

# ارائه طرح احراز اصالت سبک با قابلیت گمنامی و

## اعتماد در اینترنت اشیا

شادی جانبایی<sup>۱</sup>, حسین قرائی<sup>۲\*</sup> و ناصر محمدزاده<sup>۳</sup>

<sup>۱</sup> دانشکده فنی مهندسی، گروه مهندسی کامپیوتر، دانشگاه شاهد تهران

<sup>۲</sup> پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران)

### چکیده

اینترنت اشیا مفهوم جدیدی است که باعث حضور حس‌گرها در زندگی انسان شده است؛ به طوری که تمامی اطلاعات توسط همین حس‌گرها جمع آوری، پردازش و منتقل می‌شوند. برای برقراری یک ارتباط امن، با افزایش تعداد حس‌گرها، 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 پروتکل‌های احراز اصالت در حوزه اینترنت اشیا بررسی شده و محدودیت‌ها و آسیب‌پذیری‌های امنیتی آنها مورد تحلیل واقع شده‌اند. هم‌چنین پروتکل احراز اصالت جدیدی پیشنهاد می‌شود که گمنامی به عنوان یک پارامتر مهم، در آن لحاظ می‌شود. از طرفی تابع چکیده‌ساز و عمل‌گرهای منطقی نیز مورد استفاده قرار می‌گیرند تا هم پروتکل سبک باشد و هم حس‌گرها بتوانند به عنوان موجودیت‌هایی محدود از لحاظ محاسباتی، از آنها استفاده کنند. در این پروتکل نیازمندی‌های امنیتی از قبیل قابلیت عدم ردیابی، مقیاس‌پذیری، دسترس‌پذیری و غیره لحاظ شده‌اند 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 Janbabaei<sup>1</sup>, Hossein Gharaee<sup>\*2</sup> & Naser Mohammadzadeh<sup>3</sup>

<sup>1,3</sup>Department of Computer Engineering, Shahed University, Tehran, Iran

<sup>2</sup>Department 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 عهده‌دار مکاتبات • تاریخ ارسال مقاله: ۱۳۹۶/۷/۱۴ • تاریخ آخرین بازنگری: ۱۳۹۷/۵/۱۵ • تاریخ پذیرش: ۱۳۹۷/۵/۷



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 HIoTS 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<sup>۴</sup> و توزیع شده<sup>۵</sup>. 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 توزیع شده، نه تنها هوشمندی و ارائه خدمات در لیبه‌های شبکه قرار می‌گیرند، بلکه پلتفرم‌های مختلف نرم‌افزاری نیز می‌توانند با یکدیگر به صورت پویا همکاری کنند [5].

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

<sup>4</sup>Centralized

<sup>5</sup>Distributed

<sup>6</sup>Uncontrolled environment

<sup>7</sup>Heterogeneity

<sup>8</sup>Scalability

<sup>9</sup>Network Security

<sup>10</sup>Identity Management

<sup>11</sup>Trust

<sup>12</sup>Resilience

<sup>13</sup>Authentication

<sup>14</sup>Anonymity

## ۱- مقدمه

امروزه حدود دو میلیارد نفر در سراسر جهان برای دریافت خدماتی مانند وب‌گردی، ارسال و دریافت رایانامه، دستیابی به محظوظ 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 بهره بزنند، جهش بزرگ دیگری در حال وقوع است که در آن استفاده از اینترنت به عنوان 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/شتون در سال ۱۹۹۰ مورد استفاده نهاده و اینترنت اشیا 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 اینترنات، فراهم می‌شود. بیش از پنجاه درصد اتصالات اینترنت، اشیا هستند، که در سال ۲۰۱۱ تعداد آن‌ها بیش از پانزده بیلیون تخمین زده شد و پیش‌بینی می‌شود که تا سال ۲۰۲۰ به سی بیلیون 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

<sup>1</sup>Internet of Things

<sup>2</sup>Radio Frequency Identification

<sup>3</sup>Wireless Sensor Networks

امنیتی دیگری بر اساس گواهی نامه ضمی <sup>۳</sup> ECQV و DTLS برای اینترنت اشیا طراحی و پیاده‌سازی شد [12]. در مرحله ثبت نام این پروتکل، تمامی دستگاه‌ها گواهی ضمی خود را از CA دریافت می‌کنند. اجرای طرح تولید گواهی ضمی از طریق پروتکل دست‌تکانی، نقطه قوت این مرحله است. در مرحله برقراری کلید امن، الگوریتم تبادل کلید <sup>۴</sup> ECDH و گواهی ضمی ECQV ترکیب می‌شوند تا طرح ارائه شده، برقراری کلید و احراز اصالت را توأمًا برقرار کند. ساختار و محتوای پیام‌ها به‌طور دقیق همانند 1.2 DTLS است؛ با این تفاوت که به جای گواهی X.509 از گواهی ضمی 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 به جای استفاده از RSA، از ECC و یک کلید مشترک از پیش‌تعیین شده 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 سرخوش‌ها 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 یا انحصاری و الحق 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 سور اتفاق می‌افتد و پروتکل در مقابل حمله جعل <sup>۵</sup> آسیب‌پذیر است. در طرح [16] پروتکل احراز اصالت دیگری به همراه 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 گرهات انتهایی توسط یکدیگر و آسیب‌پذیری در مقابل حمله تکرار <sup>۶</sup> اشاره کرد. در [17]، طرح احراز اصالت گرهات انتهایی با قابلیت اعتماد توسعه یافته در شبکه‌های موردنی خود را پیشنهاد شده است. در این پروتکل علاوه بر استفاده از تابع چکیده‌ساز، عمل‌گرهای یا انحصاری و الحق، 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 جانبی 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 در این حوزه وجود دارد، اما می‌توان برخی مسائل عمومی را به عنوان قاعدة کلی در طراحی این نوع پروتکل‌ها برقرار کرد. نخست، باید گام‌های محاسباتی و هزینه‌ها را به منظور صرفه‌جویی در انرژی به کمینه رساند؛ علاوه بر این، به منظور توزیع بار محاسباتی میان گرهات، 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 دو طرفه 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 انتهایی برای احراز اصالت دومرحله‌ای مبتنی بر DTLS پیشنهاد شده است. در این طرح، گرهاتی که می‌خواهند به شبکه متصل شوند، با توجه به قابلیت‌هایشان، مجموعه رمزگاری مناسب خود را انتخاب می‌کنند؛ اما با توجه به این که هشت پیام برای دست‌تکانی استفاده می‌شود، سریار قابل توجهی به وجود می‌آید. از طرفی استفاده از گواهی نامه‌های 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 <sup>۷</sup> در آن لحاظ نشده است. از طرفی در هر دو مرحله، طرفین ارتباط جهت برقراری یک‌پارچگی، نیاز به یک کلید مخفی خواهند داشت. در سال ۲۰۱۶، یک طرح

<sup>3</sup> Elliptic Curve Qu-Vanstone

<sup>4</sup> Elliptic curve Diffie–Hellman

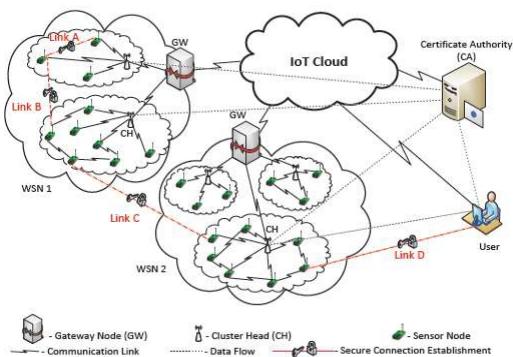
<sup>5</sup> Impersonating Attack

<sup>6</sup> Replay Attack

<sup>1</sup> Datagram Transport Layer Security

<sup>2</sup> Untraceability

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



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

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

نماد	توضیحات
SN <sub>i</sub>	گره حسگر آم
Chi	سرخوش آم
HIoTS	سور اصلی
IDi/ IDi'	شناسه حقیقی گره حسگر (سرخوش)
IDh	شناسه حقیقی سور اصلی
Ni/Ni'	اعداد تصادفی تولید شده در احراز اصالت دو حسگر (دو سرخوش)
Ki/ Ki'	کلید مشترک تعییه شده بین سرخوش و حسگر آم (بین سور و سرخوش آم)
AIDi/ AIDi'	شناسه غیرحقیقی و مستعار یکبار مصرف برای حسگر (سرخوش) آم
Tri/ Tri'	شماره تصادفی تولید شده برای بررسی تازگی پیام بین سرخوش و حسگر (سرور)
Vi/Vi'	عبارت‌هایی جهت ارزیابی پیام دریافتی
SK	کلید نشست تعیین شده در انتهای پروتکل بین دو حسگر
SKi	کلید ارسالی برای حسگر آم جهت دست‌یابی به SK
AK	کلید توافق شده بین دو سرخوش
H(.)	تابع چکیده‌ساز یک‌طرفه - تابع Hash
⊕	XOR عملگر
	عملگر الحق

مجدد در ارتباط امن بین موجودیت‌ها شکاف وجود دارد. از طرفی کل ارتباطات به یک کلید از پیش تعیین شده 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 رمزگاری RSA جهت احراز اصالت استفاده می‌شود، در حالی که امروزه به دلیل سربار محاسباتی بالا و سنگین‌بودن آن، این روش کمتر مورد توجه قرار می‌گیرد؛ سپس ECC به عنوان رمزگاری سبک‌تر نسب به RSA مطرح شده که این رمزگاری نیز برای دستگاه‌های محدود از نظر محاسباتی و پردازشی، همچنان سنگین است. در همین‌واخر توابع چکیده‌ساز و عملگرهای منطقی بیشتر مورد توجه قرار می‌گیرند، تا سبک وزنی به عنوان یکی از پارامترهای مهم برقرار شود. همچنین بسیاری از پروتکلهای ارائه شده فقط ارتباط هر موجودیت را با موجودیت بالادستی در نظر می‌گیرند؛ در حالی که ارتباط بین موجودیت‌ها با یکدیگر نیز ضروری است [11].

### ۳-۱-۳- مدل پیشنهادی

#### ۱-۳-۱- معماری مفروض

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

#### ۲-۳- طرح پیشنهادی

در تدوین این پروتکل، تلاش شده است سه رویکرد اصلی، پوشش شناسه حقیقی، تولید کلید نشست و فرآیند به روزرسانی پس از فرآیند احراز اصالت را لحظه 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 SNs هاستند که توان محاسباتی پایینی دارند و موجودیت‌های قوی HIoTS و CHها هستند که می‌توانند سربار محاسباتی بالایی را تحمل کرده و پردازش‌های سنگینی را انجام دهند.



موجودیت قابل اعتماد وارد عمل می شود و احراز اصالت بین دو حسگر را میسر می سازد. تعاملات بین حسگرهای در شکل (۳) نشان داده شده است. در ادامه این تعاملات را به تفصیل بیان می کنیم:

گام ۱: حسگر SN1 مقدار تصادفی N1 را تولید کرده و دو رابطه K1 و  $A=N1 \oplus AID2 \parallel N1$  و  $V1=H(AID1 \parallel AID2 \parallel N1 \parallel Tr1)$  را محاسبه می کند. عبارت V1 جهت ارزیابی M1 را می محاسبه می کند. در پایان گام ۱، پیام  $\{AID1, AID2, Tr1, V1, A\}$  از طریق یک کانال نامن برای CH ارسال می شود.

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 محسوب شده را با V1 دریافتی مقایسه می کند. در صورت برابر بودن این دو مقدار، SN1 برای CH احراز اصالت می شود. در صورت معتبر بودن این ارزیابی، CH از حسگری با AID2 درخواست می کند تا اطلاعات خود را جهت احراز اصالت برای CH ارسال کند. این درخواست توسط پیام  $\{AuthReq\}$  فرستاده می شود.

گام ۳: حسگر دوم با دریافت پیام M2، همانند حسگر نخست مقادیر لازم را تولید و برای CH ارسال می کند با این تفاوت که از AID حسگر نخست مطلع نیست! پیام  $\{AID2, Tr2, V2, B\}$  برای CH ارسال می شود.

گام ۴: در ابتدا، CH همانند گام ۲ عمل می کند و سپس مقادیر Tr و AID مربوط به هر دو حسگر را به روزرسانی و درنهایت CH کلید نشست بین این دو حسگر را از طریق رابطه SK =  $N1 \oplus N2$  محاسبه می کند. حال برای ارسال کلید نشست و مقدار Tr به روز شده، بایستی از دو عبارت SK2 =  $(Tr2 \parallel SK1) \oplus H(K1 \parallel AID2)$  و SK1 =  $(Tr1 \parallel SK) \oplus H(K2 \parallel AID1)$  استفاده شود. از طرفی دو Rابطه V4 =  $H(AID1 \parallel SK2 \parallel N2 \parallel Tr2)$  و V3 =  $H(AID1 \parallel SK1 \parallel N1 \parallel Tr1)$  نیز برای ارزیابی سمت گیرنده، تولید شده و روی خط ارسال می شوند. در انتهای این گام، دو پیام  $\{SK1, V4, Tr1\}$  و  $\{SK2, V3, Tr2\}$  به ترتیب برای حسگر نخست و حسگر دوم ارسال می شود.

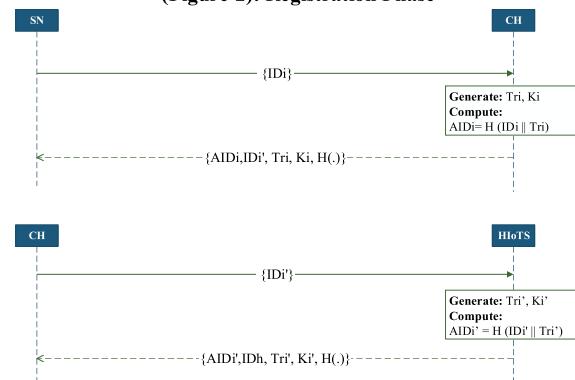
گام ۵: هریک از حسگرهای مقدار کلید نشست و Tr به روزرسانی شده را با استفاده از SK1 و V4 (یا SK2 و V3) به ترتیب برای حسگر نخست و حسگر دوم ارسال می شود.

### ۳-۲-۱- مرحله ثبت نام

در این مرحله گرهای حسگر، شناسه حقیقی خود را از طریق یک کانال ارتباطی امن برای سرخوشی ارسال می کنند؛ سپس سرخوشی دو مقدار تصادفی Trseq و K را تولید کرده و مقدار شناسه غیر حقیقی مستعاری (AIDI) را برای حسگر محاسبه می کند تا از طریق همان کانال به حسگر منتقل شود. این مقادیر در پایگاه داده خود سرخوشی نیز ذخیره خواهد شد تا در مراحل احراز هویت، مقادیر آنها مورد بررسی قرار گیرد. همچنین همین فرآیند برای ثبت نام سرخوشی ها در HIoTS نیز تکرار خواهد شد تا تمامی موجودیت ها در شبکه و توسط نهاد مرتبه بالاتر ثبت نام شوند. ذکر این نکته ضروری است که در پروتکل پیشنهادی، توزیع کلید به صورت سلسه مراتبی است بدین صورت که حسگرهای نیازی به ثبت نام در HIoTS نخواهند داشت و هر CH به طور مستقیم وظیفه ثبت نام حسگرهای 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



### ۳-۲-۲- مرحله احراز اصالت

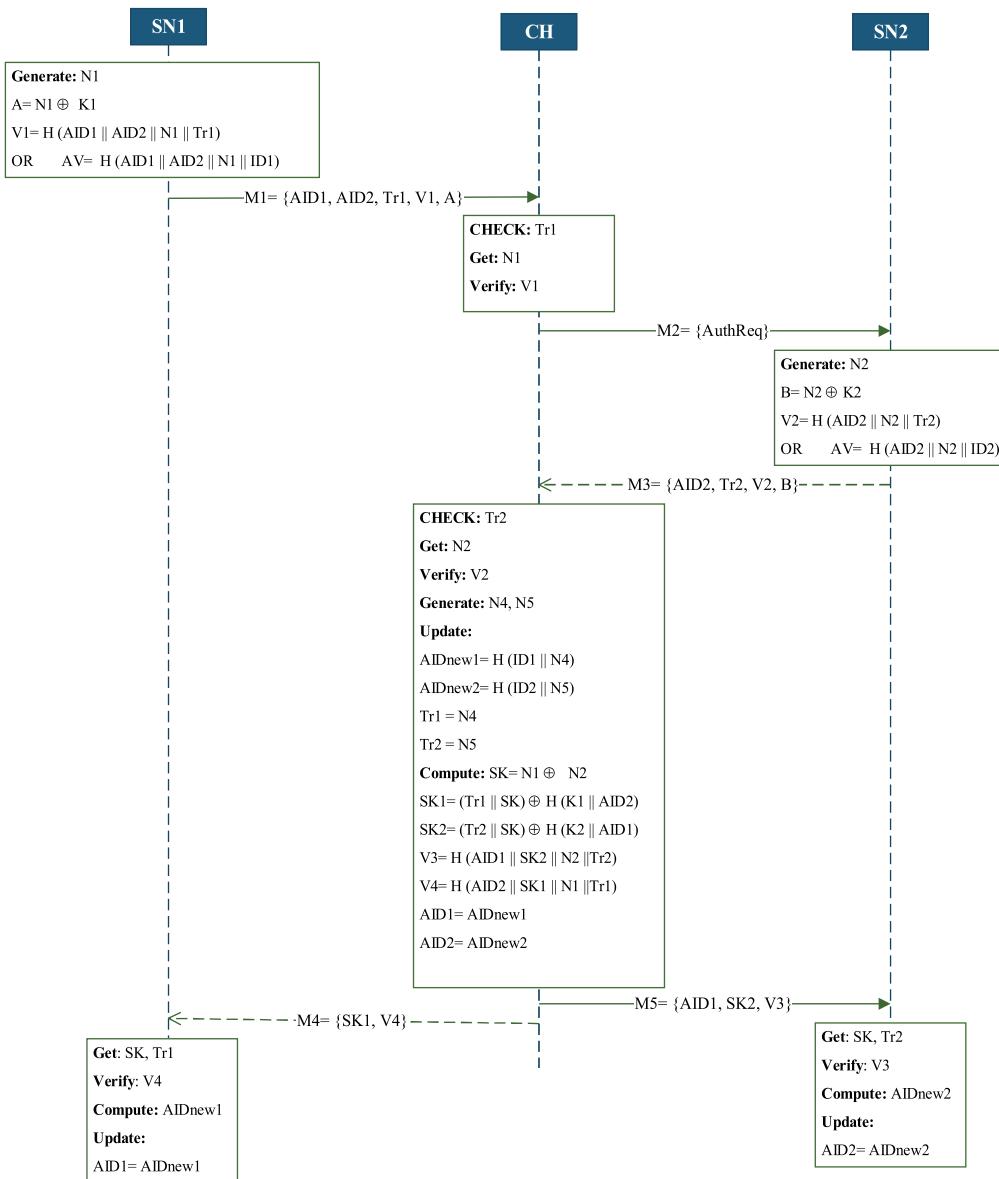
در این مرحله، دو گره حسگر می خواهند به صورت گمنام یکدیگر را احراز اصالت کرده و در انتها کلید نشستی با یکدیگر برقرار و از طریق آن کلید، داده هایی را باهم مبادله کنند. تعاملات بین این دو حسگر باتوجه به موقعیت آنها به دو دسته طبقه بندی می شود: دو حسگر در CH یکسان و دو حسگر در دو CH متفاوت. با این حال برای احراز اصالت دو حسگر در CH های متفاوت، نیاز به احراز اصالتها توسط HIoTS نیز خواهیم داشت.

#### احراز اصالت بین دو حسگر در CH یکسان:

هنگامی که دو حسگر در CH یکسانی واقع شده اند، برای احراز اصالت یکدیگر از CH کمک می گیرند، چون CH به عنوان

AID2 = H (ID2 || N5) و (ID1 || N4) به روزرسانی شوند.

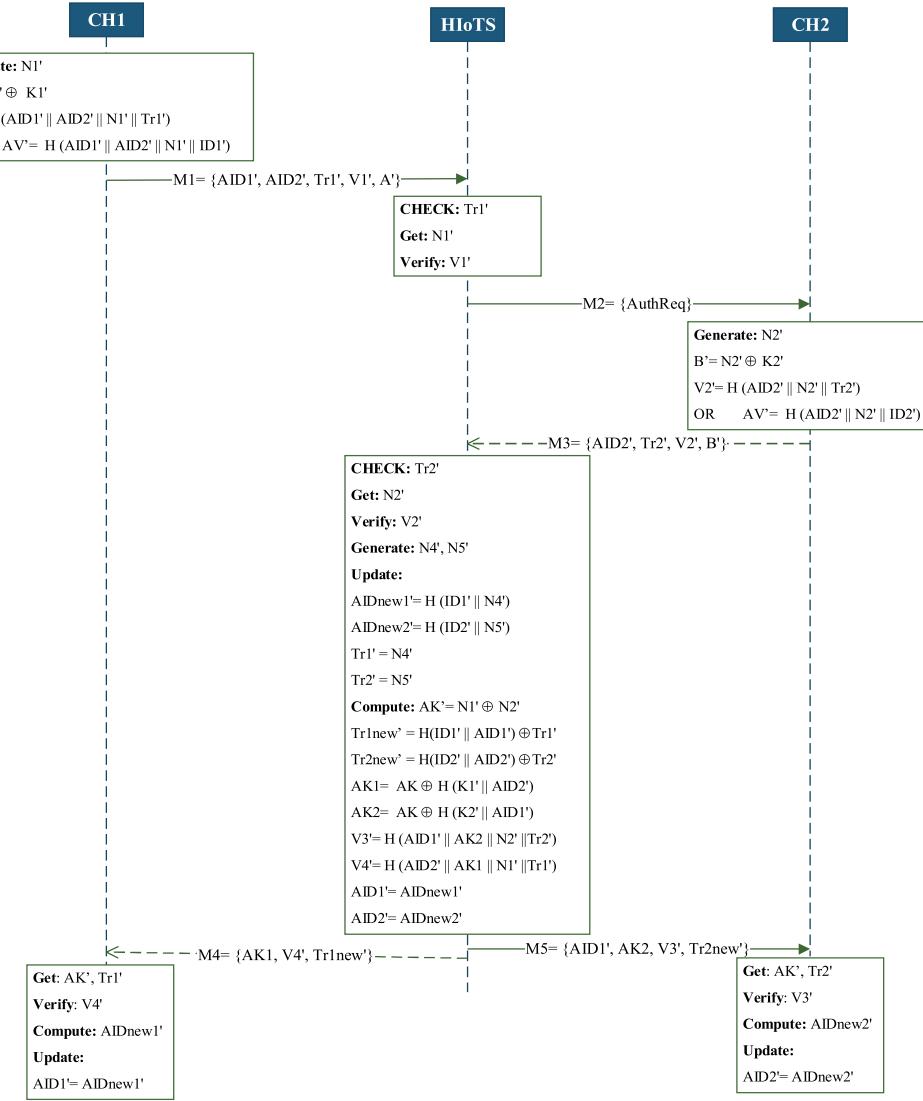
و V3) دریافتی به دست آورده و ارزیابی می‌کنند. در انتها با استی مقادیر AID ها از طریق روابط



(شکل-۳): احراز اصالت بین دو حسگر موجود در سرخوشة 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 سلسه‌مراتبی استفاده شده است. حسگرهای برای احراز اصالت به CH و CHها به شکل (۴) احراز اصالت بین دو حسگر در CHها مختلف را نشان می‌دهد. روند احراز اصالت در شکل (۴) همانند شکل (۳) است، به همین دلیل دوباره آن را تشریح نمی‌کنیم. از طرفی بسیاری از گام‌های شکل (۵) مشابه احراز اصالت حسگرهای موجود در CH یکسان است، به همین سبب تفاوت‌های این دو پروتکل در ادامه توضیح داده می‌شوند:

احراز اصالت بین دو حسگر در CHها متفاوت: هنگامی که دو حسگر در CHها متفاوتی قرار دارند، احراز اصالت با کمک هر دو CH انجام می‌شود. SN1 در خواست خود را به CH مربوط به خودش ارسال می‌کند؛ CH1 چون مقدار AID مقصد را ندارد، مقادیر را برای CH می‌فرستد؛ CH2 نیز با حسگر مورد نظر ارتباط برقرار می‌کند. درواقع ارتباط بین حسگرهای از طریق CHها میسر می‌شود. نکته حائز اهمیت این است که CHها برای احراز اصالت یکدیگر به موجودیت بالادستی یا همان HIoTS رجوع می‌کنند و درنهایت کلیدی بین آنها برقرار می‌شود تا هر زمان که لازم شد



(شکل-۴): احراز اصالت بین دو سرخوشه

(Figure-4): Authentication between cluster heads

گام ۶: SN2 مقدار N1 و Tr2 را محاسبه و مقدار AID2 را به روزرسانی می کند. درنهایت مقدار کلید نشست برای این ارتباط محاسبه می شود.

گام ۷: در این مرحله مقدار N2 ترکیب شده با AK و V4 تولید شده توسط CH2، برای CH1 ارسال می شود.

گام ۸: با دریافت پیام {AID2, AID1, D, V4}، در ابتدا مقدار N2 را به دست می آورد و سپس مقدارهای AID1 و Tr1 را به روزرسانی می کند. درنهایت پیام M6= {AID2, AID1, D, V4}، در SN1 ارسال می شود.

گام ۹: SN1 مقدار N2 و Tr1 را محاسبه و مقدار AID1 را به روزرسانی می کند. همچنین با به دست آوردن N2 می تواند کلید نشست SK را نیز محاسبه کند.

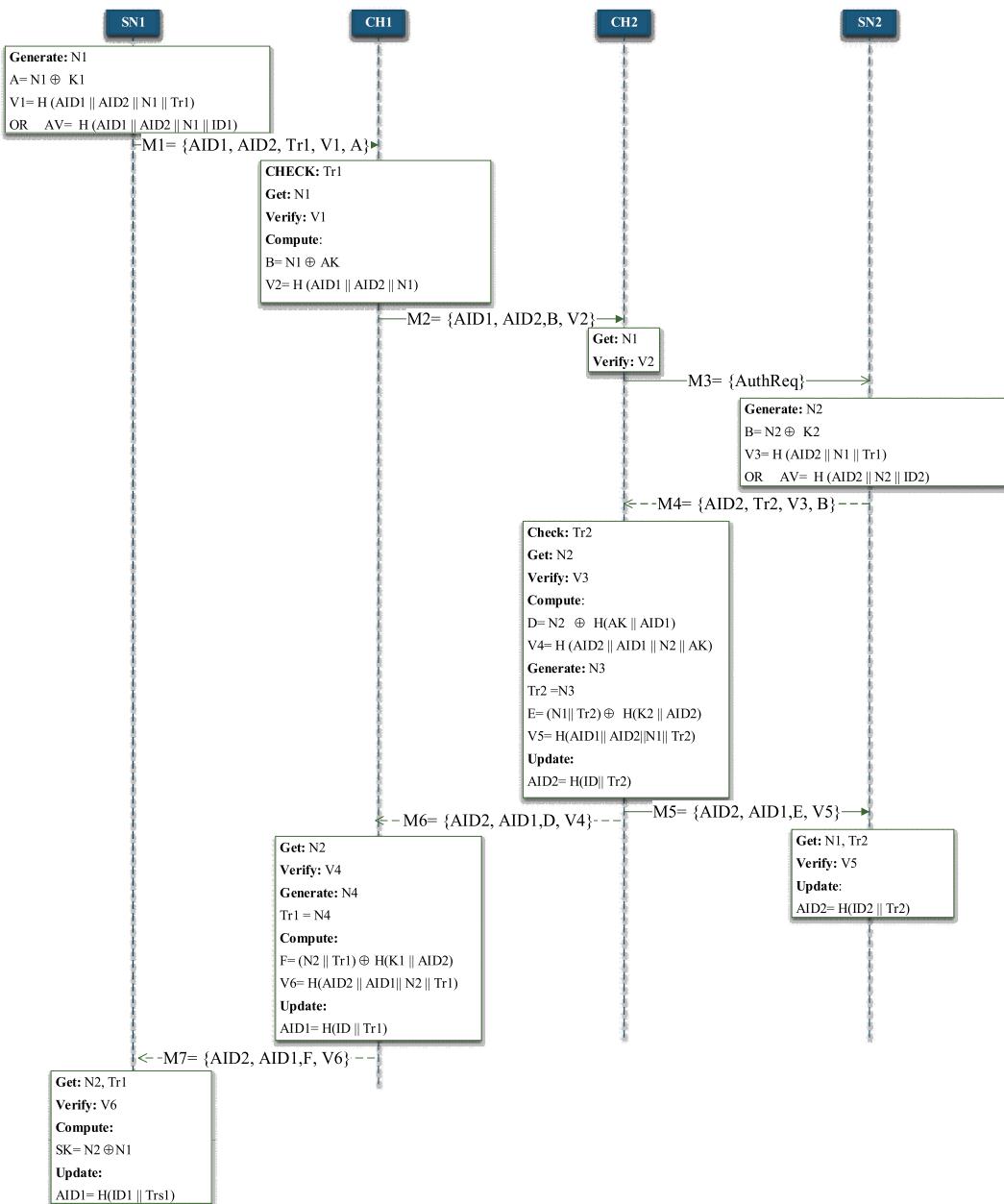
گام ۱: همانند گام ۱ در شکل (۳) انجام می شود.

گام ۲: CH1 پس از دریافت پیام M1 از حسنگر SN1، آن را احراز اصالت و سپس دو رابطه V2= B= N1 ⊕ AK و M2= H (AID1 || AID2 || N1) را تولید و پیام {AID1, AID2, B, V2} می کند.

گام ۳: CH مقصد در ابتدا مقدار N1 را به دست می آورد و سپس از SN مورد نظر می خواهد که اطلاعاتش را برای CH ارسال کند.

گام ۴: این مرحله همانند گام ۱ انجام می شود.

گام ۵: CH2 ابتدا SN2 را احراز اصالت می کند و مقدار N2 را محاسبه و سپس مقادیر E= (N1 || Tr2) ⊕ H (K2 || AID2) و V5= H (AID1 || AID2 || N1 || Tr2) را برای SN2 ارسال می 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، مقایسه‌پذیری، 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 درنتیجه 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 مقابله احراز اصالت کند؛ اما در صورت اتمام طول عمر، ارتباط بایستی دوباره از مرحله ثبت نام آغاز شود. به عبارت دیگر طرح ابطال کلید بر حسب طول عمر کلید است.

## ۴- تحلیل

### ۴-۱- برآورده ساختن نیازمندی‌های امنیتی

حمله ناهم‌زنی<sup>۴</sup> یا حمله انکار سرویس<sup>۵</sup> را افزایش می‌دهد و به طور کلی دسترس پذیری 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 ID حس‌گر استفاده شده است تا اگر چنین حملاتی رخ داد، به جای V1، عبارت AV ارسال شود. به همین دلیل دسترس پذیری 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 رمزگاری، راه حل سبک‌تری ارائه شود. هم‌چنین در بخش ۳-۴ بار محاسباتی پروتکل پیشنهادی با سایر طرح‌ها مقایسه خواهد شد تا سبک وزنی آن به صورت کمی نیز تضمین شود.

#### ۴-۲ 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) ترکیب شده 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. به طور 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 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، به دلیل وجود مقدار تصادفی N1 و N2، مقدار عبارت‌های V4 و V3 دریافتی با مقدار محاسبه شده متفاوت خواهد بود و حمله تکرار کشف خواهد شد.

**حمله مرد میانی<sup>۶</sup>:** با توجه به عبارت‌های ارسالی V1 تا V6 در پیام‌های M1 تا M7 و فرآیند احراز اصالت هر یک از

(جدول-۲): نیازمندی‌های اینترنت اشیا

(Table-2): IoT Requirements

ردیابی <sup>۷</sup>	توافق کلید منصفانه	مقیاس پذیری	قابلیت عدم ردیابی	گمنامی	احراز اصالت دوطرفه
✓	✓	✗	✗	✓	[14]
✓	✓	✓	✓	✓	[17]
✓	✗	✗	✓	✓	[15]
✓	✗	✓	✓	✓	[16]
✓	✓	✓	✗	✗	[12]
✓	✓	✓	✓	✓	طرح پیشنهادی

**احراز اصالت دوطرفه:** برای اثبات احراز اصالت دوطرفه دو حالت موجود است: ارتباط بین حس‌گرها در سرخوشه یکسان و دو سرخوشه متفاوت. این ویژگی به طور کامل در تشریح پروتکل مشخص شده است. برای احراز اصالت موجودیت‌ها از عبارت‌های  $i = 1, \dots, 6$   $V_i$  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 به روزرسانی آن پس از هر ارتباط، باعث می‌شود تا هیچ موجودیتی جز موجودیت قابل اعتماد بالادستی نتواند فعالیت‌های حس‌گر را دنبال کند.

**مقیاس پذیری<sup>۸</sup>:** در ابتدا و در تمامی مراحل پروتکل‌های پیشنهادی، مقایسه Tri<sup>۹</sup> (Tri) مربوطه با مقدار ذخیره شده در پایگاه داده، باعث می‌شود تا بر محاسباتی شبکه با افزایش تعداد موجودیت‌ها، افزایش چشم‌گیری نداشته باشد و درنتیجه نیازی به انجام عملیات سنگین جستجو نخواهد بود.

**توافق کلید به صورت منصفانه<sup>۱۰</sup>:** در پروتکل پیشنهادی هر دو موجودیت به یک اندازه در تولید کلید سهیم هستند. درنتیجه توافق کلید SK به صورت منصفانه انجام شده است تا در مراحل بعد، اطلاعات به صورت ایمن بین SNها مبادله شود.

**دسترس پذیری<sup>۱۱</sup>:** در بسیاری از پروتکل‌های احراز اصالت، یک سری کلید محروم‌های بین موجودیت‌ها وجود دارد که بعد از هر بار نشست، به روزرسانی می‌شوند. این به روزرسانی امکان

<sup>1</sup> Scalability<sup>2</sup> Fair Key Agreement<sup>3</sup> Availability<sup>4</sup> De-synchronization Attack<sup>5</sup> Denial of Service Attack<sup>6</sup> Man In the Middle

### ۴-۳- مقایسه هزینه محاسباتی

حس‌گرها قدرت پردازشی و محاسباتی پایینی دارند؛ به همین جهت بایستی هزینه محاسباتی پروتکل پیشنهادی با پروتکلهای پیشین مقایسه شود (جدول ۴). نمادهای  $T_{mul}$ ,  $T_{inv}$ ,  $T_{ecm}$ ,  $T_{eca}$  و  $Th$  به ترتیب نشان‌دهنده زمان اجرای عملیات ضرب پیمانه‌ای، عملیات معکوس ضربی، عملیات 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]
$\approx 4.32T_{mul}$	$12_{TH} + 6T_{XOR} + 28T_{\parallel}$	[16]
$\approx 6.48T_{mul}$	$18_{TH} + 11T_{XOR} + 10T_{\parallel}$	[17]
$\approx 7.21T_{mul}$	$20_{TH} + 30T_{XOR} + 18T_{\parallel}$	[15]
$\approx 5.76T_{mul}$	$16_{TH} + 9T_{XOR} + 30T_{\parallel}$	طرح پیشنهادی

با توجه به [18]،  $T_{eca} \approx 5T_{mul}$ ,  $T_{inv} \approx 3T_{mul}$ ,  $T_{ecm} \approx 1200T_{mul}$  و  $Th \approx 0.36T_{mul}$  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 به عنوان یکی از مسائل کلیدی این حوزه ظاهر می‌شود؛ که به علت محدودیت‌های محاسباتی اشیا، بهتر است از راه حل‌های سبک و متقاضان استفاده شود. از طرفی یکی از مباحثت 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 V1 تا V4 قرار می‌گیرند تا هم مقدار حقیقی پنهان و هم مقادیر ارسالی به صورت 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 به روزرسانی مراحل احراز اصالت، خلی وارد کند، احتمال رخداد حمله ناهمگام‌سازی به وجود می‌آید. سازوکار لازم برای مقابله با این حمله، استفاده از عبارت AV به جای Vi است. در عبارت AV به جای Tr از ID حس‌گر استفاده می‌شود تا اگر خلی در به روزرسانی Tr به وجود 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

ناهمگام‌ساز	آنکار سرویس	استراق سمع	جعل هویت	تکرار	مرد میانی	طرح پیشنهادی
✓	✓	✗	✗	✗	✓	[14]
✓	✓	✓	✓	✓	✓	[17]
✗	✗	✓	✗	✓	✗	[15]
✓	✓	✓	✓	✗	✓	[16]
✓	✓	✓	✓	✓	✓	طرح پیشنهادی

<sup>1</sup> 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 *Inter-national 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 Interna-tional 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، تمايلی به شناخته‌شدن در شبکه ندارند و ترجیح می‌دهند به صورت 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 استانداردی، 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 پایرجا بوده است. برخی دیگر بیشتر روی سبک وزنی تمرکز کرده و به جای 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. علاوه‌بر این بسیاری از پروتکلهای ارائه شده، تنها ارتباط یک موجودیت با موجودیت بالادستی را در نظر گرفته‌اند؛ در حالی که بررسی ارتباط بین موجودیت‌ها نیز امری ضروری به نظر می‌رسد.

لذا بر آن شدیم تا پروتکل احراز اصالتی به صورت سلسه‌مراتبی بین موجودیت‌ها در خوش‌بینی و دو خوش‌بینی مقاومت ارائه کنیم که ضمن برآورده 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 یا 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

- [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 ۱۳۹۰ تکمیل کرد. از سال ۱۳۹۰ تاکنون عضو هیأت علمی دانشگاه شاهد و زمینه‌های پژوهشی مورد علاقه ایشان محاسبات کوانتمی، 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. Gurrov, and M. Yliantila, "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. Gurrov, and M. Yliantila, "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 جانبabaei تحصیلات خود را در مقاطع 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 قرائی تحصیلات خود را در مقاطع 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

فصلنامه

سال ۱۳۹۷ شماره ۴ پیاپی ۳۸

