جعل هویت	تازه بودن داده و مقاومت در برابر حمله تکرار	احراز اصالت و یکپارچگی
طرح پیشنهادی	**دارد**	دارد	دارد	دارد	دارد
[۹]	**ندارد**			دارد	
[۱۵]			ندارد	دارد	ندارد
[۱۸-۱۶]			ندارد	دارد	ندارد
[۳۲-۲۳]، [۳۴]، [۴۰-۳۶] و [۲۱-۱۹]			ندارد		ندارد
[۲۲]	**ندارد**		دارد		دارد
[۱۳]	**ندارد**		دارد	دارد	دارد
[۴۵-۴۱]				ندارد	
[۴۰-۲۲]	**ندارد**				
[۲۱-۱۹]	**دارد**		ندارد		ندارد
[۴۵-۴۱]		ندارد			
[۱۸-۱۵]		ندارد			

۵- نتیجه‌گیری

طرح ارائه‌شده شامل دو قسمت است. بخشی که از رمزنگاری کلاسیک بهره می‌برد و بخشی که از رمزنگاری کوانتومی استفاده می‌کند. با استفاده از طرح جدید معرفی‌شده در این مقاله می‌توانیم با بهره‌گیری از فناوری رمزنگاری کلاسیک و کوانتومی نیازمندی‌های امنیتی مختلف در شبکه اینترنت اشیاء نظامی را برآورده کنیم. در واقع، می‌توان از طرح ارائه‌شده برای برآورده کردن نیازهای امنیتی حیاتی همچون احراز اصالت، محرمانگی، انکارناپذیری و غیره در شبکه ذکر شده استفاده کرد. ارزشمند است که بیان کنیم از این طرح جدید نه‌تنها در شبکه اینترنت

اشیاء نظامی می‌توان استفاده کرد بلکه می‌توان در بسیاری از شبکه‌های هوشمند دیگر همچون شبکه هوشمند برق، شبکه بلاک‌چین و غیره نیز استفاده کرد. طرح ارائه‌شده در مرحله اول از احراز اصالت کلاسیک بهره می‌برد. این مرحله با استفاده از رمزنگاری کلید عمومی و به‌طور خاص توسط طرح امضای دیجیتال جدید معرفی شده انجام می‌شود تا لایه‌های شبکه از اصالت هویت مقابل اطمینان حاصل کنند. استفاده از رمزنگاری کلید عمومی مربوط به این مرحله است، سپس طرح ارائه‌شده با استفاده از تسهیم راز کوانتومی، کلید رمزنگاری را با هویتی که اصالت آن قبلاً توسط احراز اصالت کلاسیک احراز شده است تبادل می‌کند. در ادامه با استفاده از این کلید به اشتراک گذاشته شده اطلاعات جمع‌آوری‌شده رمز شده و به لایه بالا ارسال می‌شوند. این طرح در برابر بسیاری از

حمله‌های کلاسیک مطرح در شبکه اینترنت اشیاء نظامی مقاوم است. همچنین، در برابر حمله کامپیوترهای کوانتومی نیز از امنیت لازم برخوردار است. در مقایسه با طرح‌های مشابه، طرح ارائه شده نیازمندی‌های امنیتی بیشتری را با سازوکارهای کارا برآورده می‌کند که در قسمت تحلیل امنیتی طرح راجع به آن‌ها صحبت شد.

۶- مراجع

[1] L. Yushi, J. Fei, and Y. Hui, "Study on application modes of military Internet of Things (MIOT)," 2012 IEEE International Conference on Computer Science and Automation Engineering (CSAE) , pp. 630-634, 2012.

[2] R. P Feynman, "Simulating physics with computers," International journal of theoretical physics 21.6-7, pp. 467-488, 1982.

[3] A. M. Childs and et al., "Quantum walks on graphs," Proceedings of 35th ACM Symposium on Theory of Computing STOC, 2003.

[4] H. C. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," IEEE International Conference on Computers Systems and Signal Processing, vol. 560, pp. 175-179, 1984.

[5] "IoT Roadmap - Iran Telecommunication Research Center," 1396. (In Persian) [Online]. Available: https: //iot.itrc.ac.ir/sites/default/files/PRESENTATION%20-IOT.pdf.

[6] "The Guardian," 2016. [Online]. Available: https: //www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper.

[7] "Military Applications Iot," 2018. [Online]. Available: http: //wfiot2018.iot.ieee.org/sps2-military-applications-iot/.

[8] "Global Research," 2015. [Online]. Available: https: //www.globalresearch.ca/nsa-cyber-war-will-use-internet-of-things-as-weapons-platform-your-home-is-the-battlefield/5425526.

[9] "The Hill," Morgan Wright, Opinion Contributor- 03/14/18 06: 00 AM EDT, 2018. [Online]. Available: https: //thehill.com/opinion/technology/378286-for-national-security-the-internet-of-things-is-the-internet-of-trouble.

[10] "High Council of Cyberspace," 1396. (In Persian) [Online]. Available: http: //www.ion.ir/News/305245.html.

[11] "The need for national coordination in the use of the Internet of Things," Establishment of Internet of Things Working Group at the National Cyberspace Center, 1396. (In Persian) [Online]. Available: majazi.ir.

[12] "Goals and Achievements - Internet of Things," 1396. (In Persian). [Online]. Available: https: //iot.itrc.ac.ir/node/83

[13] M. A. Jan, F. Khan, M. Alam, and M. Usman, "A payload-based mutual authentication scheme for Internet of Things," Future Generation Computer Systems 92, pp. 1028-1039, 2019.

[14] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," Future Generation Computer Systems 91, pp. 244-251, 2019.

[15] D. Chen, N. Zhang, and Z. Qin, "S2M: a lightweight acoustic fingerprints based wireless device authentication protocol," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 88-100, 2017.

[16] C. Lai, H. Li, R. Lu, and X. 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.

[17] 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, p. 2678-2686, 2015.

[18] C. Lai, H. Li, R. Lu, R. Jiang, and X. Shen, "LGTH: a lightweight group authentication protocol for machine-type communication in LTE networks," Proceedings of the IEEE Global Communications Conference (GLOBECOM '13) ,pp. 832-837, 2013.

[19] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," Security and Communication Networks, vol. 7, no. 12, pp. 2728-2742, 2014.

[20] S. Chabridon, R. Laborde, T. Desprats, A. Oglaza, P. Marie, and S. M. Marquez, "A survey on addressing privacy together with quality of context for context management in the Internet of Things," Annals of Telecommunications-Annales des Telecommunication vol. 69, no. 1-2, pp. 47-62, 2014.

[21] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," Journal of Network and Computer Applications, vol. 42, pp. 120-134, 2014.

[22] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for internet of things: a comprehensive survey," Security and Communication Networks, 2017.

[23] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. 32, article no. 1181, pp. 17-31, 2015.

[24] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: the road ahead," Computer Networks, vol. 76, pp. 146-164, 2015.

[25] C. C. Aggarwal, N. Ashish, and A. Sheth, "The Internet of Things: A Survey from the Data-Centric Perspective," Managing and Mining Sensor Data, Springer US, Boston, MA, pp. 383-428, 2013.

[26] D. Miorandi, S. Sicari, F. d. Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," AdHoc Networks, vol. 10, no. 7, pp. 1497-1516, 2012.

[27] R. H. Weber, "Internet of Things , New security and privacy challenges," Computer Law & Security Review, vol. 26, no. 1, pp. 23-30, 2010.

[28] C. M. Medaglia and A. Serbanati, “An Overview of Privacy and Security Issues in the Internet of Things,” The Internet of Things, Springer New York, NY, USA, pp. 389-395, 2010.

[29] D. Airehrour, J. Gutierrez, and S. K. Ray, “Secure routing for internet of things: A survey,” Journal of Network and Computer Applications, vol. 66, pp. 198-213, 2016.

[30] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, “Twenty Security Considerations for Cloud-Supported Internet of Things,” IEEE Internet of Things Journal, vol. 3, no. 3, pp. 269-284, 2016.

[31] S. Li, T. Tryfonas, and H. Li, “The Internet of Things: a security point of view,” Internet Research, vol. 26, no. 2, pp. 337-359, 2016.

[32] W. Xie, Y. Tang, S. Chen, Y. Zhang, and Y. Gao, “Security of Web of Things: A Survey (Short Paper),” Advances in Information and Computer Security, vol. 9836 of Lecture Notes in Computer Science, Springer International Publishing, Cham, pp. 61-70, 2016.

[33] D. He and S. Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography,” IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72-83, 2015.

[34] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, “Security and privacy challenges in industrial internet of things,” Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC ’15), IEEE, San Francisco, Calif, USA, pp. 1-6, 2015.

[35] J. Granjal, E. Monteiro, and J. S. Silva, “Security for the internet of things: a survey of existing protocols and open research issues,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015.

[36] S. L. Keoh, S. S. Kumar, and H. Tschofenig, “Securing the internet of things: a standardization perspective,” IEEE Internet of Things Journal, vol. 1, no. 3, pp. 265-275, 2014.

[37] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, “Security of the internet of things: perspectives and challenges,” Wireless Networks, vol. 20, no. 8, pp. 2481-2501, 2014.

[38] R. Roman, J. Zhou and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” Computer Networks, vol. 57, no. 10, pp. 2266-2279, 2013.

[39] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the internet of things: a review,” Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE ’12) , pp. 648-651, 2012.
Wang, Mingzhong, Dan Liu, Liehuang Zhu, Yongjun Xu, and Fei Wang. “LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication” Computing 98, no. 7, pp. 685-708, 2016.

[40] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, “Key manage ment systems for sensor networks in the context of the Internet of Things,” Computers Electrical Engineering, vol. 37, no. 2, pp. 147-159, 2011.

[41] C. Lai, R. Lu, D. Zheng, H. Li, and X. Sherman, “GLARM: group-based lightweight authentication scheme for resourceconstrained machine to machine communications,” Computer Networks, pp. 66-81, 2016.

[42] 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,” Proceedings of the 2014 1st IEEE International Conference on Communications, ICC, pp. 1011-1016, 2014.

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

[44] C. Lai, H. Li, X. Liang, R. Lu, K. Zhang, and X. Shen, “CPAL: A conditional privacy-preserving authentication with access linkability for roaming service,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 46-57, 2014.

[45] 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.

[46] M. Hillery, V. Bužek, and A. Berthiaume, “Quantum secret sharing,” Phys. Rev. A 59, vol. 59, no. 3, pp. 1829-1834, 1998.

[47] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, “Quantum key distribution via quantum encryption,” Phys. Rev. A, American Physical Society, vol. 64, no. 2, pp. 24302-24306, 2001.

[48] R. Pass, E. Shi, and F. Tramer, “Formal abstractions for attested execution secure processors,” In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Cham, pp. 260-289, 2017.

[49] M. M. Jaghal and M. A. Dostari, “Provide solutions to improve security and privacy in the health system using SIM card,” Scientific Journal of Electronic and Cyber Defense, vol. 7, no. 1, Sequential Issue 25, pp. 11-24, 1398. (In Persian)

[50] “shotspotter,” 2018. [Online]. Available: http: //www.shotspotter.com.

[51] “europa,” Official Journal L 281 , 23/11/1995 P. 0031 - 0050, 1995. [Online]. Available: https: //eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX: 31995L0046: en: HTML.

[52] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Letters from the Past - A PRL Retrospective, vol. 67, no. 6, pp. 661-663, 1991.

[53] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Physical review letters, 68.21: 3121, 1992.

[54] H. Bechmann-Pasquinucci and N. Gisin, “Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography,” Physical Review A 59.6: 4238, 1999.

[55] N. Gisin and et al., “Towards practical and fast quantum cryptography,” arXiv preprint quant-ph/0411022, 2004.