

ارائه طرح احراز اصالت سبک با قابلیت گمنامی و اعتماد در اینترنت اشیا

شادی جانبابائی^۱، حسین قرائی^{۲*} و ناصر محمدزاده^۳

^۱ دانشکده فنی مهندسی، گروه مهندسی کامپیوتر، دانشگاه شاهد تهران

^۲ پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

چکیده

اینترنت اشیا مفهوم جدیدی است که باعث حضور حس گرها در زندگی انسان شده است؛ به طوری که تمامی اطلاعات توسط همین حس گرها جمع آوری، پردازش و منتقل می شوند. برای برقراری یک ارتباط امن، با افزایش تعداد حس گرها، نخستین چالش، احراز اصالت بین آنها است. گمنامی، سبک وزنی و قابلیت اعتماد نیز از جمله مواردی هستند که باید مد نظر قرار گیرند. در این پژوهش پروتکل های احراز اصالت در حوزه اینترنت اشیا بررسی شده و محدودیت ها و آسیب پذیری های امنیتی آنها مورد تحلیل واقع شده اند. هم چنین پروتکل احراز اصالت جدیدی پیشنهاد می شود که گمنامی به عنوان یک پارامتر مهم، در آن لحاظ می شود. از طرفی تابع چکیده ساز و عمل گرهای منطقی نیز مورد استفاده قرار می گیرند تا هم پروتکل سبک باشد و هم حس گرها بتوانند به عنوان موجودیت هایی محدود از لحاظ محاسباتی، از آنها استفاده کنند. در این پروتکل نیازمندی های امنیتی از قبیل قابلیت عدم ردیابی، مقیاس پذیری، دسترس پذیری و غیره لحاظ شده اند و پروتکل در مقابل حملات مختلف از جمله حمله جعل هویت، تکرار، مرد میانی و ... مقاوم است. واژگان کلیدی: اینترنت اشیا، احراز اصالت، گمنامی، سبک وزنی و اعتماد.

The Lightweight Authentication Scheme with Capabilities of Anonymity and Trust in Internet of Things (IoT)

Shadi Janbabaei¹, Hossein Gharaee^{2*} & Naser Mohammadzadeh³

^{1,3}Department of Computer Engineering, Shahed University, Tehran, Iran

²Department of Network Security, ICT Research Institute (ITRC), Tehran, Iran

Abstract

The Internet of Things (IoT), is a new concept that its emergence has caused ubiquity of sensors in the human life. All data are collected, processed, and transmitted by these sensors. As the number of sensors increases, the first challenge in establishing a secure connection is authentication between sensors. Anonymity, lightweight, and trust between entities are other main issues that should be considered. However, this challenge also requires some features so that the authentication is done properly. Anonymity, light weight and trust between entities are among the issues that need to be considered. In this study, we have evaluated the authentication protocols concerning the Internet of Things and analyzed the security vulnerabilities and limitations found in them. A new authentication protocol is also proposed-using the hash function and logical operators, so that the sensors can use them as computationally limited entities. This protocol is performed in two phases and supports two types of intra-cluster and inter-cluster communication. The analysis of proposed protocol shows that security requirements have been met and the protocol is resistant against various attacks. In the end, confidentiality and authentication of the protocol are proved applying AVISPA tool and the veracity of the protocol using the BAN logic. Focusing on this issue, in this paper, we have evaluated the authentication protocols in the Internet of Things and analyzed their limitations and security vulnerabilities.

* نویسنده عهده دار مکاتبات • تاریخ ارسال مقاله: ۱۳۹۶/۷/۱۴ • تاریخ آخرین بازنگری: ۱۳۹۷/۵/۷ • تاریخ پذیرش: ۱۳۹۷/۵/۱۵ • Corresponding author



Moreover, a new authentication protocol is presented which the anonymity is its main target. The hash function and logical operators are used not only to make the protocol lightweight but also to provide some computational resources for sensors. In compiling this protocol, we tried to take into account three main approaches to covering the true identifier, generating the session key, and the update process after the authentication process. As with most authentication protocols, this protocol is composed of two phases of registration and authentication that initially register entities in a trusted entity to be evaluated and authenticated at a later stage by the same entity. It is assumed that in the proposed protocol we have two types of entities; a weak entity and a strong entity. The poor availability of SNs has low computing power and strong entities of CH and HIoT that can withstand high computational overhead and carry out heavy processing. We also consider strong entities in the proposed protocol as reliable entities since the main focus of this research is the relationship between SNs. On the other hand, given the authenticity of the sensors and the transfer of the key between them through these trusted entities, the authenticity of the sensors is confirmed, and the relationship between them is also reliable. This protocol supports two types of intra-cluster and inter-cluster communication. The analysis of the proposed protocol shows that security requirements such as untraceability, scalability, availability, etc. have been met and it is resistant against the various attacks like replay attack, eavesdropping attack.

Keywords: Internet of things, Authentication, Anonymity, Lightweight.

می‌دهد [4]. این فناوری دو حالت کلی دارد: متمرکز^۴ و توزیع‌شده^۵. در یک رویکرد متمرکز، پلتفرم‌های برنامه کاربردی در اینترنت (به عنوان مثال خدمات ابر) قرار گرفته و اطلاعاتی را از موجودیت‌های واقع در شبکه کسب کرده و داده‌های خام و خدماتی را برای سایر موجودیت‌ها فراهم می‌کنند. از سوی دیگر، در یک رویکرد توزیع‌شده، نه تنها هوشمندی و ارائه خدمات در لبه‌های شبکه قرار می‌گیرند، بلکه پلتفرم‌های مختلف نرم‌افزاری نیز می‌توانند با یکدیگر به صورت پویا همکاری کنند [5].

محیط کنترل‌نشده^۶، ناهمگونی^۷، مقیاس‌پذیری^۸ و منابع محدود، ویژگی‌های اصلی اینترنت اشیا را تشکیل می‌دهند. براساس این ویژگی‌ها، نیازمندی‌های امنیتی این فناوری نیز در پنج مجموعه امنیت شبکه^۹، مدیریت شناسه^{۱۰}، حریم خصوصی، قابلیت اعتماد^{۱۱} و انعطاف‌پذیری^{۱۲} طبقه‌بندی می‌شوند [6]. احراز اصالت^{۱۳} یکی از زیرشاخه‌های اصلی مدیریت شناسه است که در آن اعتبار هویت ادعا شده، مورد بررسی قرار می‌گیرد. به عبارت بهتر، احراز اصالت، ارائه اطلاعات توسط یکی از موجودیت‌های ارتباطی است که این اطلاعات بایستی به‌طور دقیق با هویت یاد شده، هم‌خوانی داشته باشند [7]. هم‌چنین گمنامی^{۱۴} نیز یکی از مهم‌ترین زیرشاخه‌های حریم خصوصی محسوب می‌شود که با وجود آن مهاجم توانایی ردیابی موجودیت را نداشته و در نهایت امکان برخی حملات

⁴ Centralized

⁵ Distributed

⁶ Uncontrolled environment

⁷ Heterogeneity

⁸ Scalability

⁹ Network Security

¹⁰ Identity Management

¹¹ Trust

¹² Resilience

¹³ Authentication

¹⁴ Anonymity

۱- مقدمه

امروزه حدود دو میلیارد نفر در سراسر جهان برای دریافت خدماتی مانند وب‌گردی، ارسال و دریافت رایانه، دست‌یابی به محتوا و خدمات اینترنتی، بازی‌ها و غیره از اینترنت استفاده می‌کنند. برای این که بیش‌تر مردم به این زیرساخت ارتباطات و اطلاعات جهانی دسترسی یابند و از آن بهره‌برند، جهش بزرگ دیگری در حال وقوع است که در آن استفاده از اینترنت به‌عنوان یک پلتفرم جهانی مفروض است. از طریق این پلتفرم، ماشین‌ها و اشیای هوشمند می‌توانند با یکدیگر ارتباط و همکاری داشته باشند. این فناوری، با نام اینترنت اشیا (IoT) شناخته می‌شود [1]. عبارت اینترنت اشیا برای نخستین بار توسط کوین اشتون در سال ۱۹۹۰ مورد استفاده قرار گرفت. اشتون جهانی را توصیف کرد که در آن همه چیز، از جمله اشیای بی‌جان، برای خودشان هویت دیجیتالی داشته باشند و به رایانه‌ها اجازه داده شود تا آن‌ها را سازماندهی و مدیریت کنند [2]. به عبارت دیگر، اینترنت اشیا فناوری نوینی است که در آن برای هر موجودیتی (انسان، حیوان و یا اشیا) امکان ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترنت، فراهم می‌شود. بیش از پنجاه درصد اتصالات اینترنت، اشیا هستند، که در سال ۲۰۱۱ تعداد آن‌ها بیش از پانزده بلیون تخمین زده شد و پیش‌بینی می‌شود که تا سال ۲۰۲۰ به سی بلیون دستگاه برسد [3]. فناوری‌های تعبیه‌شده از قبیل شناسایی خودکار رادیویی (RFID)، فناوری‌های ارتباطات بی‌سیم، شبکه‌های حس‌گر (WSN)، شبکه تجهیزات تعبیه‌شده و ... فناوری اینترنت اشیا را شکل

¹ Internet of Things

² Radio Frequency Identification

³ Wireless Sensor Networks

امنیتی دیگری بر اساس گواهی‌نامه‌ی $ECQV^3$ و $DTLS$ برای اینترنت اشیا طراحی و پیاده‌سازی شد [12]. در مرحله‌ی ثبت نام این پروتکل، تمامی دستگاه‌ها گواهی‌نامه‌ی $ECQV$ را دریافت می‌کنند. اجرای طرح تولید گواهی‌نامه‌ی $ECQV$ از طریق پروتکل دست‌تکانی، نقطه‌ی قوت این مرحله است. در مرحله‌ی برقراری کلید امن، الگوریتم تبادل کلید $ECDH^4$ و گواهی‌نامه‌ی $ECQV$ ترکیب می‌شوند تا طرح ارائه‌شده، برقراری کلید و احراز اصالت را تماماً برقرار کند. ساختار و محتوای پیام‌ها به‌طور دقیق همانند $DTLS 1.2$ است؛ با این تفاوت که به‌جای گواهی $X.509$ از گواهی‌نامه‌ی $ECQV$ استفاده شده است. در طرح [13]، پروتکل احراز اصالت دومرحله‌ای برای شبکه‌های حس‌گر بی‌سیم پیشنهاد شده است. این پروتکل در سال ۲۰۱۴، کامل‌تر شده و برای استفاده در برنامه‌های کاربردی اینترنت اشیا نیز پیشنهاد شد [14]. در این دو پروتکل به‌جای استفاده از RSA ، از ECC و یک کلید مشترک از پیش تعیین‌شده استفاده می‌شود تا پروتکل سبک‌تر از طرح‌های قبلی شود؛ اما بسیاری از چالش‌های اینترنت اشیا از جمله گمنامی و قابلیت عدم ردیابی در این پروتکل لحاظ نشده است. همچنین وجود یک کلید نشست ثابت بین دو گره، جستجوی خطی درجه n جهت حفظ تازگی پیام و ارتباط سنگین $DTLS$ موجود بین سرخوشه‌ها از جمله نقاط ضعف پروتکل یادشده است. برای سبک‌تر ساختن پروتکل‌های احراز اصالت در اینترنت اشیا، طرح‌های احراز اصالت [15] و [16] مبتنی بر تابع چکیده‌ساز، عمل‌گرهای یای انحصاری و الحاقی مطرح شده‌اند. در [15] پروتکل احراز اصالت برچسب $RFID$ مبتنی بر تابع چکیده‌ساز ارائه شده است. در این پروتکل احراز اصالت فقط بین برچسب و سرور اتفاق می‌افتد و پروتکل در مقابل حمله جعل^۵ آسیب‌پذیر است. در طرح [16] پروتکل احراز اصالت دیگری به‌همراه گمنامی و قابلیت عدم ردیابی ارائه شده است. از جمله نقاط ضعف این طرح می‌توان به بالابودن حجم کاری سرور، نبود کلید نشست در انتهای احراز اصالت، عدم احراز اصالت گره‌های انتهایی توسط یکدیگر و آسیب‌پذیری در مقابل حمله تکرار^۶ اشاره کرد. در [17]، طرح احراز اصالت گره‌های انتهایی با قابلیت اعتماد توسعه‌یافته در شبکه‌های موردی خودرو پیشنهاد شده است. در این پروتکل علاوه بر استفاده از تابع چکیده‌ساز، عمل‌گرهای یای انحصاری و الحاقی، یک مجموعه کلید امن مبتنی بر زنجیره چکیده‌ساز نیز تولید می‌شود؛ اما برای احراز اصالت

به سیستم‌ها محدود شود [8,9]. از طرفی احراز اصالت دو جانبه و برقراری کلید دو موضوع اساسی در بررسی پروتکل‌های احراز اصالت هستند [7]. هدف پروتکل‌های احراز اصالت، اطمینان یافتن یک موجودیت از هویت موجودیت دیگر است. گرچه محدودیت‌های بسیاری نیز در این حوزه وجود دارد، اما می‌توان برخی مسائل عمومی را به‌عنوان قاعده کلی در طراحی این نوع پروتکل‌ها برقرار کرد. نخست، باید گام‌های محاسباتی و هزینه‌ها را به‌منظور صرفه‌جویی در انرژی به کمینه رساند؛ علاوه بر این، به‌منظور توزیع بار محاسباتی میان گره‌ها، ویژگی‌ها و قابلیت‌های دستگاه‌ها بایستی مدنظر قرار گیرد. در نهایت، تعداد پیام‌هایی که رد و بدل می‌شوند و طول آنها، پارامترهایی هستند که باید با ملاحظه انتخاب شوند [10]. حال به این نتیجه می‌رسیم که احراز اصالت دوطرفه به همراه مجموعه‌ای از ویژگی‌های مرتبط با اینترنت اشیا، یکی از مهم‌ترین چالش‌های روز محسوب می‌شود که بایستی بیش از پیش مورد تحلیل و بررسی قرار گیرد. در ادامه، ابتدا کارهای مرتبط، ویژگی‌ها، آسیب‌پذیری‌ها و محدودیت‌های موجود مورد بررسی قرار می‌گیرند و معماری مورد استفاده جهت طراحی پروتکل توصیف می‌شود؛ سپس پروتکل پیشنهادی به تفصیل تشریح شده و پس از آن به تحلیل امنیتی و مقایسه بار محاسباتی آن با سایر پروتکل‌ها خواهیم پرداخت.

۲- کارهای مرتبط

در اینترنت اشیا، ارتباط بین موجودیت‌ها به چندین دسته طبقه‌بندی می‌شود. احراز اصالت، حس‌گرهای انتهایی یکی از این نوع ارتباطات است [11]. در [9]، معماری انتها به انتهایی برای احراز اصالت دومرحله‌ای مبتنی بر $DTLS^1$ پیشنهاد شده است. در این طرح، گره‌هایی که می‌خواهند به شبکه متصل شوند، با توجه به قابلیت‌هایشان، مجموعه رمزنگاری مناسب خود را انتخاب می‌کنند؛ اما با توجه به این که هشت پیام برای دست‌تکانی استفاده می‌شود، سربر قابل توجهی به وجود می‌آید. از طرفی استفاده از گواهی‌نامه‌های $X.509$ و کلید عمومی RSA با دست‌تکانی $DTLS$ برای حس‌گرهایی با قدرت محاسباتی پایین و محدودیت بالای منابع، بیش از حد سنگین است. همچنین ویژگی‌هایی از اینترنت اشیا مانند گمنامی و قابلیت عدم ردیابی^۲ در آن لحاظ نشده است. از طرفی در هر دو مرحله، طرفین ارتباط جهت برقراری یک پارچگی، نیاز به یک کلید مخفی خواهند داشت. در سال ۲۰۱۶، یک طرح

³ Elliptic Curve Qu-Vanstone

⁴ Elliptic curve Diffie-Hellman

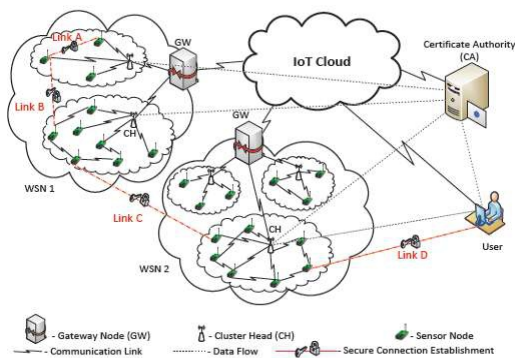
⁵ Impersonating Attack

⁶ Replay Attack

¹ Datagram Transport Layer Security

² Untraceability

همچنین موجودیت‌های قوی را در پروتکل پیشنهادی موجودیت‌های قابل اعتماد در نظر می‌گیریم؛ چون تمرکز اصلی در این پژوهش ارتباط بین SNها است. از طرفی باتوجه به این‌که احراز اصالت بین حس‌گرها و انتقال کلید نشست بین آنها از طریق این موجودیت‌های قابل اعتماد انجام می‌شود، پس با تأیید احراز اصالت حس‌گرها، ارتباط بین آنها نیز قابل اعتماد خواهد بود. نمادهای استفاده‌شده در پروتکل پیشنهادی در جدول (۱) نشان داده شده است.



(شکل-۱): معماری مفروض
(Figure-1): Assumed architecture

(جدول-۱): نمادهای استفاده‌شده در طراحی پروتکل پیشنهادی
(Table-1): Notations

نماد	توضیحات
SN _i	گره حس‌گر آام
Chi	سرخوشه آام
HIoTS	سرور اصلی
IDI/ IDi'	شناسه حقیقی گره حس‌گر (سرخوشه)
IDh	شناسه حقیقی سرور اصلی
Ni/Ni'	اعداد تصادفی تولیدشده در احراز اصالت دو حس‌گر (دو سرخوشه)
Ki/ Ki'	کلید مشترک تعبیه شده بین سرخوشه و حس‌گر آام (بین سرور و سرخوشه آام)
AIDI/ AIDI'	شناسه غیرحقیقی و مستعار یک‌بار مصرف برای حس‌گر (سرخوشه) آام
Tri/ Tri'	شماره تصادفی تولید شده برای بررسی تازگی پیام بین سرخوشه و حس‌گر(سرور)
Vi/Vi'	عبارتهایی جهت ارزیابی پیام دریافتی
SK	کلید نشست تعیین شده در انتهای پروتکل بین دو حس‌گر
SK _i	کلید ارسالی برای حس‌گر آام جهت دستیابی به SK
AK	کلید توافق‌شده بین دو سرخوشه
H(.)	تابع چکیده‌ساز یک‌طرفه- تابع Hash
⊕	عمل‌گر XOR
	عمل‌گر الحاق

مجدد در ارتباط امن بین موجودیت‌ها شکاف وجود دارد. از طرفی کل ارتباطات به یک کلید از پیش تعیین‌شده وابسته‌اند که در صورت فاش شدن آن کل ارتباطات زیر سؤال می‌رود. تحلیل و بررسی کارهای پیشین، نشان می‌دهد که در ابتدا از زیرساخت PKI و رمزنگاری RSA جهت احراز اصالت استفاده می‌شد، درحالی‌که امروزه به دلیل سربار محاسباتی بالا و سنگین بودن آن، این روش کمتر مورد توجه قرار می‌گیرد؛ سپس ECC به‌عنوان رمزنگاری سبک‌تر نسب به RSA مطرح شده که این رمزنگاری نیز برای دستگاه‌های محدود از نظر محاسباتی و پردازشی، همچنان سنگین است. در همین اواخر توابع چکیده‌ساز و عمل‌گرهای منطقی بیشتر مورد توجه قرار می‌گیرند، تا سبک وزنی به‌عنوان یکی از پارامترهای مهم برقرار شود. همچنین بسیاری از پروتکل‌های ارائه‌شده فقط ارتباط هر موجودیت را با موجودیت بالادستی در نظر می‌گیرند؛ درحالی‌که ارتباط بین موجودیت‌ها با یکدیگر نیز ضروری است [11].

۳- مدل پیشنهادی

۳-۱- معماری مفروض

مدل پروتکل احراز اصالت مفروض طرح پیشنهادی در شکل (۱) نمایش داده شده است [14]. همان‌طور که مشخص است، موجودیت‌ها می‌توانند به‌صورت عمودی و افقی با یکدیگر در ارتباط باشند. ارتباط بین دو حس‌گر در یک سرخوشه، ارتباط افقی و ارتباط بین کاربر و حس‌گر، یک ارتباط عمودی محسوب می‌شود. تمرکز ما در این پژوهش ارتباط بین حس‌گرها است.

۳-۲- طرح پیشنهادی

در تدوین این پروتکل، تلاش شده است سه رویکرد اصلی، پوشش شناسه حقیقی، تولید کلید نشست و فرآیند به‌روزرسانی پس از فرآیند احراز اصالت را لحاظ کنیم. این پروتکل همانند بیشتر پروتکل‌های احراز اصالت از دو مرحله ثبت نام و احراز اصالت تشکیل شده که در ابتدا موجودیت‌ها در یک نهاد قابل اعتماد ثبت نام می‌کنند تا در مرحله بعد به کمک همان نهاد مورد ارزیابی و احراز اصالت قرار گیرند. فرض بر این است که در پروتکل پیشنهادی دو نوع موجودیت ضعیف و موجودیت قوی داریم. موجودیت ضعیف SNها هستند که توان محاسباتی پایینی دارند و موجودیت‌های قوی CHها و HIoTSها هستند که می‌توانند سربار محاسباتی بالایی را تحمل کرده و پردازش‌های سنگینی را انجام دهند.

موجودیت قابل اعتماد وارد عمل می‌شود و احراز اصالت بین دو حس گر را میسر می‌سازد. تعاملات بین حس گرها در شکل (۳) نشان داده شده است. در ادامه این تعاملات را به تفصیل بیان می‌کنیم:

گام ۱: حس گر SN1 مقدار تصادفی $N1$ را تولید کرده و دو رابطه $V1 = H(AID1 || AID2 || N1)$ و $A = N1 \oplus K1$ را محاسبه می‌کند. عبارت $V1$ جهت ارزیابی سمت گیرنده تولید و در پایان گام ۱، پیام $M1 = \{AID1, AID2, Tr1, V1, A\}$ از طریق یک کانال ناامن برای CH ارسال می‌شود.

گام ۲: CH با دریافت پیام $M1$ ، در ابتدا مقدار $Tr1$ دریافتی را با مقدار ذخیره شده در پایگاه داده مقایسه و سپس مقدار $N1$ را به دست آورده و با توجه به مقادیر دریافتی، مقدار $V1$ را محاسبه و $V1$ محاسبه شده را با $V1$ دریافتی مقایسه می‌کند. در صورت برابری این دو مقدار، SN1 برای CH احراز اصالت می‌شود. در صورت معتبر بودن این ارزیابی، CH از حس گری با $AID2$ درخواست می‌کند تا اطلاعات خود را جهت احراز اصالت برای CH ارسال کند. این درخواست توسط پیام $M2 = \{AuthReq\}$ فرستاده می‌شود.

گام ۳: حس گر دوم با دریافت پیام $M2$ ، همانند حس گر نخست مقادیر لازم را تولید و برای CH ارسال می‌کند با این تفاوت که از AID حس گر نخست مطلع نیست! پیام $M3 = \{AID2, Tr2, V2, B\}$ برای CH ارسال می‌شود.

گام ۴: در ابتدا، CH همانند گام ۲ عمل می‌کند و احراز اصالت حس گر دوم نیز انجام می‌شود؛ سپس مقادیر Tr و AID مربوط به هر دو حس گر را به روزرسانی و در نهایت کلید نشست بین این دو حس گر را از طریق رابطه $SK = N1 \oplus N2$ محاسبه می‌کند. حال برای ارسال کلید نشست و مقدار Tr به روز شده، بایستی از دو عبارت $SK1 = (Tr1 || SK) \oplus H(K1 || AID2)$ و $SK2 = (Tr2 || SK) \oplus H(K2 || AID1)$ استفاده شود. از طرفی دو رابطه $V3 = H(AID1 || SK2 || N2 || Tr2)$ و $V4 = H(AID2 || SK1 || N1 || Tr1)$ نیز برای ارزیابی سمت گیرنده، تولید شده و روی خط ارسال می‌شوند. در انتهای این گام، دو پیام $M4 = \{SK1, V4, Tr1\}$ و $M5 = \{AID1, SK2, V3, Tr2\}$ به ترتیب برای حس گر نخست و حس گر دوم ارسال می‌شود.

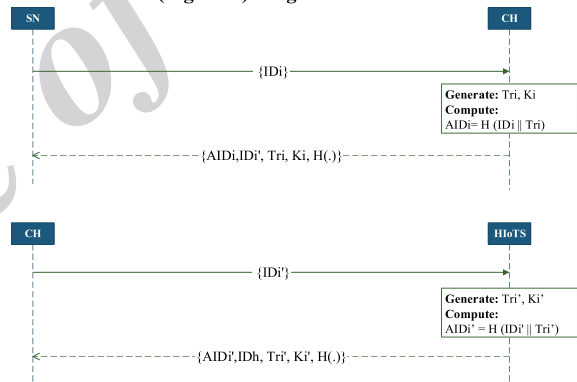
گام ۵: هریک از حس گرها مقدار کلید نشست و Tr به روزرسانی شده را با استفاده از $SK1$ و $V4$ (یا $SK2$

۱-۲-۳- مرحله ثبت نام

در این مرحله گره‌های حس گر، شناسه حقیقی خود را از طریق یک کانال ارتباطی امن برای سرخوشه ارسال می‌کنند؛ سپس سرخوشه دو مقدار تصادفی $Trseq$ و K را تولید کرده و مقدار شناسه غیرحقیقی مستعاری ($AIDi$) را برای حس گر محاسبه می‌کند تا از طریق همان کانال به حس گر منتقل شود. این مقادیر در پایگاه داده خود سرخوشه نیز ذخیره خواهند شد تا در مراحل احراز هویت، مقادیر آنها مورد بررسی قرار گیرد. هم‌چنین همین فرآیند برای ثبت نام سرخوشه‌ها در HIoTS نیز تکرار خواهد شد تا تمامی موجودیت‌ها در شبکه و توسط نهاد مرتبه بالاتر ثبت نام شوند. ذکر این نکته ضروری است که در پروتکل پیشنهادی، توزیع کلید به صورت سلسله‌مراتبی است بدین صورت که حس گرهای نیازی به ثبت نام در HIoTS نخواهند داشت و هر CH به طور مستقیم وظیفه ثبت نام حس گرها را بر عهده دارد. پروتکل این مرحله در شکل (۲) نمایش داده شده است.

(شکل ۲): مرحله ثبت نام پروتکل پیشنهادی

(Figure-2): Registration Phase



۲-۲-۳- مرحله احراز اصالت

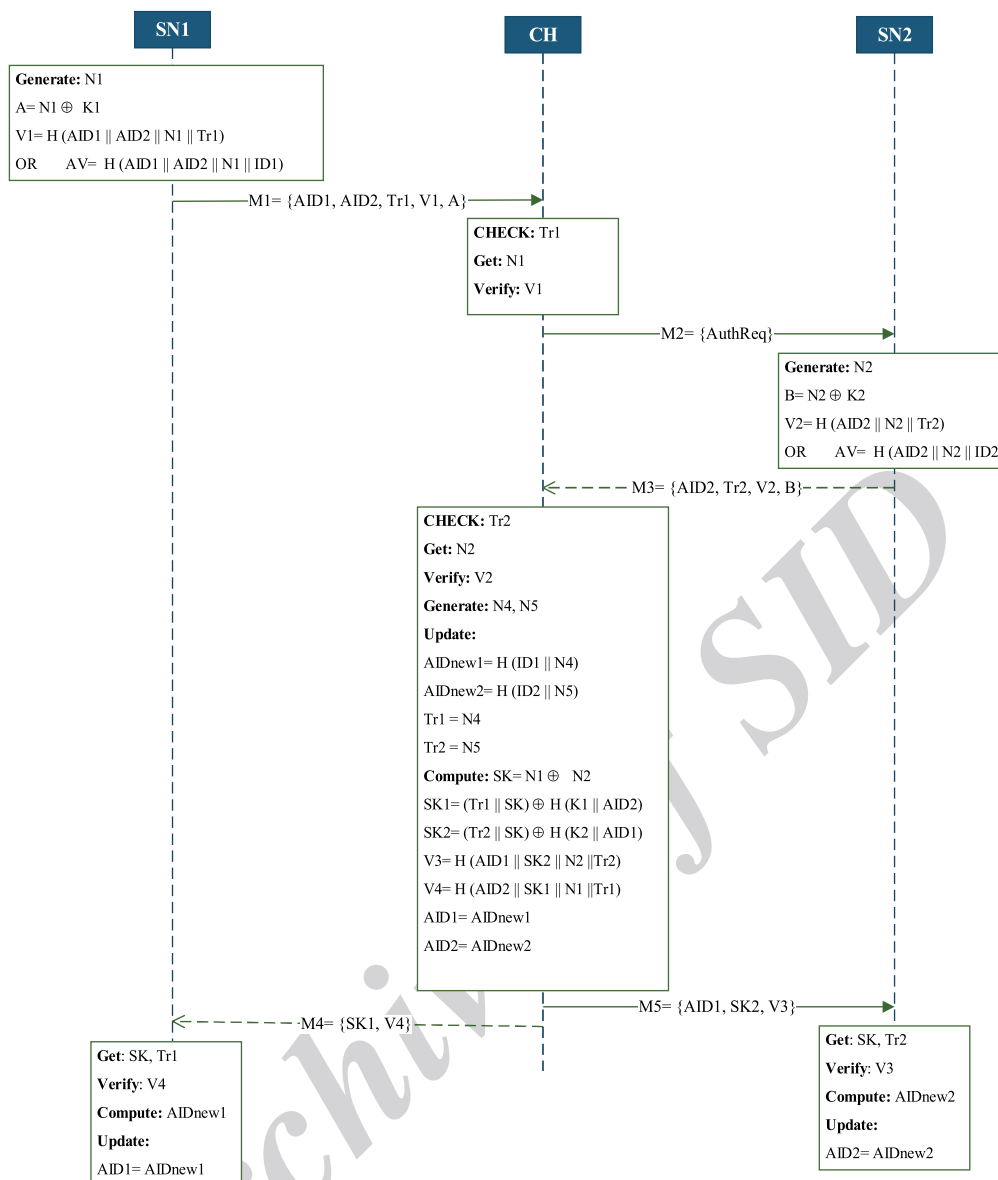
در این مرحله، دو گره حس گر می‌خواهند به صورت گمنام یکدیگر را احراز اصالت کرده و در انتها کلید نشست با یکدیگر برقرار و از طریق آن کلید، داده‌هایی را باهم مبادله کنند. تعاملات بین این دو حس گر با توجه به موقعیت آنها به دو دسته طبقه‌بندی می‌شود: دو حس گر در CH یکسان و دو حس گر در دو CH متفاوت. با این حال برای احراز اصالت دو حس گر در CH‌های متفاوت، نیاز به احراز اصالت CH‌ها توسط HIoTS نیز خواهیم داشت.

احراز اصالت بین دو حس گر در CH یکسان:

هنگامی که دو حس گر در CH یکسانی واقع شده‌اند، برای احراز اصالت یکدیگر از CH کمک می‌گیرند، چون CH به عنوان

و (V3 دریافتی به دست آورده و ارزیابی می کنند. در انتها بایستی مقدار AIDها از طریق روابط $AID1 = H(ID1 \parallel N4)$ و $AID2 = H(ID2 \parallel N5)$ به روزرسانی شوند.

در انتها بایستی مقدار AIDها از طریق روابط $AID1 = H(ID1 \parallel N4)$ و $AID2 = H(ID2 \parallel N5)$ به روزرسانی شوند.

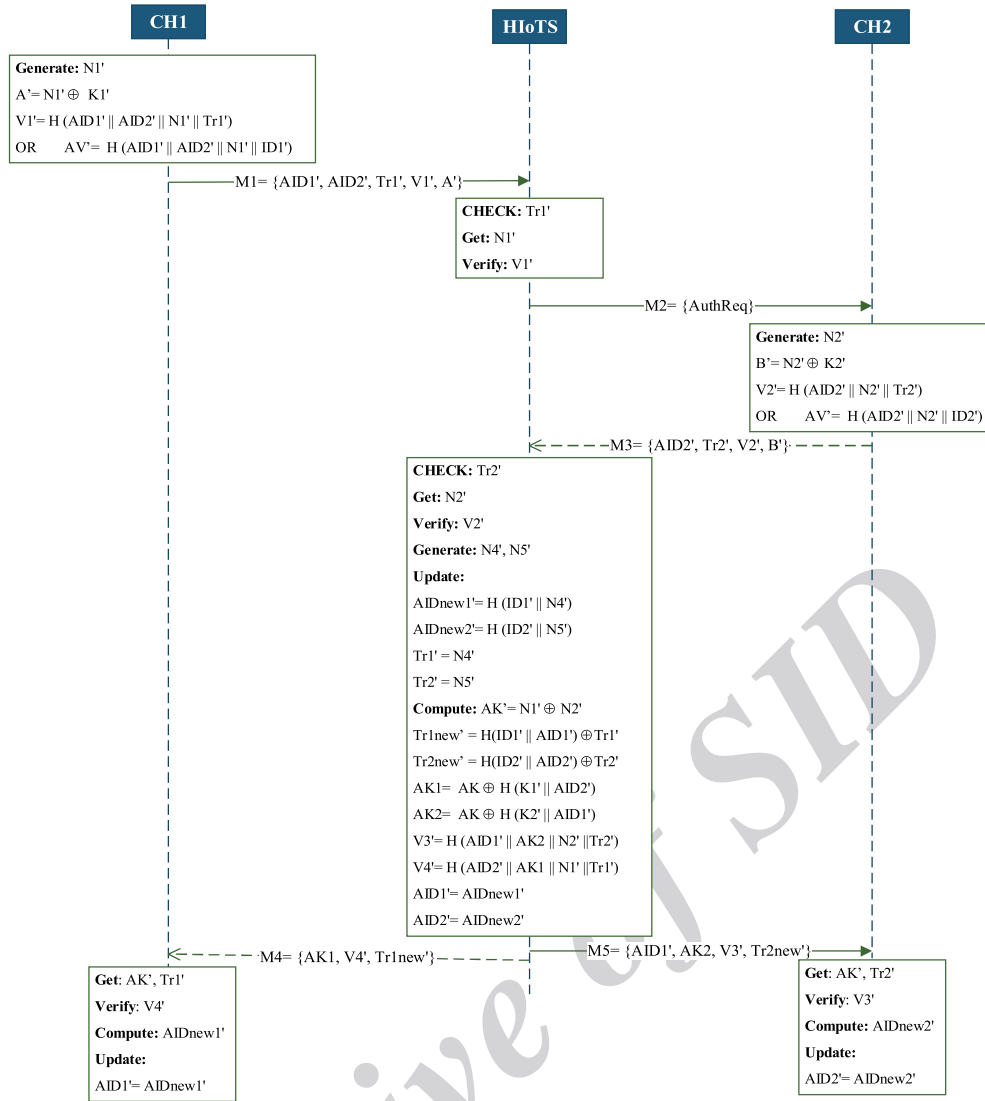


(شکل-۳): احراز اصالت بین دو حس گر موجود در سرخوشه یکسان
(Figure-3): Authentication between two sensors in the same cluster head

از آن کلید جهت برقراری ارتباط استفاده کنند. به عبارت دیگر، برای احراز اصالت موجودیتها از روش سلسه مراتبی استفاده شده است. حس گرها برای احراز اصالت به CH و CHها به شکل (۴) رجوع می کنند. شکل (۴) احراز اصالت بین دو CH و شکل (۵) احراز اصالت بین دو حس گر در CHهای مختلف را نشان می دهد. روند احراز اصالت در شکل (۴) همانند شکل (۳) است، به همین دلیل دوباره آن را تشریح نمی کنیم. از طرفی بسیاری از گامهای شکل (۵) مشابه احراز اصالت حس گرهای موجود در CH یکسان است، به همین سبب تفاوت های این دو پروتکل در ادامه توضیح داده می شوند:

احراز اصالت بین دو حس گر در CHهای متفاوت:

هنگامی که دو حس گر در CHهای متفاوتی قرار دارند، احراز اصالت با کمک هر دو CH انجام می شود. SN1 درخواست خود را به CH مربوط به خودش ارسال می کند؛ چون مقدار AID مقصد را ندارد، مقادیر را برای CH2 می فرستد؛ CH2 نیز با حس گر مورد نظر ارتباط برقرار می کند. درواقع ارتباط بین حس گرها از طریق CHها میسر می شود. نکته حائز اهمیت این است که CHها برای احراز اصالت یکدیگر به موجودیت بالادستی یا همان HIoTS رجوع می کنند و در نهایت کلیدی بین آنها برقرار می شود تا هر زمان که لازم شد

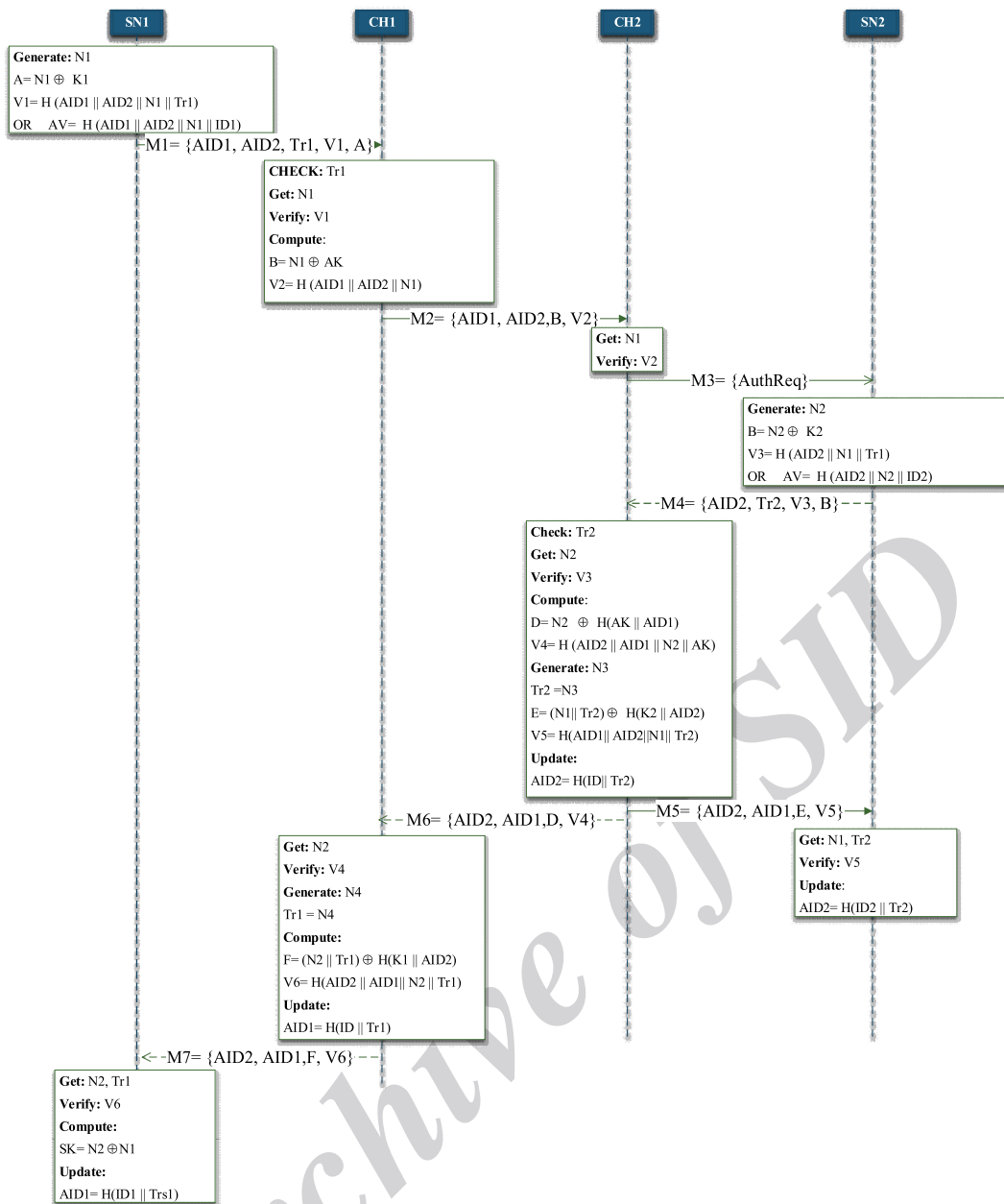


(شکل-۴): احراز اصالت بین دو سرخوشه

(Figure-4): Authentication between cluster heads

گام ۱: همانند گام ۱ در شکل (۳) انجام می‌شود.
 گام ۲: CH1 پس از دریافت پیام $M1$ از حس‌گر $SN1$ ، آن را احراز اصالت و سپس دو رابطه $B = N1 \oplus AK$ و $V2 = H(AID1 || AID2 || N1)$ را تولید و پیام $M2 = \{AID1, AID2, B, V2\}$ را برای CH مقصد ارسال می‌کند.
 گام ۳: CH مقصد در ابتدا مقدار $N1$ را به دست می‌آورد و سپس از SN مورد نظر می‌خواهد که اطلاعاتش را برای CH ارسال کند.
 گام ۴: این مرحله همانند گام ۱ انجام می‌شود.
 گام ۵: CH2 ابتدا $SN2$ را احراز اصالت می‌کند و مقدار $N2$ را محاسبه و سپس مقادیر $E = (N1 || Tr2) \oplus H(K2 || AID2)$ و $V5 = H(AID1 || AID2 || N1 || Tr2)$ را برای $SN2$ ارسال می‌کند.

گام ۶: $SN2$ مقدار $N1$ و $Tr2$ را محاسبه و مقدار $AID2$ را به‌روزرسانی می‌کند. درنهایت مقدار کلید نشست برای این ارتباط محاسبه می‌شود.
 گام ۷: در این مرحله مقدار $N2$ ترکیب‌شده با AK و $V4$ تولیدشده توسط CH2، برای CH1 ارسال می‌شود.
 گام ۸: CH1 با دریافت پیام $M3 = \{AID2, Tr2, V2, B\}$ در ابتدا مقدار $N2$ را به دست می‌آورد و سپس مقدارهای $Tr1$ و $AID1$ را به‌روزرسانی می‌کند. درنهایت پیام $M4 = \{AK1, V4', Tr1new'\}$ برای $SN1$ ارسال می‌شود.
 گام ۹: $SN1$ مقدار $N2$ و $Tr1$ را محاسبه و مقدار $AID1$ را به‌روزرسانی می‌کند. هم‌چنین با به‌دست‌آوردن $N2$ می‌تواند کلید نشست SK را نیز محاسبه کند.



(شکل-۵): احراز اصالت بین دو حسگر در سرخوشه‌های متفاوت
(Figure-5): Authentication between two sensors in the same cluster head

پروتکل‌های پیشنهادی مجموعه‌ای از نیازمندی‌های مطرح شده در حوزه IoT و احراز اصالت را در بر می‌گیرند. این نیازمندی‌ها عبارتند از: احراز اصالت دوطرفه، گمنامی، قابلیت عدم ردیابی، مقیاس‌پذیری، توافق کلید منصفانه، دسترس‌پذیری و سبک وزنی. همان‌طور که در جدول (۲) مشخص است، طرح پیشنهادی به‌گونه‌ای طراحی شده که تمامی نیازمندی‌های امنیتی یادشده را پوشش دهد. این نیازمندی‌ها در طرح [17] و همکاران نیز برقرار هستند؛ اما براساس جدول (۴)، بار محاسباتی و در نتیجه زمان اجرای پروتکل [17] در مقایسه با پروتکل پیشنهادی بیشتر شده است.

ذکر این نکته ضروری است که در پروتکل پیشنهادی، طول عمری برای کلید در نظر گرفته می‌شود، تا زمانی که این محدوده به پایان نرسیده باشد، موجودیت می‌تواند از طریق کلید، خود را برای موجودیت مقابلش احراز اصالت کند؛ اما در صورت اتمام طول عمر، ارتباط بایستی دوباره از مرحله ثبت نام آغاز شود. به عبارت دیگر طرح ابطال کلید برحسب طول عمر کلید است.

۴- تحلیل

۴-۱- برآورده ساختن نیازمندی‌های امنیتی

دسترس پذیری	توافق کلید منصفانه	مقیاس پذیری	قابلیت عدم ردیابی	گمنامی	احراز اصالت دوطرفه	
✓	✓	✓	×	×	✓	[14]
✓	✓	✓	✓	✓	✓	[17]
✓	×	×	✓	✓	✓	[15]
✓	×	✓	✓	✓	✓	[16]
✓	✓	✓	×	×	✓	[12]
✓	✓	✓	✓	✓	✓	طرح پیشنهادی

حمله ناهم‌زمانی^۴ یا حمله انکار سرویس^۵ را افزایش می‌دهد و به‌طور کلی دسترس‌پذیری فرآیند احراز اصالت را مورد تهدید قرار می‌دهد. در پروتکل پیشنهادی برای جلوگیری از این حملات عبارت AV تولید شده است. در این عبارت به جای Tr از ID حس‌گر استفاده شده است تا اگر چنین حملاتی رخ داد، به جای V1، عبارت AV ارسال شود. به همین دلیل دسترس‌پذیری در این پروتکل برقرار شده است.

سبک وزنی: با توجه به این که حس‌گرها محدودیت‌های محاسباتی و پردازشی دارند، برای احراز اصالت فقط از تابع چکیده‌ساز و عمل‌گرهای یای انحصاری و الحاق استفاده شده است تا نسبت به سایر روش‌ها و توابع رمزنگاری، راه‌حل سبک‌تری ارائه شود. هم‌چنین در بخش ۳-۴ بار محاسباتی پروتکل پیشنهادی با سایر طرح‌ها مقایسه خواهد شد تا سبک وزنی آن به‌صورت کمی نیز تضمین شود.

۲-۴- مقابله با حملات مختلف

در این بخش، انواع حملات مختلف را نام برده و دلیل مقاومت پروتکل پیشنهادی در مقابل این حملات را بیان می‌کنیم.

حمله جعل هویت: در پروتکل پیشنهادی، فقط حس‌گر قانونی می‌تواند پیام M1 یا M3 را برای CH ارسال کند. چون این پیام‌ها شامل Tri مخفی بین حس‌گر و CH، N1 (یا N2) ترکیب‌شده با کلید مشترک بین حس‌گر و CH هستند. به همین جهت، مهاجم برای محاسبه این پیام‌ها نیاز دارد تا مقدار کلید مشترک بین حس‌گر و CH را داشته باشد. به‌طور مشابه، فقط CH قانونی می‌تواند پیام‌های M4 و M5 را تولید کند؛ چون این پیام‌ها نیز وابسته به کلید مشترک بین حس‌گر و CH هستند. به همین علت، پروتکل در مقابله با حمله جعل هویت مقاوم است.

حمله تکرار: فرض کنید مهاجم پیام M1 را ضبط کرده و بعدها دوباره برای CH ارسال می‌کند. با توجه به این که CH در همان ابتدا مقدار Tr1 را بررسی می‌کند، در صورت تکرار، این حمله کشف می‌شود. روال مشابهی برای پیام M3 نیز رخ می‌دهد؛ زیرا CH بلافاصله بعد از دریافت آن، مقدار Tr2 را تطبیق می‌دهد. هم‌چنین اگر پیام‌های M4 و M5 توسط مهاجم دوباره برای حس‌گرها ارسال شوند، به‌دلیل وجود مقدار تصادفی N1 و N2، مقدار عبارت‌های V4 و V3 دریافتی با مقدار محاسبه‌شده متفاوت خواهد بود و حمله تکرار کشف خواهد شد.

حمله مرد میانی: با توجه به عبارت‌های ارسالی V1 تا V6 در پیام‌های M1 تا M7 و فرآیند احراز اصالت هر یک از

احراز اصالت دوطرفه: برای اثبات احراز اصالت دوطرفه دو حالت موجود است: ارتباط بین حس‌گرها در سرخوشه یکسان و دو سرخوشه متفاوت. این ویژگی به‌طور کامل در تشریح پروتکل مشخص شده است. برای احراز اصالت موجودیت‌ها از عبارت‌های $V_i (i=1, \dots, 6)$ استفاده شده است. **گمنامی:** پروتکل‌های پیشنهادی با استفاده از AID گمنام شده‌اند؛ چون مهاجم نمی‌تواند هویت واقعی حس‌گرها را شناسایی کند.

قابلیت عدم ردیابی: ساختار پویای AID و به‌روزرسانی آن پس از هر ارتباط، باعث می‌شود تا هیچ موجودیتی جز موجودیت قابل اعتماد بالادستی نتواند فعالیت‌های حس‌گر را دنبال کند.

مقیاس‌پذیری: در ابتدا و در تمامی مراحل پروتکل‌های پیشنهادی، مقایسه Tri (Tri') مربوطه با مقدار ذخیره‌شده در پایگاه داده، باعث می‌شود تا بار محاسباتی شبکه با افزایش تعداد موجودیت‌ها، افزایش چشم‌گیری نداشته باشد و در نتیجه نیازی به انجام عملیات سنگین جستجو نخواهد بود. **توافق کلید به‌صورت منصفانه:** در پروتکل پیشنهادی هر دو موجودیت به یک اندازه در تولید کلید سهیم هستند. در نتیجه توافق کلید SK به‌صورت منصفانه انجام شده است تا در مراحل بعد، اطلاعات به‌صورت ایمن بین SNها مبادله شود. **دسترس‌پذیری:** در بسیاری از پروتکل‌های احراز اصالت، یک سری کلید محرمانه بین موجودیت‌ها وجود دارد که بعد از هر بار نشست، به‌روزرسانی می‌شوند. این به‌روزرسانی امکان

⁴ De-synchronization Attack

⁵ Denial of Service Attack

⁶ Man In the Middle

¹ Scalability

² Fair Key Agreement

³ Availability

۴-۴- مقایسه هزینه محاسباتی

حس گرهای قدرت پردازشی و محاسباتی پایینی دارند؛ به همین جهت بایستی هزینه محاسباتی پروتکل پیشنهادی با پروتکل‌های پیشین مقایسه شود (جدول ۴). نمادهای T_{mul} ، T_{inv} ، T_{eca} ، T_{ecm} و T_h به ترتیب نشان‌دهنده زمان اجرای عملیات ضرب پیمانه‌ای، عملیات معکوس ضربی، جمع نقطه‌ای منحنی بیضوی، عملیات ضرب نقطه‌ای منحنی بیضوی و عملیات تابع چکیده‌ساز هستند. زمان اجرای عملیات مختلف براساس ضرب پیمانه‌ای بیان و زمان اجرای پروتکل‌ها به‌طور تقریبی محاسبه می‌شوند.

(جدول ۴): مقایسه بار محاسباتی و زمان اجرای پروتکل‌ها

(Table-4): Comparison of computational cost and protocol time execution

زمان اجرای پروتکل	بار محاسباتی	
$\approx 2406.44T_{mul}$	$2T_{ecc}+T_{+ecc}+2T_H+2T_{MAC}$	[14]
$\approx 4.32T_{mul}$	$12T_H + 6T_{XOR} + 28T_{ }$	[16]
$\approx 6.48T_{mul}$	$18T_H + 11T_{XOR} + 10T_{ }$	[17]
$\approx 7.21T_{mul}$	$20T_H + 30T_{XOR} + 18T_{ }$	[15]
$\approx 5.76T_{mul}$	$16T_H + 9T_{XOR} + 30T_{ }$	طرح پیشنهادی

باتوجه به [18]، $T_{eca} \approx 5T_{mul}$ ، $T_{inv} \approx 3T_{mul}$ ، $T_{ecm} \approx 1200T_{mul}$ و $T_h \approx 0.36T_{mul}$ است. مقایسه پروتکل پیشنهادی با پروتکل‌های مشابه، بیان‌گر این موضوع است که پروتکل پیشنهادی توانسته است با مقدار مناسبی، هزینه محاسباتی و زمان اجرا، ویژگی‌های مختلفی را برآورده ساخته و در مقابل حملات گوناگون مقاوم باشد.

۵- نتیجه‌گیری

اینترنت اشیا مفهوم جدیدی است که در سال‌های اخیر، توجهات بسیاری را به خود جلب کرده است. این‌که تمامی اشیا بتوانند از طریق اینترنت با یکدیگر ارتباط برقرار کنند، مبنای کار این مفهوم است. با افزایش ارتباطات، احراز اصالت به‌عنوان یکی از مسائل کلیدی این حوزه ظاهر می‌شود؛ که به‌علت محدودیت‌های محاسباتی اشیا، بهتر است از راه‌حل‌های سبک و متقارن استفاده شود. از طرفی یکی از مباحث مهم در اینترنت اشیا، مسئله گمنامی است بدین معنا که کاربران و

این عبارات در سمت گیرنده، هرگونه تغییر در داده‌ها توسط فرد میانی، قابل تشخیص خواهد بود. از طرفی تمامی مقادیر موجود در عبارت‌های ارسالی روی خط نیز ارسال می‌شوند که در صورت ایجاد تغییر، در طول فرآیند احراز اصالت این تغییر کشف می‌شود.

حمله استراق سمع: در صورتی که مهاجم پیام‌های ارسالی را شنود کند، به داده‌های حساس و مهم دسترسی پیدا نمی‌کند؛ زیرا این داده‌ها قبل از ارسال با یک مقدار تصادفی ترکیب شده و در عبارت‌های V_1 تا V_4 قرار می‌گیرند تا هم مقدار حقیقی پنهان و هم مقادیر ارسالی به‌صورت تصادفی تولید شود.

حمله انکار سرویس: در صورتی که مهاجم پیام‌ها را شنود کرده و مجموعه‌ای از آنها را دوباره و یکجا برای CH ارسال کند، فقط با بررسی مقدار Tr ، امکان کشف این حمله وجود دارد؛ چون سایر محاسبات اضافی جهت احراز اصالت انجام نمی‌شوند. به همین سبب، امکان جلوگیری از حمله انکار سرویس وجود دارد.

حمله ناهمگام‌سازی: اگر مهاجم بتواند در فرآیندهای به‌روزرسانی مراحل احراز اصالت، خللی وارد کند، احتمال رخداد حمله ناهمگام‌سازی به‌وجود می‌آید. سازوکار لازم برای مقابله با این حمله، استفاده از عبارت AV به جای V_i است. در عبارت AV به جای Tr از ID حس‌گر استفاده می‌شود تا اگر خللی در به‌روزرسانی Tr به‌وجود آمد، حمله ناهمگام‌سازی رخ ندهد.

در جدول (۳) نیز مقاومت پروتکل پیشنهادی با پروتکل‌های پیشین مقایسه شده است. حملات عبارتند از: جعل هویت، تکرار، مرد میانی، استراق سمع، انکار سرویس و ناهمگام‌سازی.

(جدول ۳): مقابله با حملات مختلف

(Table-3): Resistance against attacks

ناهمگام‌سازی	انکار سرویس	استراق سمع	مرد میانی	تکرار	جعل هویت	
✓	✓	×	×	×	✓	[14]
✓	✓	✓	✓	✓	✓	[17]
×	×	✓	×	✓	×	[15]
✓	✓	✓	✓	×	✓	[16]
✓	✓	✓	✓	✓	✓	طرح پیشنهادی

¹ Eavesdropping Attack

and research challenges," *Ad Hoc Networks*, vol. 10, pp. 1497-1516, 2012.

- [2] K. Ashton, "That 'internet of things' thing," *RFID Journal*, vol. 22, pp. 97-114, 2009.
- [3] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*, 2014, pp. 1-8.
- [4] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, pp. 49-69, 2011.
- [5] 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, pp. 2266-2279, 2013.
- [6] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," in *Secure Internet of Things (SIoT), 2015 International Workshop on*, 2015, pp. 49-57.
- [7] J. M. Kizza, "Computer Network Security Protocols," in *Guide to Computer Network Security*, ed: Springer, 2015, pp. 357-386.
- [8] M. R. Kanjee, K. Divi, and H. Liu, "A physiological authentication scheme in secure healthcare sensor networks," in *Sensor Mesh and Ad Hoc Communications and Networks (SECON), 2010 7th Annual IEEE Communications Society Conference on*, 2010, pp. 1-3.
- [9] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, and G. Carle, "A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication," in *Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on*, 2012, pp. 956-963.
- [10] M. Hernandez-Goya and P. Caballero-Gil, "Analysis of Lightweight Cryptographic Solutions for Authentication in IoT," in *International Conference on Computer Aided Systems Theory*, 2013, pp. 373-380.
- [11] S. Janbabaei, H. Gharaee, and N. Mohammadzadeh, "Lightweight, anonymous and mutual authentication in IoT infrastructure," in *Telecommunications (IST), 2016 8th International Symposium on*, 2016, pp. 162-166.
- [12] D. A. Ha, K. T. Nguyen, and J. K. Zao, "Efficient authentication of resource-constrained IoT devices based on ECQV implicit certificates and datagram transport layer security protocol," in *Proceedings of the Seventh Symposium on Information and Communication Technology*, 2016, pp. 173-179.

موجودیت‌های شبکه، تمایلی به شناخته‌شدن در شبکه ندارند و ترجیح می‌دهند به‌صورت گمنام ارتباطات خود را با سایر موجودیت‌ها حفظ کنند. با بررسی پژوهش‌های پیشین و تحلیل آسیب‌پذیری‌ها و مشکلات آنها، مشاهده شد که بیش‌تر پروتکل‌های احراز اصالت، پارامترهای مهم در این حوزه را یکجا لحاظ نکرده‌اند. برخی، از گواهی‌نامه‌های استاندارد، از جمله گواهی‌نامه X.509 و کلید عمومی RSA استفاده کرده‌اند که برای حس‌گرهایی با قدرت محاسباتی پایین و منابع محدود، بیش از حد سنگین است؛ برخی، بیش‌تر روی گمنامی توجه داشته و از رمزنگاری‌هایی مانند رمزنگاری خم بیضوی استفاده کرده‌اند، اما همچنان مشکل سنگینی پروتکل پابرجا بوده است. برخی دیگر بیشتر روی سبک وزنی تمرکز کرده و به‌جای استفاده از توابع رمزنگاری، از تابع چکیده‌ساز و عملگرهای منطقی ساده بهره برده‌اند؛ اما این پروتکل‌ها نیز در مقابل حملات خاصی آسیب‌پذیر بوده‌اند. از طرفی، هر یک از این پژوهش‌ها، بخشی از نیازمندی‌های امنیتی محیط اینترنت اشیا را در نظر گرفته‌اند و موفق به جلوگیری از برخی حملات خاص نشده‌اند. علاوه‌براین بسیاری از پروتکل‌های ارائه‌شده، تنها ارتباط یک موجودیت با موجودیت بالادستی را در نظر گرفته‌اند؛ درحالی‌که بررسی ارتباط بین موجودیت‌ها نیز امری ضروری به‌نظر می‌رسد.

لذا بر آن شدیم تا پروتکل احراز اصالتی به‌صورت سلسله‌مراتبی بین موجودیت‌ها در خوشه یکسان و دو خوشه متفاوت ارائه کنیم که ضمن برآورد ساختن نیازمندی‌های امنیتی لازم، از جمله گمنامی، قابلیت عدم ردیابی و سبک‌وزنی، تا حد ممکن نیز نسبت به حملات مقاوم باشد. در طراحی این پروتکل از تابع چکیده‌ساز و عملگرهای منطقی یای انحصاری و الحاق استفاده شده است. در ادامه، پروتکل پیشنهادی از چند منظر مورد تحلیل واقع شد. بدین صورت که ابتدا نیازمندی‌های امنیتی پروتکل‌ها با یکدیگر مقایسه شده و سپس ارزیابی مناسبی از مقاومت آنها در برابر حملات گوناگون ارائه شد. درنهایت، هزینه محاسباتی مبتنی بر عمل ضرب پیمانه‌ای برآورد و تخمین زده شد. با توجه به مقایسه‌ها، به این نتیجه رسیدیم که پروتکل پیشنهادی با حفظ سبک‌وزنی توانسته ویژگی‌های مختلفی را پوشش دهد و با حملات مختلف مقابله کند.

6- References

۶- مراجع

- [1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications

عضو هیئت علمی مرکز تحقیقات مخابرات است و زمینه‌های پژوهشی مورد علاقه ایشان طراحی مدارات VLSI دیجیتال، آنالوگ و سیگنال مختلط، پردازش سیگنال‌های دیجیتال، سامانه‌های تشخیص و پیش‌گیری از نفوذ، مرکز عملیات امنیت و اجزای آن و مراکز اشتراک‌گذاری و تحلیل اطلاعات است.

نشانی رایانامه ایشان عبارت است از:

gharaee@itrc.ac.ir



ناصر محمدزاده تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی کامپیوتر در دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف به ترتیب در سال‌های ۱۳۸۲ و ۱۳۸۴ به اتمام

رسانید. او مقطع دکترای مهندسی کامپیوتر را در دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی امیرکبیر در سال ۱۳۸۹ تکمیل کرد. از سال ۱۳۹۰ تاکنون عضو هیأت علمی دانشگاه شاهد و زمینه‌های پژوهشی مورد علاقه ایشان محاسبات کوانتومی، طراحی مدارات VLSI دیجیتال، پردازش سیگنال‌های دیجیتال، سامانه‌های تشخیص و پیش‌گیری از نفوذ است.

نشانی رایانامه ایشان عبارت است از:

mohammadzadeh@shahed.ac.ir

- [13] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*, 2014, pp. 2728-2733.
- [14] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.
- [15] K. Srivastava, A. K. Awasthi, S. D. Kaul, and R. Mittal, "A hash based mutual RFID tag authentication protocol in telecare medicine information system," *Journal of medical systems*, vol. 39, p. 153, 2015.
- [16] P. Gope and T. Hwang, "Untraceable sensor movement in distributed IoT infrastructure," *Sensors Journal, IEEE*, vol. 15, pp. 5340-5348, 2015.
- [17] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *Systems Journal, IEEE*, vol. 8, pp. 749-758, 2014.
- [18] 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, pp. 72-83, 2015.



شادی جانبابائی تحصیلات خود را در مقطع کارشناسی رشته مهندسی فناوری اطلاعات در دانشگاه صنعتی ارومیه در سال ۱۳۹۱ به اتمام رساند و مدرک کارشناسی ارشد خود را در رشته مهندسی فناوری اطلاعات گرایش امنیت اطلاعات از دانشگاه شاهد تهران در سال ۱۳۹۵ اخذ کرد. نشانی رایانامه ایشان عبارت است از:

sh_janbabaei@yahoo.com



حسین قرانی تحصیلات خود را در مقطع کارشناسی مهندسی برق-الکترونیک در دانشکده مهندسی برق دانشگاه خواجه نصیرالدین طوسی در سال ۱۳۷۷ به اتمام رسانید. مقاطع

کارشناسی ارشد و دکترای مهندسی برق - الکترونیک را در دانشکده مهندسی برق دانشگاه تربیت مدرس به ترتیب در سال‌های ۱۳۷۹ و ۱۳۸۸ تکمیل کرد. از سال ۱۳۸۱ تاکنون