Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 11, Number 3, Autumn, pp. 48-63
Received: 11/17/2021, Revised: 08/26/2022, Accepted: 11/08/2022

An Efficient Group-based Authentication and Key Agreement Protocol in the Internet of Things environment

Zahra Jalali[1], Rahman Hajian[2] and Seyed Hossein Erfani[3*]
1- Department of Information Technology Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran.
2- Department of Information Technology Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran.
3*- Department of Computer Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran.
[1]missjalali@yahoo.com, [2]hajian.rh@gmail.com, and [3*]h_erfani@azad.ac.ir

Corresponding author's address: Seyed Hossein Erfani, Faculty of Engineering, South Tehran Branch, Islamic Azad University, Tehran, Iran.

Abstract- Considering the increasing expansion of the Internet of Things (IoT) applications and the limitation of end devices in energy resources, sending/receiving fewer data in order to reduce energy consumption is essential. The authentication and key agreement in the IoT networks face many important challenges, most of which are the high computational overhead of existing group key agreements, having negative impacts on network performance. In this paper, we propose an authentication and key agreement protocol that support group communication and uses the Chebyshev polynomial in its calculations, which compare to linear pairing and elliptic curve cryptography, while having enough security, imposes less overhead on the IoT networks. Our proposed protocol is a good option for use in IoT applications including home automation, smart meters, and vehicular sensor networks. The proposed group authentication improves the efficiency of communication compared to other similar protocols and is resistant to various types of internal and external attacks. The security assessment of the proposed protocol has been done using a Random Oracle Model (ROM) and informally.

Keywords- Internet of Things, Security, Group Key Agreement, Mutual Authentication, Random Oracle Model.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۱۱، شماره ۳، پاییز ۱۴۰۱ ، صفحه ۴۸-۶۳
دریافت:۱۴۰۰/۰۸/۲۶ ، بازنگری: ۱۴۰۱/۰۶/۰۴، پذیرش: ۱۴۰۱/۰۸/۱۷

یک طرح توافق کلید و احرازهویت کارا مبتنی بر ارتباطات گروهی در محیط اینترنت اشیا

زهرا جلالی[۱]، رحمان حاجیان[۲]، سید حسین عرفانی*[۳]
۱- کارشناسی ارشد، گروه مهندسی فناوری اطلاعات، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.
۲- کارشناسی ارشد، گروه مهندسی فناوری اطلاعات، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.
*۳- استادیار، عضو هیات علمی، گروه مهندسی کامپیوتر، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.
[1]missjalali@yahoo.com, [2]hajian.rh@gmail.com, [3*]h_erfani@azad.ac.ir

* نشانی نویسنده مسئول: سیدحسین عرفانی، تهران، خیابان پیروزی - بلوار نبرد جنوبی -خیابان ده حقی (آهنگ) - نبش بلوارکوثر، مجتمع فنی و مهندسی.

چکیده- با توجه به گسترش روزافزون کاربردهای اینترنت اشیا (IoT) و محدودیت دستگاه‌های انتهایی در مصرف انرژی، ارسال و دریافت کمتر داده‌ها در راستای ذخیره انرژی در این شبکه‌ها از ضروریات است. توافق کلید و احرازهویت در شبکه‌های IoT با چالش‌های مهمی روبه‌رو است. یکی از مشکلات اکثر طرح‌های احرازهویت و توافق کلید گروهی موجود، داشتن سربار محاسباتی بالا است که تاثیر منفی بر روی عملکرد شبکه دارد. در این پژوهش یک پروتکل احرازهویت و توافق کلید برای شبکه‌های IoT ارائه نموده‌ایم که از ارتباطات گروهی پشتیبانی می‌کند و در محاسبات رمزنگاری آن از چندجمله‌ای چبیشف استفاده شده است؛ چراکه در مقایسه با رمزنگاری‌های جفت‌سازی خطی و رمزنگاری خم بیضوی (ECC) ضمن داشتن امنیت کافی، سربار کمتری را به شبکه IoT تحمیل می‌کند. پروتکل پیشنهادی گزینه‌ی مناسبی برای استفاده در اتوماسیون خانگی، کنتورهای هوشمند، شبکه‌های حسگر خودرویی و مانند آن است. طرح احرازهویت گروهی پیشنهادی، کارایی ارتباطات را نسبت به سایر طرح‌های مشابه بهبود می‌بخشد و در مقابل انواع حملات داخلی و خارجی مقاوم است. ارزیابی امنیتی پروتکل پیشنهادی با استفاده مدل اوراکل تصادفی و به‌صورت غیر رسمی انجام گرفته شده است.

واژه‌های کلیدی: اینترنت اشیا، امنیت، توافق کلید گروهی، احرازهویت متقابل، مدل اوراکل تصادفی.

۱- مقدمه

فناوری رو به رشد اینترنت اشیا (IoT)[۱]، به‌عنوان شبکه‌ای از سرویس‌ها، اشیای مختلف را به یکدیگر متصل می‌کند و ارتباطات ماشین به ماشین (M2M)[۲] و دستگاه به دستگاه (D2D)[۳] را فراهم می‌سازد. کاربردهای گسترده IoT سبب تولید داده‌های اندازه‌گیری‌شده همگن و ناهمگن می‌شود [۲،۱] که از جمله آنها می‌توان به خانه هوشمند، سیستم حمل و نقل هوشمند، سلامت هوشمند، نظارت هوشمند و مانند آن اشاره نمود.

امنیت یکی از ویژگی‌های مهم در هر لایه IoT است. پیاده‌سازی موفق یک سیستم IoT در صورتی محقق خواهد شد که نگرانی‌های امنیتی در خصوص حملات و چالش‌های امنیتی در طراحی ارتباطات بین دستگاه‌های IoT مورد توجه قرار گرفته شوند. مکانیزم‌های امنیتی مانند احرازهویت و کنترل دسترسی برای کاربردهای IoT در مقالات زیادی بررسی گردیده است [۳]. پژوهش حاضر، به‌طور خاص بر روی امنیت در لایه فیزیکی و لایه تبادل داده، برای ساخت یک کلید نشست ایمن و کارا تمرکز دارد.

ارتباطات دستگاه‌های IoT می‌تواند به‌صورت دستگاه به دستگاه یا گروهی و دسته‌ای شکل گیرد. در ارتباطات D2D، تعامل بین دو موجودیت و یا تعامل در معیت یک شخص ثالث مورد اعتماد انجام می‌پذیرد [۴]. در ارتباطات گروهی به‌جای تولید K کلید نشست با

تک تک اعضای گروه به‌صورت مجزا، یک کلید گروه ایجاد می‌شود و تمام گره‌های عضو گروه می‌توانند به این کلید دست پیدا کنند. با این‌حال، سازوکار ساخت کلید گروه باید به‌گونه‌ای باشد که در مقابل حمله جعل، حمله انکار سرویس و حمله دست‌یابی گره‌های مخرب و حذف شده به کلید نشست ایمن باشد؛ و گمنامی کاربران و دستگاه‌های IoT حفظ گردد [۵].

طرح‌های توافق کلید و احرازهویت گروهی به مجموعه‌ای از دستگاه‌های عضو و مجاز اجازه می‌دهند که یک کلید نشست را به اشتراک بگذارند؛ به‌گونه‌ای که هر عضو سهمی در تولید کلید داشته باشد. پروتکل‌های توافق کلید گروهی به‌دلیل ایجاد یک گروه می‌تواند سربار را به نسبت احرازهویت D2D بهبود بخشند. با این حال، چالش‌هایی در طراحی و پیاده‌سازی آنها وجود دارد که باید مد نظر قرار گرفته شوند. همچنین از آنجا که این گروه‌ها به‌صورت پویا در نظر گرفته می‌شوند، باید مکانیزمی جهت اضافه شدن و ترک کردن گره‌ها و حذف گره‌های مخرب اتخاذ شود [۷،۶].

رویکرد امضای گروهی بدون گواهینامه یکی از روش‌های احرازهویت سریع برای شبکه‌هایی با تعداد دستگاه‌های زیاد است. رمزنگاری کلید عمومی بدون گواهینامه (CLBS)[۴] توسط الریامی [۸] در سال ۲۰۰۳ معرفی گردید و مشکل سپردن کلید در رمزنگاری مبتنی بر شناسه و مدیریت گواهینامه و مشکل حافظه را برطرف نمود. طرح‌های CLBS و طرح‌های احرازهویت دسته‌ای که به عملیات‌های جفت‌سازی خطی[۵] یا عملیات‌های ضرب نقطه‌ای زیادی نیاز دارند سربار محاسباتی را به شدت بالا می‌برند و برای دستگاه‌های IoT متحرک با انرژی محدود مناسب نیستند.

۱-۱- انگیزه و مشارکت

در سال‌های اخیر تحقیقات در خصوص صنایع نسل چهارم و پنجم اینترنت اشیا مورد توجه دولت‌ها قرار گرفته است. در شبکه‌های IoT به ناچار داده‌های حساس به حریم خصوصی و امنیت مبادله می‌شود و این نکته آنها را برای مهاجمان جذاب کرده است. در شبکه‌های IoT که ارتباطات گروهی امکان‌پذیر است، احرازهویت گروهی و ایجاد کلید گروه، سربار ارتباطات و محاسبات ناشی از ایجاد کلید را به شدت کاهش می‌دهد. همچنین یکی از مشکلات اکثر طرح‌های احرازهویت و توافق کلید گروهی موجود، داشتن سربار محاسباتی بالای آنها است که تاثیر منفی بر روی عملکرد شبکه نظیر تاخیر بیشتر و افزایش انرژی مصرفی دارد. در این پژوهش یک پروتکل احرازهویت و توافق کلید برای شبکه‌های IoT با قابلیت پشتیبانی از ارتباطات گروهی ارائه گردیده است که مزایای زیر را به همراه دارد.

- استفاده از چندجمله‌ای چبیشف[۶] در محاسبات رمزنگاری، به‌دلیل داشتن سربار محاسباتی کمتر نسبت به رمزنگاری‌های جفت‌سازی خطی و رمزنگاری خم بیضوی (ECC)[۷].
- آشکارسازی نقاط ضعف امنیتی طرح پیشین.
- اثبات ایمن بودن طرح پیشنهادی در مقابل انواع حملات داخلی و خارجی به کمک مدل اوراکل تصادفی.
- بهبود کارایی نسبت به طرح‌های پیشین.

ساختار پژوهش حاضر به این شرح زیر است که در بخش دوم، مروری بر روش‌های پیشین و مقدمات رمزنگاری انجام گردیده است. در بخش سوم طرح توافق کلید گروهی پیشنهادی ارائه گردید. سپس در بخش چهارم، ارزیابی امنیتی و کارایی روش پیشنهادی و سایر طرح‌های موجود انجام گردیده است. در نهایت در بخش پنجم، نتیجه‌گیری و کارهای پیشنهادی ارائه گردیده است.

۲- پیشینه

در مقایسه با روش‌های احرازهویت سنتی، در تایید هویت گروهی به‌جای احرازهویت فردی، کاربران به‌صورت گروهی یکدیگر را تایید می‌کنند که سربار را به شدت کاهش می‌دهد. ازاین‌رو بسیار مطلوب است که در محیط‌های گروه محور مانند ارتباطات چندپخشی و ارتباطات کنفرانسی از احرازهویت گروهی استفاده شود.

ژیا و همکاران [۹] پروتکل احرازهویت گروهی چآین [۱۰] را مورد بررسی قرار دادند و نشان دادند که مهاجم می‌تواند در یک مدل ارتباطی ناهمزمان، بدون شناسایی شدن، به‌عنوان یک گره مشروع خود را جا بزند. آنها یک شبکه حق رای گمنام را به طرح چآین [۱۰] اضافه نمودند. معتمید و همکاران [۱۱] یک پروتکل احرازهویت گروهی مقیاس‌پذیر بر مبنای طرح‌های ترکیباتی با قابلیت تحمل‌پذیری خطا برای شبکه‌های IoT ارائه دادند. نظریه طراحی بیضوی، تحمل خطا بر مبنای تعداد اعضای گروه یک آستانه را مشخص می‌کند. یک پروتکل احرازهویت گروهی برای شبکه بی‌سیم خصوصی برق توسط لی و همکاران [۱۲] ارائه شد که از یک تابع محافظ حریم خصوصی برای احرازهویت استفاده می‌کند.

یک رویکرد احرازهویت دسته‌ای توسعه‌پذیر و کارا همراه با قابلیت گمنامی برای شبکه‌های حسگر خودرویی توسط ژانگ و همکاران [۱۳] ارائه گردید که از سیستم کلید خصوصی از پیش‌بارگذاری‌شده استفاده نمی‌کند. همچنین، علاوه بر مدیریت لیست ابطال گواهی‌ها (CRL)[۸]، یک طرح ابطال شناسه محافظ حریم خصوصی مشروط را پشتیبانی می‌کند که تنها موجودیت مجاز (TA)[۹] می‌تواند وسایل

نقلیه را ردیابی و ابطال کند. پران و همکاران [۱۴] یک پروتکل احرازهویت توسعه یافته به نام SEGB را برای ارتباطات M2M در شبکه تکامل بلندمدت (LTE)[۱۰] ارائه دادند. پروتکل SEGB-AKA به محرمانگی رو به جلو و رو به عقب دست می‌یابد. یک پروتکل مسیریابی و توافق کلید گروهی برای شبکه‌های ادهاک خودرویی (VANET)[۱۱] به نام TROPHY توسط سیرن و همکاران [۱۵] ارائه گردید. گره‌های شبکه با ارسال پیام TROPHY در شبکه، اطلاعات خود را به‌روز می‌کنند. این پیام‌ها در تمام شبکه پخش همگانی می‌شوند. یک موجودیت متمرکز مسئول ابطال گواهینامه‌ها است. شریدا و همکاران [۱۶] و ژو و همکاران [۱۷] نیز پروتکل‌های توزیع کلید و احرازهویت گروهی برای شبکه‌های VANET را ارائه دادند.

شبکه‌های فوق چگال (UND)[۱۲]، از تکنولوژی‌های کلیدی نسل پنجم ارتباطات (5G)، برای ارائه اتصال‌پذیری مطمئن و پیوسته به دستگاه‌های کاربران و دستیابی به یکپارچگی و اعتبارسنجی در ارتباطات، نیاز دارد تا چالش‌های مرتبط با احرازهویت و اعتبارسنجی اطلاعات را برطرف نماید. یائو و همکاران [۱۸] یک رویکرد احرازهویت و ایجاد کلید نشست سبک به نام LBAKA برای شبکه‌های UND کاربرمحور ارائه دادند که رویکرد احرازهویت دسته‌ای سبک‌وزن و توافق کلید یک به یک را با یکدیگر مطابقت می‌دهد. ارتباطات D2D به‌عنوان تکنولوژی ارتباط مستقیم کاربردهای گسترده‌ای دارد و نقش مهمی را در 5G بازی می‌کند. سان و همکاران [۱۹] یک مکانیزم کشف دستگاه نزدیک با قابلیت گمنامی و مکانیزم احرازهویت دستی برای D2Dهای ناهمگن بر مبنای یک امضای دسته‌ای بدون گواهینامه بی‌نیاز از جفت شدن و کارا ارائه دادند که احرازهویت متقابل و تأئید دسته‌ای را بدون نیاز به گواهینامه فراهم می‌آورد. یک پروتکل احرازهویت و توافق کلید گروهی توسط لای و همکاران [۲۰] که برای تمامی سناریوهای شبکه تکامل بلند مدت (LTE) مناسب است ارائه گردید؛ که پروتکل از رمزنگاری دیفی-هلمن مبتنی بر ECC برای حفظ محرمانگی رو به جلو و عقب استفاده می‌نماید.

یک طرح احرازهویت محافظ حریم خصوصی بر مبنای گواهینامه عمومی و امضای مبتنی بر شناسه توسط وانگ و همکاران برای شبکه‌های VANET مطرح گردید [۲۱]. در این طرح عامل مجاز TA یک گواهینامه بلند مدت را به هر گره ثبت شده اختصاص می‌دهد. تنها گره‌هایی که یک گواهی معتبر دارند می‌توانند شناسه کوتاه مدت و گمنام را از واحد کنار جاده‌ای (RSU) دریافت نمایند، تا بتوانند پیام‌ها را امضا کنند. کائو و همکاران [۲۲] یک پروتکل احرازهویت گروهی مبتنی بر رمزنگاری ECC به نام GBAAM برای ارتباطات ماشینی در شبکه‌های نسل چهارم موبایل ارائه دادند. چوی و همکاران [۲۳] پروتکل احرازهویت گروهی ارائه دادند که قابلیت حذف و اضافه اعضا به گروه را در طرح خود در نظر گرفته است.

یک طرح توافق کلید گروهی مبتنی بر چند جمله‌ای چبیشف با حفظ حریم خصوصی مشروط برای شبکه VANET توسط یانگ و همکاران [۲۴] ارائه شد. سیستم اینترنت اشیا هوشمند، IoT را قادر می‌سازد تا محاسبات هوشمندانه‌تری انجام دهد. ژانگ و همکاران [۲۵] پروتکل توافق کلید گروهی سلسله مراتبی برای معماری سه لایه ابر، لبه و دستگاه‌های سیار ارائه دادند. ژیا و همکاران [۲۶] طرحی را برای احرازهویت گروهی در خانه‌های هوشمند معرفی کردند که از تابع غیرهمسان فیزیکی (PUF) و تکنیک استخراج کننده فازی درمحاسبات خود استفاده می‌کند. براکن [۲۷] پروتکل توافق کلید گروهی مبتنی بر ECC را ارائه داد که مقیاس‌پذیری بهتری را نسبت به طرح‌های مشابه دارد چرا که سربار بیتی پیام‌های همه پخشی شده را کاهش داده است.

بنابراین کاربردهای IoT به‌طرز شگفت‌انگیزی در حال گسترش هستند. درصورتی این کاربردها موثر و کارا واقع خواهند شد که پروتکل احرازهویت و اعتبارسنجی موفقی به کار گرفته شود. تا کنون پروتکل‌های زیادی در این زمینه ارائه شده‌اند که نیازمندی‌های امنیتی مانند حفظ حریم خصوصی، احرازهویت، یکپارچگی و محرمانگی را فراهم می‌آورند؛ اما آنها کارایی لازم را برای نگهداری کلید گروه با قابلیت غیرقابل پیگیری بودن ندارند و مستعد حملات شناخته شده هستند. ازاین‌رو، برآن شدیم تا یک پروتکل توافق کلید گروهی ایمن و کارا، مناسب برای محیط‌های IoT ارائه دهیم که در بخش ۳ ارائه شده است.

۲-۱- مقدمات رمزنگاری

در این بخش مفاهیم امنیتی مورد نیاز در این پژوهش و مدل مهاجم شرح داده شده است. علائم و نمادهای مورد استفاده در این پژوهش در جدول ۱ نشان داده شده است.

نگاشت آشوب چبیشف. رمزنگاری مبتنی بر نقشه آشفته چبیشف [۲۹،۲۸] می‌تواند برای یک طرح توافق کلید و احرازهویت ایمن و کارا به کار گرفته شود. با داشتن عدد صحیح r به‌عنوان درجه چندجمله‌ای و متغیر تصادفی $x \epsilon [-1, +1]$، چندجمله‌ای چبیشف به‌صورت زیر است

$$T_r(x) = 2xT_{r-1}(x) - T_{r-2}(x), mod\ p\ , Wherer\ r \geq 2, T_0(x) = 1, and\ T_1 = x \quad (۱)$$

در این رمزنگاری موارد زیر صادق هستند

تعریف ۱. برای عدد صحیح n و متغیر x که $x \epsilon [-\infty, +\infty]$ چندجمله‌ای چبیشف بهبودیافته $T_n(x): [-\infty, +\infty] \rightarrow [-\infty, +\infty]$ در فرمول (۲) و قاعده فرمول بازگشتی در فرمول (۳) تعریف می‌شود.

$$T_n(x) = cos(n * arccos(x)) \quad (۲)$$

$$T_n(x) = 2xT_{n-1}(x) - 2xT_{n-2}(x)(mod\ p)(n \geq 2) \quad (۳)$$

که p یک عدد اول است و $T_0(x) = 1$ و $T_1(x) = x$. مهم‌ترین ویژگی چندجمله‌ای چبیشف خاصیت شبه گروه بودن آن است. همچنین ترکیب‌بندی زیر دارای خاصیت جابجایی است.

$$T_n(T_m(x)) = T_m(T_n(x)) \quad (۴)$$

جدول ۱: علائم و نمادهای استفاده شده در این پژوهش.

نماد	توضیحات	نماد	توضیحات
$\boldsymbol{T}(.)$	چندجمله‌ای چبیشف بهبودیافته	s, Q_{TA}	کلید عمومی و خصوصی سرور TA
$\boldsymbol{MTCD_{ij}}$	اُمین $MTCD$ در گروه اُم	s_j, Q_j	کلید عمومی و خصوصی $MTCD_j$
$\boldsymbol{IMSI_j}$ $\boldsymbol{IMSI_{MTCD_{ij}}}$	شناسه بین‌المللی و منحصر به فرد $MTCD_{ij}$	y, z	رشته بیت تصادفی و یک‌بار مصرف (نانس)
$\boldsymbol{PIN_j}$	شماره رمز $MTCD_{ij}$	$K^{ASME}_{MTCD_{ij}}$	کلید نشست بین TA و $MTCD_{ij}$
$\boldsymbol{KDF}(.)$	تابع استخراج کلید	T_{ij}	مهرزمانی ۶۴ بیت
$\boldsymbol{p}$	عدد اول بسیار بزرگ	ΔT	تاخیر انتقال مجاز
$\boldsymbol{TA}$	سرور احرازهویت	$\mathcal{A}$	مهاجم
$\boldsymbol{h}(\cdot)$	تابع هش	$\oplus, \|\|$	XOR و الحاق
$\boldsymbol{Extract}(.)$	تابع استخراج ۳۲ بیت مهرزمانی	x	پارامتر عمومی تابع چبیشف
$\boldsymbol{GID_i}$	شناسه گروه اُم	GK_i	کلید گروه اُم

تعریف ۲. مسئله لگاریتم گسسته مبتنی بر نقشه چبیشف (CMDDHP). به ازای هر مقدار x و y داده شده، از نظر محاسباتی تشخیص r به‌گونه‌ای که شرط $T_r(x)(mod\ p) = y$ برقرار شود، امکان‌پذیر نیست. به‌عبارت دیگر، احتمال درستی محاسبه r توسط مهاجم چندجمله‌ای زمان $\mathcal{A}$ با داشتن $\{x, T_r(x)(mod\ p)\}$، در فرمول (۵) آمده است. Z_p^* مجموعه اعداد بین $[0, 1-p]$ است. p یک عدد اول بسیار بزرگ و $Adv^{DLP}(\mathcal{A})$ شانس برنده شدن مهاجم را نشان می‌دهد که بسیار ناچیز است [۳۰،۳۱].

$$Adv^{DLP}(\mathcal{A}) = Pr[\mathcal{A}(\{x, T_r(x)(mod\ p))] = r;\ r \epsilon Z_p^* \quad (۵)$$

تعریف ۳. مسئله محاسبات دیفی-هلمن مبتنی بر نقشه آشفته (CMCDHP). به ازای $\{x, T_r(x)(mod\ p), T_s(x)(mod\ p)\}$ داده شده، از نظر محاسباتی تشخیص $T_{r.s}(x)$ امکان‌پذیر نیست. به‌عبارت دیگر، هیچ مهاجم چندجمله‌ای زمان $\mathcal{A}$ وجود ندارد که بتواند $T_{r.s}(x)$ را محاسبه کند. احتمال محاسبه صحیح به‌صورت زیر است [۳۰،۳۱].

$$Adv^{CMDDHP}(\mathcal{A}) = Pr[\mathcal{A}(x, T_r(x)(mod\ p),\ T_s(x)(mod\ p), T_{r.s}(x)(mod\ p))] = 1;\ r, s \epsilon Z_p^* \quad (۶)$$

تعریف ۴. مسئله دیفی-هلمن تصمیم مبتنی بر نقشه آشفته CMCDHP[۱۳]. به ازای مقادیر $\{(x, T_r(x)(mod\ p), T_s(x)(mod\ p), T_z(x)(mod\ p)\}$ داده شده هیچ مهاجم چندجمله‌ای زمانی وجود ندارد که بتواند تفاوت بین $T_{r.s}(x)\ mod\ p$ و $T_z(x) mod\ p$ را متوجه شود. احتمال اینکه مهاجم بین $T_{r.s}(x)$ و $T_z(x)$ تفاوت قائل شود به‌صورت زیر است

$$Adv^{CMDDHP}(\mathcal{A}) = Pr[\mathcal{A}(x, T_r(x)(mod\ p),\ T_s(x)(mod\ p), T_{r.s}(x)(mod\ p))] = 1;\ r, s \epsilon Z_p^*] - Pr[\mathcal{A}(\{x, T_r(x) mod\ p,\ T_s(x) mod\ p, T_z(x) mod\ p)] = 1;\ r, s, z \epsilon Z_p^*] \quad (۷)$$

تابع درهم ساز یک طرفه. تابع درهم‌ساز (هَش) ، تابعی یک طرفه است که ورودی با طول متغییر را دریافت و خروجی با طول ثابت را تولید می‌کند. یک تابع هَش یک‌طرفه باید این خصوصیات را فراهم کند ۱) تابع $h(.)$ برای همه کاربران و مهاجم مشخص شده است. ۲) بتوان برای پیام دلخواه m مقدار $h(m)$ را محاسبه نمود. ۳) چنانچه کاربر غیرمجاز مقدار $h(m)$ را در اختیار داشته باشد، امکان محاسبه m از روی $h(m)$ در زمان منطقی امکان‌پذیر نباشد. ۴) در تابع درهم‌ساز امکان رخداد تصادم ضعیف باشد؛ به‌عبارتی با داشتن پیام x، پیدا کردن پیام y که $x \neq y$ به نحوی که $h(x) = h(y)$ برقرار باشد، از نظر محاسباتی در زمان منطقی غیرممکن باشد.

مدل مهاجم. یک مهاجم چندجمله‌ای زمان به نام $\mathcal{A}$ که بر روی کانال‌های ارتباطی کنترل کامل دارد را در نظر می‌گیریم. فرض می‌شود که مهاجم می‌تواند حملات مختلفی شامل حمله مردی در میان، حمله تکرار، حمله انکار سرویس و مانند آن را انجام دهد. مهاجم $\mathcal{A}$ می‌تواند ارتباطات مبادله شده بین اعضای گروه را شنود، مسدود، حذف، تغییر و یا تکرار کند. همچنین می‌تواند یک پیام را به کانال عمومی اضافه کند. مهاجم کنترلی بر روی پیام‌های مبادله شده در کانال‌های خصوصی ندارد و تلاش می‌کند تا با کمک اطلاعات به دست آمده از کانال‌های عمومی، خود را به‌عنوان یک موجودیت مجاز جعل کند.

۲-۲- نقاط ضعف پروتکل روی‌چاودری و همکاران

روی‌چاودری و همکاران [۳۱] طرح توافق کلید گروهی برای ارتباطات ماشینی با استفاده از چندجمله‌ای چبیشف ارائه دادند که جزئیات آن در [۳۱] آمده است. در اینجا نقاط ضعف امنیتی این طرح بررسی شده است.

نامقاوم در برابر حمله تکرار. پروتکل روی‌چاودری و همکاران تنها در محاسبات درون گروهی از مهر زمانی استفاده می‌کند؛ و در ارتباطات بین رهبرگروه و سرور احرازهویت که در کانال عمومی انجام می‌شود از آن استفاده نشده است. مهاجم می‌تواند پیام درخواست احرازهویت شامل $\{IMSI_{MTCD_{ij}}, GID_i, T1_{MTCD_{ij}}, r_{MTCD_{ij}}, H_{MTCD_{ij}}\}$ را شنود، و در یک بازه‌ی زمانی دیگر مجددا ارسال کند. از آنجا که سرور TA نمی‌تواند این پیام‌ها را تا مدت زمان زیادی در حافظه‌ی موقت (بافر) خود نگهداری کند، پس از خالی شدن ، این پیام از نظر TA معتبر خواهد بود و مهاجم یک حمله تکرار قوی را پیاده‌سازی خواهد کرد.

نقض قابلیت گمنامی و غیر قابل پیگیری بودن. در پروتکل روی‌چاودری و همکاران شناسه دستگاه‌های IoT و شناسه گروه یعنی $IMSI_{MTCD_{ij}}$ و GID_i به‌صورت آشکار در کانال عمومی منتشر می‌شوند. ازاین‌رو، مهاجم تنها با شنود کانال می‌تواند هویت دستگاه‌های IoT را شناسایی و پیام‌های آنها را رهگیری کند. بنابراین قابلیت گمنامی و رهگیری پیام‌ها نقض خواهد شد.

نامقاوم در برابر حمله عامل درونی. امنیت کلید نشست باید به گونه‌ای باشد که اگر یکی از اجزای مخفی کلید افشا شود مهاجم نتواند به کلید آن نشست یا کلید نشست‌های قبل و بعد دست یابد؛ یا بتواند حمله جعل را انجام دهد. اگر کلید K_{MTCD_j} افشا شود، مهاجم با دریافت پیام سوم $\langle M_{agg}, H_{agg}\rangle$ یک نانس تصادفی Z^A را انتخاب و مقدار $T1_{HSS} = T_Z^A = (\acute{Q}_\iota) \bmod p$ و $T_Z^A{}_{HSS} = T_Z^A(T1_{Gi}) \bmod p$ و $H^A_{MTCD_{ij-HSS}} = h\left(k_{MTCD_{ij}} \| IMSI_{MTCD_{ij}} \| T_Z^A{}_{MTCD_{ij}}\right)$ را محاسبه می‌کند. سپس با دانستن کلید گروهی GK_i، مطابق مراحل زیر می‌تواند خودش را به‌عنوان یک عضو مورد تایید در گروه جا بزند، و یا یک عضو جعلی را به شبکه اضافه نماید

۱) مهاجم با شنود پیام اول $\{IMSI_{MTCD_{ij}}, GID_i, T1_{MTCD_{ij}}, T1_{G_i}, r_{MTCD_{ij}}, H_{MTCD_{ij}}\}$ به $T1_{G_i}$ و GID_i دست پیدا می‌کند.

۲) مهاجم با دریافت پیام چهارم $\{r_{HSS}, T1_{HSS}, GID_i, H_{HSS}, H_{HSS-agg}\}$ تغییرات را در آن ایجاد می‌کند که ابتدا نانس z^A را انتخاب و $T1^A_{HSS} =$ $H^A_{HSS} =$ و $T2^A_{HSS} = T_z^A(T1_{G_i}) \bmod p$ ،$T_z^{\acute{A}}(\acute{Q}_\iota) \bmod p$ $h(GK_i \| GID_i \| T2^A_{HSS} \| r_{HSS})$ را محاسبه که Q_i کلید عمومی TA است. پیام چهارم جعل‌شده $\{r_{HSS}, T1^A_{HSS}, GID_i, H^A_{HSS}, H_{HSS-agg}\}$ را برای گروه پخش همگانی می‌کند. از آنجا که $H_{HSS} = H^A_{HSS}$ برقرار است، هویت جعلی تایید می‌شود. به این ترتیب عامل درونی متخاصم می‌تواند دستگاه‌های جعلی غیرمجاز را در دیگر نشست‌ها اضافه نماید.

۳- روش پیشنهادی

در اینجا پروتکل پیشنهادی برای ارتباطات ماشینی در محیط IoT ارائه شده است. فازهای پروتکل پیشنهادی مرحله آغازین، ثبت‌نام و احرازهویت و توافق کلید گروهی متقابل است.

۳-۱- مدل سیستم

موجودیت‌ها و نقش‌های پروتکل پیشنهادی در ادامه تعریف شده‌اند.

MTCD[۱۴]. دستگاهی است که می‌تواند اطلاعات را از برنامه‌های کاربردی خاص جمع‌آوری و داده‌ها را برای انجام پردازش‌های بیشتر به سرور MTC ارسال کند. یک MTCD همچنین می‌تواند به‌عنوان یک فعال‌ساز عمل کند و به برخی از دستورات دریافت شده از طرف سرور MTC مجاز، پاسخ دهد. هر MTCD به یک ماژول USIM مجهز و یک شناسه IMSI به آن اختصاص داده شده است. همچنین کلید رمز از پیش به اشتراک گذاشته K بین MTCD و سرور احرازهویت در زمان ثبت‌نام دستگاه به اشتراک گذاشته می‌شود.

گروه MTCDها. تعدادی از MTCDها متناسب با وظیفه‌ای که به آنها اختصاص داده شده است، یک گروه را تشکیل می‌دهند. دستگاه‌ها از قبل تعریف و در سرور احرازهویت (TA) ثبت‌نام می‌شوند. گروه‌ها می‌توانند ثابت و از پیش تعریف شده، یا پویا باشند. MTCDها نیاز دارند تا یکسری داده را به‌صورت دوره‌ای برای سرور ارسال کنند و در صورت نیاز دستوراتی را دریافت کنند و اقدامات متناسب با آن را انجام دهند. آنها همچنین می‌توانند به‌صورت مستقیم از طریق یک کانال خصوصی و یا از طریق رهبر گروه به‌صورت غیرمستقیم در یک کانال ناامن ارتباط برقرار کنند.

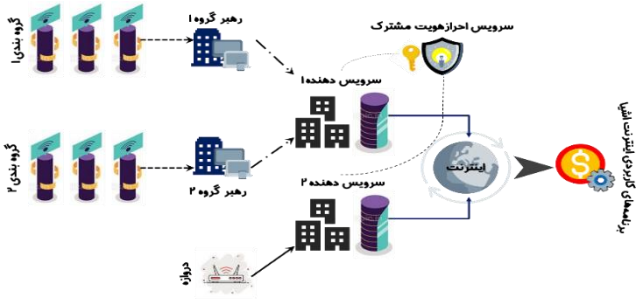
رهبر گروه (GL). با تشکیل گروه، یک عضو از اعضای گروه به‌عنوان رهبر گروه انتخاب می‌شود. طریقه انتخاب می‌تواند به‌صورت تصادفی یا نوبتی - چرخشی، و یا براساس معیارهای مشخصی نظیر: توان مصرفی، طول عمر باتری، گره‌های رهبر انتخاب شده در دوره‌های قبل و مانند آن باشد. همچنین می‌توان یک گره ثابت مانند گره

دروازه یا مسیریاب که در مقایسه با MTCDهای معمولی قدرت محاسباتی و ارتباطی بیشتری دارند را به‌عنوان رهبر گروه در نظر گرفت. در این حالت، فرایند انتخاب GL سربار کمتری خواهد داشت که سبب بهبود کارایی می‌گردد. بااین‌حال، محدودیت‌هایی را برای محیط‌های پویا و متحرک به‌وجود خواهد آورد.

سرور احرازهویت (TA). دارای یک مخزن اشتراکی متمرکز است که تمام مشترکین یک شبکه خاص در آن ثبت شده‌اند و مسئول احرازهویت تمامی MTCDها قبل از دادن اجازه دسترسی به شبکه است. در اینجا، سرور ارائه دهنده خدمات و سرور احرازهویت به‌عنوان یک موجودیت در نظر گرفته شده‌اند.

۳-۲- مدل شبکه

در اینجا مدل ارتباطی ماشینی (MTC) به‌عنوان مثال وسیله نقلیه با هرچیزی (V2X)[۱۵] که اجازه می‌دهد تا وسایل نقلیه با دیگر اعضای موجود در شبکه سیستم ترافیکی ارتباط تک‌گام یا چندگام و همچنین ارتباطات گروهی داشته باشند را در نظر می‌گیریم. مدل پیشنهادی در شکل ۱ نشان داده شده است. کاربردهایی که می‌توان برای این سناریو در نظر گرفت، یک سناریوی معمولی کنتورهای هوشمند است که می‌تواند برای مدیریت سودمندی، نظارت محیط، کنترل مصرف برق و سایر کاربردهای مشابه به‌کار گرفته شود.



شکل ۱: مدل پیشنهادی

شناسه گروه GID_i و کلید گروه GK_i در فاز توافق کلید گروهی به اشتراک گذاشته می‌شود. دستگاهی که بالاترین قابلیت ارتباطی و بیش‌ترین ظرفیت ذخیره‌سازی را داشته باشد، به‌عنوان رهبر گروه انتخاب می‌شود. گروه پویا است؛ به‌عبارتی عضویت در گروه می‌تواند با ورود یک عضو جدید و یا حذف یکی از اعضای گروه تغییر کند. گروه می‌تواند به‌صورت یک درخت باینری مجازی تشکیل شود. دستگاه‌های MTCD به‌عنوان گره‌های برگ انتخاب می‌شوند.

ایجاد گروه در سه فاز اختصاص کلید خصوصی به هر دستگاه، ساخت درخت باینری توسط اعضای گروه، ایجاد کلید گروه و اشتراک آن بین سرور ابر و اعضای گروه انجام می‌شود. رمزواره‌ای که در گره ریشه / رهبر محاسبه می‌شود، به‌عنوان رمزواره گروه در نظر گرفته می‌شود. کلید گروه پیشنهادی، حریم خصوصی بین دستگاه‌ها و سرور ابر و همچنین احرازهویت متقابل را فراهم می‌آورد. در مدل پیشنهادی، سرور احرازهویت، در هر درخواست دستگاه‌های IoT را به‌صورت گروهی احرازهویت می‌کند. هر دروازه به‌عنوان رهبر گروه (GL) فعالیت می‌کند. دستگاه‌های عضو وظیفه ارسال شناسه‌های مخفی خود به GL را دارند. GL همگی شناسه‌ها را در قالب یک پیام برای TA ارسال می‌کند. اعضای گروه و TA باید به‌صورت متقابل یکدیگر را احرازهویت کنند.

۳-۳- پروتکل پیشنهادی

پروتکل پیشنهادی یک کاربرد از چندجمله‌ای چبیشف بسط‌یافته را لحاظ می‌کند تا یک پروتکل احرازهویت و توافق کلید گروهی متقابل برای ارتباطات ماشینی را معرفی کند. در پروتکل پیشنهادی، تعدادی از MTCDها در قالب یک گروه، اعضای گروه را احرازهویت می‌کنند. هنگامی‌که احرازهویت با موفقیت انجام پذیرد، یک کلید گروه مشترک بین اعضای گروه و هسته شبکه (سرور احرازهویت) ایجاد می‌شود. سپس، اعضای گروه پروتکل احرازهویت متقابل و توافق کلید گروهی را شروع می‌کنند. MTCD پیام درخواست احرازهویت خود را برای GL ارسال می‌کند؛ GL پیام‌های دریافتی را تجمیع و یک پیام واحد را برای TA ارسال می‌کند.

۳-۳-۱- مرحله آغازین

شامل انتشار پارامترهای عمومی توسط TA است. TA الگوریتم رمزنگاری و رمزگشایی $Enc(.)/Dec(.)$ را انتخاب و مقدار $x \epsilon (-\infty, +\infty)$ را به‌عنوان مقدار اولیه برای چندجمله‌ای چبیشف $T(.)$ انتخاب می‌کند. سپس عدد تصادفی $s \epsilon Z_p^*$ را به‌عنوان شاه‌کلید خصوصی خود اتخاذ، و کلید عمومی خود را به‌صورت $Q_{TA} = T_s(x)\ mod\ p$ محاسبه می‌کند که p یک عدد اول بسیار بزرگ است. علاوه‌براین، تابع هش یک‌طرفه $h(.)$ را انتخاب و پارامترهای $\{p, x, T(.), Q_{TA}, h(.), Enc(.)/Dec(.)\}$ را در فضای عمومی منتشر می‌کند و کلید خصوصی s را نزد خود مخفی نگه می‌دارد. TA شماره IMSI و شماره پین PIN_j را به هر دستگاه MTCD اختصاص می‌دهد که به‌صورت ایمن در حافظه آن‌ها نگهداری می‌شود. از PIN_j در فاز ثبت‌نام MTCD استفاده می‌شود.

۳-۳-۲- مرحله ثبت‌نام دستگاه MTCD

هنگامی‌که MTCD برای اولین بار در TA ثبت‌نام می‌کند، کلیه مراحل ایجاد کلید خصوصی و عمومی انجام می‌شود و یک کلید

عمومی را از طریق کانال ایمن دریافت می‌کند. $IMSI_{MTCD_j}$ نشان دهنده شناسه اشتراک بین‌المللی j اُمین MTCD و PIN_j به‌عنوان کلید مخفی بین $MTCD_j$ و TA است. در طول فاز آغازین، $MTCD_j$ به کمک کلید خصوصی s_j کلید عمومی خود را به‌صورت $Q_j = T_x(s_j) mod\ p$ ایجاد می‌کند. همچنین $MTCD_j$ یک شماره توالی SQN_j را با TA به اشتراک می‌گذارد؛ که بعد از هر بار احرازهویت موفق یک واحد به آن اضافه می‌شود. $MTCD_j$ مطابق مراحل زیر توسط TA ثبت‌نام می‌شود.

مرحله ۱. $MTCD_j$ شناسه $IMSI_{MTCD_j}$ و شماره پین PIN_{MTCD_j} را وارد می‌کند. عدد تصادفی $s_j \in Z_q^*$ را به‌عنوان کلید خصوصی خود انتخاب و مقادیر $Q_j = T_{s_j}(x)\ mod\ p$، $K_j = T_{s_j}(Q_{TA}) mod\ p$، $HID_j = IMSI_{MTCD_j} \oplus h(K_j \| t_1)$ و $MP_j = h(IMSI_{MTCD_j} \| PIN_j \| Q_j \| K_j \| t_1)$ را محاسبه که t_1 زمان تولید پیام است. پیام $\{HID_j, MP_j, Q_j, t_1\}$ را برای TA در کانال خصوصی ارسال می‌کند.

مرحله ۲. TA با دریافت پیام $\{HID_j, MP_j, Q_j, t_1\}$ در زمان t_2، ابتدا شرط $|t_2 - t_1| \le \Delta t$ بررسی می‌کند. در صورت تازه بودن، مقدار $K_j' = T_s(Q_j) mod\ p$ را محاسبه و $IMSI_{MTCD_j} = HID_j \oplus h(K_j' \| t_1)$ را بازیابی و اعتبار آن را در پایگاه داده خود بررسی می‌کند؛ اگر موجود نباشد از کاربر درخواست یک شناسه دیگر می‌شود. در صورتی‌که شناسه وجود داشته باشد مقدار PIN_j فراخوانی و $MP_j' = h(IMSI_{MTCD_j} \| PIN_j \| Q_j \| K_j' \| t_1)$ محاسبه می‌شود. سپس $MP_j' ?= MP_j$ ارزیابی و درصورت برقرار بودن، صحت مقادیر دریافتی تائید می‌شود. TA سپس عدد تصادفی r_j را انتخاب و مقادیر $e_j = h(PIN_j \| K_j') \oplus r_j$، $M_j = T_s\left(T_{r_j}(x)\right) mod\ p$، و $F_j = h\left(M_j \| IMSI_{MTCD_j} \| r_j \| t_2\right)$ را محاسبه می‌کند و پیام $\{F_j, e_j, SQN_j, t_2\}$ را از طریق یک کانال امن در اختیار $MTCD_j$ قرار می‌دهد. TA همچنین Q_j و SQN_j متناظر با $IMSI_{MTCD_j}$ را در پایگاه داده خود ذخیره می‌کند.

مرحله ۳. پس از دریافت $\{F_j, e_j, t_2\}$ توسط $MTCD_j$ و بررسی شرط تازه بودن پیام، دستگاه $MTCD_j$ مقدار $r_j = e_j \oplus h(PIN_j \| K_j')$ و $M_j' = T_{r_j}(Q_{TA}) mod\ p$ را محاسبه و شرط $F_j ?= h(M_j' \| IMSI_{MTCD_j} \| r_j \| t_2)$ را ارزیابی می‌کند. اگرشرط برقرار باشد، $MTCD_j$ مقدار M_j را درون حافظه خود ذخیره می‌کند. خلاصه این مرحله در شکل ۲ نشان داده شده است.

۳-۳-۳- تشکیل گروه و ایجاد کلید گروه

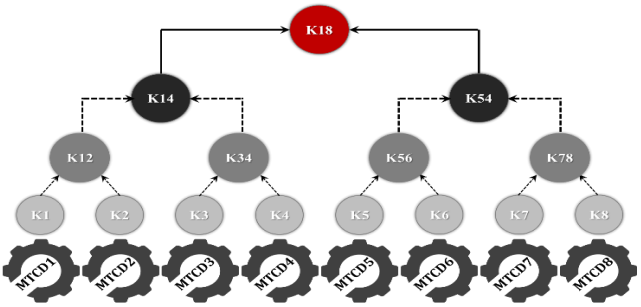
هر دستگاه در تولید کلید گروه سهیم است. اعضای گروه i اُم با شناسه GID_i کلید GK_i را با یکدیگر به اشتراک می‌گذارند. برای ایجاد کلید مشترک بین دستگاه‌های عضو، می‌توان از یک ساختار

دستگاه $MTCD_j$	سرور احرازهویت TA
وارد کردن PIN_j، $IMSI_j$ تولید کلید خصوصی $s_j \in Z_q^*$ و محاسبه $Q_j = T_{s_j}(x)\ mod\ p, K_j = T_{s_j}(Q_{TA}) mod\ p$ $HID_j = IMSI_{MTCD_j} \oplus h(K_j \| t_1), MP_j = h(IMSI_{MTCD_j} \| PIN_j \| Q_j \| K_j \| t_1)$ HID_j, MP_j, Q_j, t_1 ← ارسال در کانال خصوصی	
	بررسی تازگی پیام $|t_2 - t_1| \le \Delta t$ و محاسبه $K_j' = T_s(Q_j)\ mod\ p, IMSI_{MTCD_j} = HID_j \oplus h(K_j' \| t_1)$ فراخوانی PIN_j و محاسبه $MP_j' = h(IMSI_{MTCD_j} \| PIN_j \| Q_j \| K_j' \| t_1)$ بررسی شرط $MP_j' ?= MP_j$ و پذیرفتن Q_j به‌عنوان کلید عمومی معتبر، تولید عدد تصادفی $r_j \in Z_q^*$ و محاسبه $e_j = h(PIN_j \| K_j') \oplus r_j, \quad M_j = T_s\left(T_{r_j}(x)\right) mod\ p, \quad F_j = h(M_j \| IMSI_{MTCD_j} \| r_j \| t_2)$ حذف PIN_j، ذخیره Q_j، M_j و SQN_j در حافظه دیتابیس متناظر با $IMSI_{MTCD_j}$ $\{F_j, e_j, SQN_j, t_2\}$ → ارسال در کانال خصوصی
بررسی تازگی پیام، و محاسبه $r_j = e_j \oplus h(PIN_j \| K_j'), M_j' = T_{r_j}(Q_{TA}) mod\ p$ $F_j ?= h(M_j' \| IMSI_{MTCD_j} \| r_j \| t_2)$ پذیرفتن (s_j, Q_j) به‌عنوان زوج کلید عمومی و خصوصی و ذخیره M_j و SQN_j	

شکل ۲: مرحله ثبت‌نام دستگاه $MTCD_j$ در سرور احرازهویت

درخت باینری مجازی استفاده کرد؛ که عضوها معادل برگ‌ها هستند و کلید تولید شده در ریشه درخت قرار می‌گیرد (شکل ۳).

ابتدا MTCD1 اعداد تصادفی x, y_1 و عدد اول p را تولید می‌کند؛ که Q_1 کلید عمومی این دستگاه است. سپس با کمک چندجمله‌ای چبیشف توکن $T_{MTCD_1} = T_{y_1}(x)\ mod\ p$ را محاسبه و مقادیر x، p و T_{MTCD_1} را به کل گروه همه‌پخشی می‌کند. MTCD2 عدد تصادفی y_2 را انتخاب و $T_{MTCD_2} = T_{y_2}(x)\ mod$ را محاسبه و همه‌پخشی می‌کند. این دو دستگاه می‌توانند همزمان توکن T_{12} را به‌صورت $T_{12} = T_{y_1}(T_{y_2}(x))mod\ p = T_{y_2}(T_{y_1}(x))\ mod\ p$ تولید کنند. همین عمل بین بقیه دستگاه‌ها دو به دو انجام می‌شود. حال در هر زیردرخت، سمت چپ‌ترین گره (مثلا MTCD1 در زیر درخت سمت چپ با ریشه T_{12})، به‌عنوان نماینده زیرگروه، مقدار چندجمله‌ای $T_{14}(x)$ را محاسبه و به کل گروه همه‌پخشی می‌کند. گره نماینده یک گره معمولی است که فقط مقدار چندجمله‌ای‌ها را حساب می‌کند. دیگر گره‌ها می‌توانند این محاسبات را تأئید و وارسی کنند. هر یک از دستگاه‌های MTCD1 تا MTCD4 می‌توانند کلید مشترک بین این چهار گره را به‌صورت $T_{14} = T_{y_1}(T_{y_2}(T_{y_3}(T_{y_4}(x))))mod\ p$ محاسبه کنند.

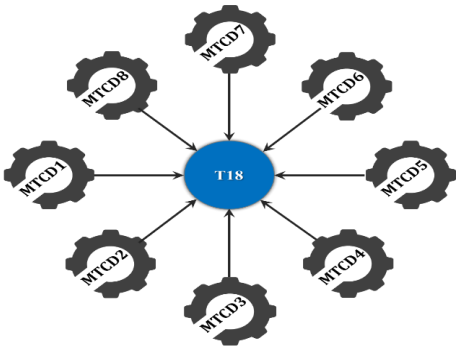


شکل ۳: ساختار درختی سلسله مراتبی برای ایجاد کلید گروه

کلید گره‌های MTCD5 تا MTCD8 به‌صورت $T_{58} = T_{y_5}(T_{y_6}(T_{y_7}(T_{y_8}(x))))mod\ p$ محاسبه می‌شود. MTCD1 (سمت چپ‌ترین گره در زیر درخت سمت چپ با ریشه k_{14}) مقدار چندجمله‌ای $T_{18}(x)$ را محاسبه و به کل گروه همه‌پخشی می‌کند. هر یک از گره‌های MTCD5 تا MTCD8 و گره‌های MTCD1 تا MTCD4 کلید مشترک گروه را به‌صورت $GK_i = h(T_{18} \parallel p \parallel \sum HID_j \parallel GID_i \parallel Extract(t_{ij}))$ محاسبه می‌نمایند.

تابع $Extract$، ۳۲ بیت اول از t_{ij} را استخراج می‌کند. فرض شده است که همه MTCDها درون گروه با یکدیگر همزمان هستند. این کار از طریق پروتکل زمان شبکه (NTP)[۱۶] [۳۱،۳۲] صورت می پذیرد. می‌توان ساختار تشکیل گروه را به‌صورت یک دایره مجازی در نظر گرفت، به‌گونه‌ای که همه گره‌ها توکن مخصوص خود را با دیگر گره‌ها به اشتراک می‌گذارند (شکل ۴).

اضافه و حذف یک عضو. ممکن است عضو جدیدی به گروه اضافه شود و یا گروه را ترک کند؛ در این‌صورت، کلید گروه باید تعویض گردد. دستگاه جدید عدد تصادفی خصوصی y_j را تولید و مقدار $T_{y_j}(x)mod\ p$ را محاسبه و یک پیام حاوی درخواست پیوستن به همراه مقدار $T_{y_j}(x)\ mod\ p$ را به کل گروه همه‌پخشی می‌کند. بعد از تشخیص محل درج دستگاه، همه اعضا درخت مجازی را با درج گره جدید به‌روز می‌کنند. با حذف یک عضو، محاسباتی که آن در آنها دخیل بوده است تغییر، و نتیجه در کل گروه همه‌پخشی می‌شود؛ که در پی آن کلید گروه به‌روزرسانی می‌شود.



شکل ۴: ساختار دایره‌ای برای ایجاد کلید گروه

۳-۳-۴- احرازهویت متقابل و توافق کلید

در این مرحله، هر MTCD عضو گروه، اطلاعات خود را برای رهبر گروه (GL) ارسال می‌کند؛ که GL وظیفه جمع‌آوری، تجمیع و ارسال آنها برای هسته شبکه را دارد. TA اعضای گروه و GL را احرازهویت و کلید نشست یک به یک را ایجاد می‌کند. علاوه‌براین، MTCDها کلید نشستی که به دست آورده‌اند را در گروه خود احرازهویت می‌کنند. این کار به کمک یک توکن که به‌صورت انفرادی برای هر عضو گروه ارسال می‌گردد، انجام می‌شود.

تولید پیام احرازهویت. $MTCD_{ij}$ عدد تصادفی y_j را تولید و توکن‌های $T1_{MTCD_{ij}} = T_{y_j}(Q_j)\ mod\ p$ و $T2_{MTCD_{ij}} = T_{y_j}\left(T_{s_j}(Q_{TA})\right)mod\ p$ را ایجاد می‌کند. $t_{ij} = Extract\ (Time: sec + ms)$، $GK_i = h(T_{1n} \parallel p \parallel \sum HID_j \parallel GID_i \parallel t_{ij})$، $HID_j = IMSI_j \oplus h(T2_{MTCD_{ij}} \parallel t_{ij})$ $m =$، $Token_{G_i} = h(h(GK_i \parallel t_{ij}) \parallel \cup_{j=1}^{l} HID_j \parallel GID_i)$، $T1_{G_i} = h\left(Token_{G_i} \parallel GID_i \parallel T_m\left(h(GK_i \parallel t_{ij})\right)mod\ p\right)$ را محاسبه می‌کند. فرمت مهرزمانی t_{ij} در NTP، ۶۴ بیتی است که ۳۲ بیت اول ثانیه و ۳۲ بیت دوم صدم‌ثانیه را نشان می‌دهد. GID_i شناسه گروه تشکیل شده و HID_j شناسه مخفی شده مربوط به هر $MTCD_{ij}$ است. مقدار $H_{MTCD_{ij}}$

$h\left(IMSI_j \parallel HID_j \parallel Token_{G_i} \parallel T1_{MTCD_{ij}} \parallel M_j \parallel T1_{G_i} \parallel t_{ij}\right)$ را محاسبه و پیام احرازهویت $< H_{MTCD_{ij}}, T1_{MTCD_{ij}}, HID_i, T1_{G_i}, Time >$ را ارسال می‌کند.

رهبر گروه. رهبر گروه پیام‌های احرازهویت را دریافت و ارزیابی می‌کند که آیا $T1_{G_i}$ها برابر هستند یا خیر. این کار سبب می‌شود که تنها گره‌های معتبر و همگام‌شده بتوانند در عملیات تجمیع شرکت داده شوند. سپس رهبر گروه مقدار $R_i = h(GK_i \parallel t_{ij}) \oplus h(T2_{MTCD_{GL}} \parallel T1_{G_i})$ را محاسبه و هش تجمیع‌شده $H_{agg} = H_{MTCD_{i1}} \oplus H_{MTCD_{i2}} \oplus \dots \oplus H_{MTCD_{il}}$ را ایجاد می‌کند و پیام تجمیع‌شده $M_{agg} = \cup_{j=1}^{l}\left(HID_j \parallel T1_{MTCD_{ij}}\right)$ را برای کل گروه با l عضو تولید می‌کند. در نهایت رهبر گروه پیام احرازهویت $< R_i, H_{agg}, M_{agg}, GID_i, T1_{G_i}, t_{ij} >$ را برای TA ارسال می‌کند.

احرازهویت و تولید کلید. TA با دریافت درخواست احرازهویت، MTCDهای فردی و گروهی را احرازهویت می‌کند. این کار با محاسبه $T2^*_{MTCD_{ij}} = T_s(Q_j \left(T1_{MTCD_{ij}}\right)) mod\ p$ و $IMSI_j = HID_j \oplus h(T2^*_{MTCD_{ij}} \parallel t_{ij})$ صورت می‌پذیرد. سپس M_j را بازیابی و مقادیر $m^* = h(GK_i \parallel t_{ij}) = R_i \oplus h(T2_{MTCD_{GL}} \parallel T1_{G_i})$، $Token^*_{G_i} = h(h(GK_i \parallel t_{ij}) \parallel \cup_{j=1}^{l} HID_j \parallel GID_i)$ و $T1''_{G_i} ? = T_m\left(h(GK_i \parallel t_{ij})\right) mod\ p$ را محاسبه و TA با بررسی $h\left(Token^*_{G_i} \parallel GID_i \parallel T_{ij}\right)$ توکن گروه را اعتبارسنجی می‌کند.

$H^*_{MTCD_{ij}} = h\left(IMSI_j \parallel HID_j \parallel Token^*_{G_i} \parallel T1_{MTCD_{ij}} \parallel M_j \parallel T1_{G_i} \parallel t_{ij}\right)$ و $H^*_{agg} = H^*_{MTCD_{i1}} \oplus H^*_{MTCD_{i2}} \oplus \dots \oplus H^*_{MTCD_{il}}$ را محاسبه می‌کند. اگر برای هر عضو $H^*_{MTCD_{ij}} = H_{MTCD_{ij}}$ و $H^*_{agg} = H_{agg}$ برابر باشند شرایط احرازهویت اعضای گروه با پیام احرازهویت M_{agg} موفقیت انجام شده است.

بر مبنای ویژگی شبه‌گروه و به کمک چندجمله‌ای چبیشف برای هر j داریم $H^*_{MTCD_{ij}} = H_{MTCD_{ij}}$. اگر $H^*_{agg} = H_{agg}$ باشد، MTCDها احرازهویت می‌شوند. این به این معنا است که محاسبات تمامی $H_{MTCD_{ij}}$ها با موفقیت به انجام رسیده است. محاسبه صحیح $T2_{MTCD_{ij}}$ به‌صورت زیر است

$$T2_{MTCD_{ij}} = T_{y_j}\left(T_{s_j}(T_s(x))\right) mod\ p = T_s\left(T_{y_j}\left(T_{s_j}(x)\right)\right) mod\ p = T_s\left(T_{y_j}(Q_j)\right) mod\ p = T_s\left(T1_{MTCD_{ij}}\right) mod\ p = T2^*_{MTCD_{ij}} \quad (۸)$$

با توجه به احرازهویت MTCDها، TA یک توکن را تولید می‌کند تا به کمک آن گره‌های عضو بتوانند او را احرازهویت کنند. این مراحل در ادامه شرح داده شده است. TA عدد تصادفی z را تولید، و مقادیر $T1_{TA}$، $T2_{TA}$ و $T3_{TA}$ را به ازای هر گروه به‌صورت $T1_{TA} = T_z(Token_{G_i}) mod\ p$، $T2_{TA} = T_z(h(GK_i \parallel t_{ij})) mod\ p$ و $T3_{TA} = T_z(x) mod\ p$ محاسبه می‌کند. سپس $T4_{TA} = T_z\left(T1_{MTCD_{ij}}\right) mod\ p$ را به ازای هر عضو محاسبه می‌کند.

برای محاسبه کلید نشست، TA کلید نشست $K^{ASME}_{MTCD_{ij}}$ را برای هر $MTCD_{ij}$ در گروه i به‌صورت $K^{ASME}_{MTCD_{ij}} = h(T2^*_{MTCD_{ij}} \oplus M_j \parallel T4_{TA} \parallel t_{TA})$ محاسبه می‌کند. t_{TA} مهر زمانی در زمان تولید پیام است. جدول اطلاعات اعضای گروه با ۳ ستون $IMSI$، $K^{ASME}_{MTCD_{ij}}$ و GID_i ایجاد می‌شود. TA مقادیر $CID_{Gl} = HID_{GL} \oplus h(K^{ASME}_{MTCD_{ij}} \parallel SQN_{ij} \parallel t_{TA})$، $R_T = h(Token_{G_i} \parallel HID_{GL} \parallel \cup_{j=1}^{l} HID_j)$ و $H_{TA} = h(R_T \parallel GID_i \parallel CID_{Gl} \parallel T2_{TA})$ و برای هر MTCD مقدار $H_{MTCD_{ij-TA}} = h\left(K^{ASME}_{MTCD_{ij}} \parallel IMSI_{MTCD_{ij}} \parallel T2_{MTCD_{ij}} \parallel T4_{HSS} \parallel CID_{Gl} \parallel t_{TA}\right)$ را محاسبه می‌کند. سپس پیام پاسخ تجمیع را به‌صورت $H_{TA-agg} = \cup_{j=1}^{l}\left(H_{MTCD_{ij-TA}}\right)$ تولید می‌کند و پیام $< T1_{TA}, T3_{TA}, H_{TA}, H_{TA-agg}, t_{TA}, t_{TA} >$ را با کمک اطلاعات عضویت موجود در گروه برای GL ارسال می‌کند.

GL پیام را برای اعضای گروه برادکست می‌کند. به‌محض دریافت پیام از طرف GL، اعضای گروه، TA را احرازهویت می‌کنند و مقادیر $T2^*_{TA} = T_m(T1_{TA}) mod\ p$، $T4^*_{TA} = T_{y_j}(T3_{TA}) mod\ p$، $K^{ASME}_{MTCD_{ij}} = h(T2_{MTCD_{ij}} \oplus M_j \parallel T4^*_{TA} \parallel T_{ij})$، $CID_{Gl} = HID_{GL} \oplus h(K^{ASME}_{MTCD_{ij}} \parallel SQN_{ij} \parallel t_{TA})$، $R_T = h(Token_{G_i} \parallel HID_{GL} \parallel \cup_{j=1}^{l} HID_j)$ و $H^*_{TA} = h(GK_i \parallel GID_i \parallel CID_{Gl} \parallel T2^*_{TA})$ را محاسبه می‌کنند. اگر $H^*_{TA} = H_{TA}$ برقرار باشد، TA توسط MTCD احرازهویت می‌شود. خاصیت شبه‌گروه چندجمله‌ای چبیشف نشان می‌دهد که این مقادیر با یکدیگر برابر خواهند بود.

$$T2'_{TA} = T_m(T1_{TA}) mod\ p = T_m\left(T_z(k_{G_i})\right) mod\ p = T_z\left(T_m(k_{G_i})\right) mod\ p = T_z\left(Token_{G_i}\right) mod\ p = T2_{TA} \quad (۹)$$

$$H'_{TA} = h(GK_i \parallel GID_i \parallel CID_{Gl} \parallel T2^*_{TA}) = h(GK_i \parallel GID_i \parallel CID_{Gl} \parallel T2_{TA}) = H_{TA} \quad (۱۰)$$

$MTCD_{ij}$ اطلاعات $IMSI$ خود و $H_{MTCD_{ij-TA}}$ را از H_{TA-agg} را استخرج می‌کند. و آن را با استفاده از شرط ارزیابی $H_{MTCD_{ij-TA}} = h\left(K^{ASME}_{MTCD_{ij}} \parallel IMSI_{MTCD_{ij}} \parallel T2_{MTCD_{ij}} \parallel T4_{TA} \parallel CID_{Gl} \parallel t_{TA}\right)$ تأئید می‌کند. اگر شرط و قرار باشد، TA توسط MTCD مجاز قلمداد می‌شود. MTCDها کلید نشست $K^{ASME}_{MTCD_{ij}}$ را به دست می‌آورد. درغیراین‌صورت، کلید نامعتبر خواهد بود. شکل ۵ پیام‌های مبادله شده در پروتکل پیشنهادی را نشان می‌دهد.

Mobile Device ($MTCD_j$)	Group Leader	TA Server
Chooses nonce $y_j \epsilon Z_q^*$ then Computes $T1_{MTCD_{ij}} = T_{y_j}(Q_j)\ mod\ p$ $t_{ij} = Extract\ (Time: sec + ms)$ $GK_i = h(T_{1n} \parallel p \parallel \sum HID_j \parallel GID_i \parallel t_{ij})$ $T2_{MTCD_{ij}} = T_{y_j}\left(T_{s_j}(Q_{TA})\right) mod\ p$ $HID_j = IMSI_j \oplus h(T2_{MTCD_{ij}} \parallel t_{ij})$ $m = h(h(GK_i \parallel t_{ij}) \parallel \bigcup_{j=1}^{l} HID_j \parallel GID_i)$ $Token_{G_i} = T_m\left(h(GK_i \parallel t_{ij})\right) mod\ p$ $T1_{G_i} = h\left(Token_{G_i} \parallel GID_i \parallel t_{ij}\right)$ $H_{MTCD_{ij}} = h\left(IMSI_j \parallel HID_j \parallel Token_{G_i} \parallel T1_{MTCD_{ij}} \parallel M_j \parallel T1_{G_i} \parallel t_{ij}\right)$ $< H_{MTCD_{ij}}, T1_{MTCD_{ij}}, HID_i, T1_{G_i}, Time >$ →	Checks Freshness $T1'_{G_i} ? = T1_{G_i}$ computes $R_i = h(GK_i \parallel t_{ij}) \oplus h(T2_{MTCD_{GL}} \parallel T1_{G_i})$ $H_{MTCD_{ij}} = h\begin{pmatrix} R_i \parallel IMSI_{GL} \parallel HID_{GL} \parallel Token_{G_i} \parallel \\ T1_{MTCD_{iGL}} \parallel M_{GL_j} \parallel T1_{G_i} \parallel t_{ij} \end{pmatrix}$ $H_{agg} = H_{MTCD_{i1}} \oplus \dots \oplus H_{MTCD_{il}}$ $M_{agg} = \bigcup_{j=1}^{l} \left(HID_j \parallel T1_{MTCD_{ij}}\right)$ $< R_i, H_{agg}, M_{agg}, GID_i, T1_{G_i}, t_{ij} >$ →	Verifies timestamp $\lvert t_{ij}^* - t_{ij} \rvert < \Delta T$ Computes $T2^*_{MTCD_{ij}} = T_s(\left(T1_{MTCD_{ij}}\right)) mod\ p$ $IMSI_j = HID_j \oplus h(T2^*_{MTCD_{ij}} \parallel t_{ij})$ Retrieve M_j and computes $h(GK_i \parallel t_{ij}) = R_i \oplus h(T2_{MTCD_{GL}} \parallel T1_{G_i})$ $m^* = h(h(GK_i \parallel t_{ij}) \parallel \bigcup_{j=1}^{l} HID_j \parallel GID_i)$ $Token^*_{G_i} = T_m\left(h(GK_i \parallel t_{ij})\right) mod\ p$ $T1''_{G_i} ? = h\left(Token^*_{G_i} \parallel GID_i \parallel T_{ij}\right)$ $H^*_{MTCD_{ij}} = h\left(IMSI_j \parallel HID_j \parallel Token^*_{G_i} \parallel T1_{MTCD_{ij}} \parallel M_j \parallel T1_{G_i} \parallel t_{ij}\right)$ $H^*_{agg} = H^*_{MTCD_{i1}} \oplus H^*_{MTCD_{i2}} \dots \oplus H^*_{MTCD_{il}}$ $H^*_{agg} = ? H_{agg}$ Chooses nonce $z \epsilon Z_q^*$ then Computes: $; T1_{TA} = T_z(k_{G_i})\ mod\ p$ $; T2_{TA} = T_z(Token_{G_i}) mod\ p$ $; T3_{TA} = T_z(x)\ mod\ p$ $T4_{TA} = T_z\left(T1_{MTCD_{ij}}\right)\ mod\ p$ $K^{ASME}_{MTCD_{ij}} = h(T2^*_{MTCD_{ij}} \oplus M_j \parallel T4_{TA} \parallel t_{TA})$ $CID_{Gl} = HID_{GL} \oplus h(K^{ASME}_{MTCD_{ij}} \parallel SQN_{ij} \parallel t_{TA})$ $R_T = h(Token_{G_i} \parallel HID_{GL} \parallel \bigcup_{j=1}^{l} HID_j)$ $H_{TA} = h(R_T \parallel GID_i \parallel CID_{Gl} \parallel T2_{TA})$ $H_{MTCD_{ij}-TA} = h\left(K^{ASME}_{MTCD_{ij}} \parallel IMSI_{MTCD_{ij}} \parallel T2_{MTCD_{ij}} \parallel T4_{TA} \parallel CID_{Gl} \parallel H_{TA} \parallel t_{TA}\right)$ $H_{TA-agg} = \bigcup_{j=1}^{l} \left(H_{MTCD_{ij}-TA}\right)$ $< T1_{TA}, T3_{TA}, H_{TA}, H_{TA-agg}, t_{TA} >$ ←
Computes $T2^*_{TA} = T_m(T1_{TA})\ mod\ p$ $T4^*_{TA} = T_{s_j}(T_{y_j}(T3_{TA}))\ mod\ p$ $K^{ASME}_{MTCD_{ij}} = h(T2_{MTCD_{ij}} \oplus M_j \parallel T4^*_{TA} \parallel t_{TA})$ $CID_{Gl} = HID_{GL} \oplus h(K^{ASME}_{MTCD_{ij}} \parallel SQN_{ij} \parallel t_{TA})$ $R_T = h(Token_{G_i} \parallel HID_{GL} \parallel \bigcup_{j=1}^{l} HID_j)$ $H_{TA} = ?\ h(R_T \parallel GID_i \parallel CID_{Gl} \parallel T2^*_{TA})$ $H_{MTCD_{ij}-TA} ? = h\left(K^{ASME}_{MTCD_{ij}} \parallel IMSI_{MTCD_{ij}} \parallel T2_{MTCD_{ij}} \parallel T4_{TA} \parallel CID_{Gl} \parallel H_{TA} \parallel t_{TA}\right)$ Accept $GK_i, HID_{GL}, K^{ASME}_{MTCD_{ij}}$	Checks $\lvert t^*_{TA} - t_{TA} \rvert < \Delta T$ Computes $< T1_{TA}, T3_{TA}, H_{TA}, H_{TA-agg}, t_{TA} >$ ←	

شکل ۵: توافق کلید و احرازهویت گروهی در پروتکل پیشنهادی

۴- ارزیابی امنیت

در این بخش تحلیل امنیتی پروتکل پیشنهادی تحت مدل اوراکل تصادفی [۳۵،۳۴،۳۳،۳۱] برپایه فرضیات مساله دیفی هلمن مبتنی بر نقشه چبیشف (CMDHP) ارائه شده است. علاوه‌براین، تحلیل و ارزیابی غیررسمی پروتکل پیشنهادی و مقاومت در برابر انواع حملات شناخته شده بررسی گردیده است.

۴-۱- تحلیل رسمی امنیت با مدل اوراکل تصادفی

این تحلیل براساس مدل بلار و راگ‌وی [۳۴] و بازی‌های متوالی [۳۵] صورت گرفته است. دو شرکت‌کننده MTCD و TA در مرحله

احرازهویت و توافق کلید گروهی با Π نشان داده‌اند. Π_p^k، k اُمین نمونه از شرکت‌کننده p در یک نشست از پروتکل را نشان می‌دهد و به‌عنوان اوراکل شناخته می‌شود. $MTCD_{ij}$ کلید بلندمدت M_{ij} و رمز موقت $K_{MTCD_{ij}}^{AMSE}$ را با TA به اشتراک می‌گذارد. علاوه‌براین، اعضای گروه i اُم کلید گروهی GK_i را با هم به اشتراک می‌گذارند.

۴-۱-۱- ادوات

شریک[۱۷]. دو نمونه Π_{MTCD}^i و Π_{TA}^i به‌عنوان شریک در نظر گرفته می‌شوند، یعنی $PID(\Pi_{MTCD}^i) = \Pi_{TA}^i$ و $PID(\Pi_{TA}^i) = \Pi_{MTCD}^i$ اگر شرایط زیر فراهم باشد

- هر دو در حالت پذیرش[۱۸] باشند. یعنی هر نمونه آخرین پیام مورد انتظار را دریافت کرده باشد، کلید نشست را ایجاد کنند، و به‌طور متقابل یکدیگر را احرازهویت کنند.
- شناسه نشست هر دو یکسان باشد. شناسه نشست به دو شرکت‌کننده و پیام‌های مبادله شده بین آنها الحاق می‌شود.

تازگی. نمونه Π^k یک نمونه تازه است، اگر کلید نشست $K_{MTCD_{ij}}^{AMSE}$ یا GK_i توسط مهاجم $\mathcal{A}$ زمانی‌که جستار[۱۹] $Reveal(\Pi^k)$ را اعمال می‌کند، قابل افشا نباشد.

مهاجم. تحت مدل ROR، مهاجم $\mathcal{A}$ می‌تواند به جستارهای زیر دسترسی داشته باشد.

- جستار اجرا $Execute(\Pi_{MTCD}^i, \Pi_{TA}^i)$ مهاجم با شبیه‌سازی حمله غیرفعال پیام‌های مبادله شده در کانال عمومی بین Π_{MTCD}^i و Π_{TA}^i را شنود می‌کند.
- جستار ارسال $Send(\Pi_p^i, m)$ حمله فعال را شبیه‌سازی می‌کند؛ مهاجم پیام m را جعل و آن را برای نمونه Π_p^i ارسال می‌کند. $\mathcal{A}$ برای دریافت پاسخ این جستار را اجرا می‌کند.
- جستار افشا $Reveal(\Pi_p^i)$ حمله دانستن کلید نشست را پیاده‌سازی می‌کند؛ که به موجب آن، $\mathcal{A}$ به کلید نشست بین Π_p^i و شریکش دست می‌یابد. کلید نشست در صورتی ایجاد می‌شود که نشست کامل شده و شرکت‌کنندگان در حالت *پذیرش* باشند. درغیراین‌صورت، مقدار *تهی* برگردانده می‌شود.
- جستار تسخیر $Corrupt(\Pi_p^i)$ رمزواره‌های بلندمدت Π_p^i را در پاسخ بر می‌گرداند و $\mathcal{A}$ کلیه اطلاعات ذخیره شده درون دستگاه قانونی را استخراج می‌کند.
- جستار سنجش کلید $TestSK(\Pi_p^i)$ امنیت معنایی کلید نشست[۲۰] Π_p^i را می‌سنجد. درصورتی‌که نشست کامل باشد و کلید نشست ایجاد شده باشد، آن را در پاسخ برمی‌گرداند. درغیراین‌صورت، مقدار *تهی* برگردانده می‌شود. $\mathcal{A}$ زمانی می‌تواند این جستار را ارسال کند که اوراکل Π_p^i *تازه* باشد. Π_p^i از طریق انداختن یک سکه بی‌طرف $b \in [0,1]$ تصمیم می‌گیرد که کلید نشست را برگرداند یا خیر. اگر $b = 1$ باشد، کلید نشست واقعی ارسال، و درغیراین‌صورت، یک کلید تصادفی تولید و در پاسخ برگردانده می‌شود.
- جستار سنجش شناسه $TestID(\Pi_p^i)$ مهاجم با پرتاب یک سکه بی‌طرف شانس خود برای دست‌یابی به شناسه اوراکل Π_p^i را امتحان می‌کند.

امنیت معنایی کلید نشست. مطابق مدل ROR، ضروری است که $\mathcal{A}$ تفاوت بین کلید نشست نمونه واقعی و یک عدد تصادفی را تشخیص دهد. چندین جستار $Test$ می‌تواند توسط مهاجم از Π_{MTCD}^i و Π_{TA}^i پرسیده شود. $Succ$ حالتی را نشان دهد که $\mathcal{A}$ بازی را ببرد. اگر خروجی $Test$ (مقدار b') در شرط $b' = b$ صدق کند، می‌گوییم مزایای مهاجم برای نقض امنیت معنایی پروتکل پیشنهادی($Adv(\mathcal{A})$) برابر زیر است:

$$Adv_{\Pi}(\mathcal{A}) = |\Pr[Succ] - 1| \qquad (۱۱)$$

اوراکل تصادفی تمام شرکت‌کنندگان و مهاجم $\mathcal{A}$ درون شبکه اجازه دارند که به تابع رمزنگاری هَش مقاوم در برابر تصادم دسترسی داشته باشند. $h(.)$ به صورت یک اوراکل تصادفی به نام $\mathcal{H}$ معرفی شده است. می‌توانیم بگوییم که پروتکل پیشنهادی به‌صورت معنایی ایمن است اگر $Adv_{\Pi}(\mathcal{A})$ ناچیز باشد. مطابق CMCDHP و CMDDHP شانس مهاجم برای برنده شدن ناچیز و به‌صورت $Adv_{\Pi}^{CMCDHP}(\mathcal{A}) \leq \varepsilon$ و $Adv_{\Pi}^{CMDDHP}(\mathcal{A}) \leq \varepsilon$ است [۳۳،۳۲]. لم‌های زیر در پروتکل پیشنهادی صادق است.

- **لم ۱.** برای هر A، B و C عضو یک تابع توزیع احتمال، با شرط $A \wedge \sim C = B \wedge \sim C$، $|Pr(A) - Pr(B)| \leq Pr(C)$ [۳۱].
- **لم۲.** برای عدد صحیح مثبت N و q عنصر $y_1, \dots, y_q$، که به‌صورت یکنواخت و مستقل از هم از مجموعه‌ای با اندازه N انتخاب شده باشند، احتمال اینکه دو مقدار i و j وجود داشته باشند که $y_i = y_j$، تقریباً برابر با $q^2/2N$ است [۳۸].

۴-۱-۲- قضیه : احتمال برنده شدن مهاجم

برای یک مهاجم جندجمله‌ای زمان $\mathcal{A}$ با حداکثر q_s جستار $Send$ و q_e جستار $Execute$ و q_h جستار $Hash$، مزایای $\mathcal{A}$ برای شکستن امنیت معنایی پروتکل پیشنهادی برابر زیر است

$$Adv_{\Pi}(\mathcal{A}) \leq (2q_s + 3q_h^2 + (q_s + q_e)^2)/p + 2q_h Adv_{CMCDHP}(\mathcal{A}) \qquad (۱۲)$$

اثبات. از رویکرد بازی‌های متوالی برای اثبات ادعای خود استفاده می‌کنیم، که از G_0 شروع و با G_5 خاتمه می‌یابد. برای هر بازی G_i رویداد $Succ_i$ را تعریف می‌کنیم. $Succ_i$ نشان‌دهنده رخدادی در

G_i است که $\mathcal{A}$ به‌درستی بیت خروجی $Test$ را حدس زده باشد. ثابت می‌کنیم که تفاوت G_i و G_{i+1} ناچیز است، حتی اگر رویداد C رخ داده باشد، یعنی $|Pr(Succ_{i+1}) - Pr(Succ_i)| \leq Pr(C)$ (مطابق لم ۱).

بازی G_0. حمله واقعی را نشان می‌دهد و تابع هش را به‌صورت یک اوراکل تصادفی مدل می‌کند. $Succ_0$ نشان می‌دهد که مهاجم به‌طور موفقیت‌آمیز خروجی $Test$ را حدس زده باشد؛ پس داریم

$$Adv_{\prod}(\mathcal{A}) = |2\Pr(Succ_0) - 1| \quad (۱۳)$$

بازی G_1. این بازی تفاوت کمی با G_0 دارد. به این صورت که تابع هش با کمک یک لیست جست‌وجو استفاده می‌شود. دیگر اوراکل‌ها نظیر $Send$، $Execute$ مشابه G_0 باقی می‌مانند. ازاین‌رو، G_0 و G_1 غیرقابل تمیز هستند و داریم

$$\Delta_0 = |\Pr(Succ_1) - \Pr(Succ_0)| = 0 \quad (۱۴)$$

بازی G_2. در این بازی، شبیه‌سازی اوراکل‌ها مشابه G_1 باقی می‌ماند و زمانی متوقف می‌شود که تصادم در مقادیر هش و متون رخ دهد. بر مبنای لم ۲، احتمال رخ دادن تصادم در اوراکل $Hash$ برابر با $q_h^2/2p$ و احتمال رخ دادن تصادم در متون برابر با $(q_s + q_e)^2)/2p$ است. بنابراین داریم

$$\Delta_1 = |\Pr(Succ_2) - \Pr(Succ_1)| \leq q_h^2/2p + (q_s + q_e)^2)/2p \quad (۱۵)$$

بازی G_3. G_2 و G_3 مشابه یکدیگر هستند، با این تفاوت که $\mathcal{A}$ تلاش می‌کند تا $IMSI_j = HID_j \oplus h(T2^*_{MTCD_{ij}} \| t_{ij})$ را به‌دست آورد. بنابراین داریم

$$\Delta_2 = |\Pr(Succ_3) - \Pr(Succ_2)| \leq q_h^2/p \quad (۱۶)$$

بازی G_4. G_3 و G_4 مشابه یکدیگرند، مگر حالتی که مهاجم بتواند توکن‌های احرازهویت $H_{MTCD_{ij}}$ و H_{TA} را حدس بزند (بدون پرسیدن اوراکل هش). بنابراین G_3 و G_4 غیرقابل تمیز هستند و داریم

$$\Delta_3 = |\Pr(Succ_3) - \Pr(Succ_2)| \leq q_s/p \quad (۱۷)$$

بازی G_5. در این بازی کلید نشست $K^{ASME}_{MTCD_{ij}}$ توسط مهاجم حدس زده می‌شود. بازی‌های G_4 و G_5 غیرقابل تمیز هستند، بنابراین داریم

$$\Delta_4 = |\Pr(Succ_4) - \Pr(Succ_3)| \leq q_h Adv_{CMCDHP}(\mathcal{A}) \quad (۱۸)$$

به‌علاوه، صرف نظر از بیت b درون جستار $TestSK$ خروجی یک مقدار تصادفی است، بنابراین داریم

$$\Pr(Succ_4) = 1/2 \quad (۱۹)$$

از مشاهدات فوق، نتایج زیر حاصل می‌شود

$$Adv_{\prod}(\mathcal{A}) = |2\Pr(Succ_0) - 1| \leq |2\Pr(Succ_4) - 1 + 2(Succ_0) - \Pr(Succ_4))| \leq 2\Pr(Succ_4) - 1 + 2\sum_{i=0}^{3}\Delta_i \quad (۲۰)$$

$$Adv_{\prod}(\mathcal{A}) \leq (2q_s + 3q_h^2 + (q_s + q_e)^2)/p + 2q_h Adv_{CMCDHP}(\mathcal{A}) \quad (۲۱)$$

۴-۲- تحلیل غیر رسمی امنیت

احرازهویت متقابل. پروتکل پیشنهادی به احرازهویت متقابل بین MTCDها و TA، دست می‌یابد. برای احرازهویت اعضای G_i، توکن $Token_{G_i} = T_m(k_{G_i}) mod\ p$ مورد نیاز است، که m و GK_i و $T1_{G_i}$ برای تمامی اعضای گروه یکسان هستند. رهبر گروه با اعتبارسنجی $T1_{G_i}$ امکان وقوع حمله DoS را کاهش می‌دهد. TA $T1_{G_i}$ را از رهبر گروه دریافت، و مقدار $T1''_{G_i} = h(Token_{G_i} \| GID_i \| t_{ij})$ را محاسبه می‌کند. از آنجا که $Token_{G_i}$ و $T2_{MTCD_{ij}}$ برای محاسبه $H_{MTCD_{ij}}$ و H_{agg} استفاده شده‌اند، H^*_{agg} محاسبه شده با H_{agg} دریافت شده برابر خواهد شد و بنابراین گروه G_i توسط TA احرازهویت می‌گردد.

هر MTCD اطلاعات فردی خود شامل $T1_{MTCD_{ij}}$ را از طریق GL برای TA ارسال می‌کند. TA سپس، مقدار $T2^*_{MTCD_{ij}} = T_s\left(T1_{MTCD_{ij}}\right) mod\ p = T_s\left(T_{y_j}(Q_j)\right) mod\ p = T_{y_i}\left(T_s(s_j(x))\right) mod\ p = T_{y_j}(T_{s_j}(Q_{TA}) mod\ p = T2_{MTCID_{ij}}$ را محاسبه می‌کند. اگر $T2^*_{MTCD_{ij}}$ صحیح باشد، $H_{MTCD_{ij}}$ و H_{agg} با $H'_{MTCD_{ij}}$ و H'_{agg} برابر خواهند شد و MTCDها به‌صورت انفرادی احرازهویت می‌شوند. به‌طور مشابه، MTCD مقدار $T2^*_{TA} = T_m(T1_{TA}) mod\ p$ را محاسبه می‌کند. $T2^*_{TA}$ برای محاسبه و تأئید H^*_{TA} استفاده می‌شود. اگر $H^*_{TA} = H_{TA}$ برقرار شود، TA را برای تمامی MTCDها احراز می‌شود. همچنین، هر MTCD توسط $H_{MTCD_{ij}-TA}$ برای جلوگیری از حمله عامل درونی TA را اعتبارسنجی می‌کند.

مقاوم در برابر حمله دانستن کلید نشست. کلید نشست $K^{ASME}_{MTCD_{ij}}$ بین MTCDها و TA به‌صورت موفقیت‌آمیز به اشتراک گذاشته می‌شود. این کلید با اطلاعات ارسال و دریافت شده و اطلاعات ذخیره شده محاسبه می‌شود. تنها کسانی به آن دست می‌یابند که اطلاعات مخفی را بدانند. همچنین این کلید از رمزهای کوتاه مدت و بلند مدت ساخته شده است که کلید هر نشست را از دیگر نشست‌ها مستقل می‌کند. در نتیجه، پروتکل پیشنهادی در مقابل حمله دانستن کلید نشست مقاوم است.

مقاوم دربرابر حمله تکرار. هر پیام حاوی مهرزمانی و اعداد تصادفی خاص خود است که در هر دور اجرا به‌روز می‌شوند. به‌عنوان مثال، اگر مهاجم پیام $< R_i, H_{agg}, M_{agg}, GID_i, T1_{G_i}, t_{ij} >$ در نشست جاری را در دور بعد استفاده و برای TA ارسال کند، مقدار $m = h(h(GK_i \| t_{ij}) \| \cup_{j=1}^{l} HID_j \| GID_i)$ مربوط به دو نشست با یکدیگر متفاوت خواهد شد. با برقرار نبودن تساوی، TA پیام درخواست احرازهویت گروه را نادیده می‌گیرد.

مقاوم در برابر حمله جعل. مهاجم با هدف فریب TA، یک MTCD را جعل می‌کند. اگر $\mathcal{A}$ عامل داخلی باشد، قادر به جعل اطلاعات گروه شامل GID_i و GK_i است. همچنین $\mathcal{A}$ می‌تواند $T1_{G_i}$ و $Token_{G_i}$ را محاسبه کند. اگرچه پیام ارسال شده از طرف $\mathcal{A}$، توسط رهبر گروه مجاز شمرده می‌شود (با محاسبه $T1_{G_i}$)، احراز $\mathcal{A}$ در TA ناموفق خواهد بود؛ چرا که $T1_{MTCD_{ij}}$ و $T2_{MTCD_{ij}}$ و $H_{MTCD_{ij}}$ برابر نخواهند شد (یعنی $H^*_{TA} \neq H_{TA}$). دلیل آن، این است که y_j، s_j، و Q_j تنها توسط $MTCD_j$ شناخته می‌شوند، و رهبر گروه مقدار $T1_{MTCD_{ij}}$ و $T2_{MTCD_{ij}}$ جعلی را رد خواهد کرد. این موضوع برای جعل TA نیز صادق است. همچنین با توجه به سختی مسئله CMDLP و CMDHP، کلید نشست قابل محاسبه یا نخواهد بود.

مقاوم در برابر حمله شخصی درمیان. فرض کنید $\mathcal{A}$ پیام $< H_{MTCD_{ij}}, T1_{MTCD_{ij}}, HID_i, T1_{G_i}, Time >$ را دریافت می‌کند و می‌کوشد آن را تغییر دهد. برای رسیدن به این هدف، $\mathcal{A}$ باید عدد تصادفی y_j^A را انتخاب، و t_{ij}^A را تولید کند. سپس، $\mathcal{A}$ سعی می‌کند $T2^A_{MTCD_{ij}} = T_{y_j^A}\left(T_{s_j}(Q_{TA})\right) mod\ p$ و $HID_j =$ $IMSI_j \oplus h(T2_{MTCD_{ij}} \parallel t_{ij})$ را محاسبه کند. برای این کار، $\mathcal{A}$ باید شناسه $IMSI_j$ و کلید خصوصی s_j را در اختیار داشته باشد تا با GLو TA ارتباط برقرار کند؛ که این مهم غیرقابل انجام است. به‌طور مشابه، $\mathcal{A}$ نمی‌تواند پیام‌های ارسال شده از طرف رهبر گروه و سرور احرازهویت را در طول مراحل احرازهویت و تولید کلید ایجاد کند. ازاین‌رو، طرح پیشنهادی در برابر حمله شخصی در میان ایمن است.

قابلیت محرمانگی کامل رو به جلو و رو به عقب. اگر رمزواره‌های بلندمدت و یا کلید نشست در یک مرحله افشا شود، مهاجم نباید کلیدهای نشست ایجاد شده در دوره‌های قبل و بعد را به دست آورد. در پروتکل پیشنهادی، رمزواره‌های بلند مدت شامل s_j و M_{ij} هستند. با تسخیر این دو، مهاجم قادر نیست $T2_{MTCD_{ij}} = T_{y_j}\left(T_{s_j}(Q_{TA})\right) mod\ p$ را محاسبه کند. زیرا y_j در یک نشست خاص اعتبار دارد و برای مهاجم شناخته شده نیست. همچنین y_j نمی‌تواند از توکن عمومی $T1_{MTCD_{ij}}$ استخراج شود؛ دلیل این امر، سختی مسئله CMDLP است. از این‌رو، پروتکل پیشنهادی محرمانگی رو به جلو و رو به عقب را فراهم می‌آورد.

مقاوم در برابر حمله تسخیر گره. رهبر گروه، به‌عنوان یک تجمیع کننده، پیام‌های اعضا را برای TA ارسال می‌کند. این وظیفه دائمی نیست و در هر تعداد دور مشخص تعویض می‌شود. درنتیجه، حتی اگر GL تسخیر شود، دسترس‌پذیری شبکه از بین نخواهد رفت. در صورت تسخیر یک MTCD، دیگر اعضای گروه و GL در خطر نخواهند بود؛ چرا که هر دستگاه به‌صورت مجزا در سرور TA ثبت‌نام و رمزواره‌های خود را دریافت می‌کند. همچنین هر موجودیت کلید خصوصی‌اش را خودش انتخاب می‌کند، و در صورت تسخیر TA، کلید خصوصی دستگاه‌ها افشا نخواهد شد. بنابراین، طرح پیشنهادی در برابر این حمله ایمن است.

در طرح‌های مقایسه‌شده نواقص امنیتی نظیر عدم داشتن قابلیت گمنامی یا غیرقابل رهگیری بودن و یا نداشتن پویایی در اعضای گروه وجود دارد که برای شبکه‌هایی با تحرک‌پذیری بالا مناسب نیستند. پروتکل پیشنهادی مشکلات آنها را برطرف نموده و مقایسه ویژگی‌های امنیتی این طرح‌ها در جدول ۲ نشان داده شده است.

جدول ۲: مقایسه ویژگی‌های امنیتی

ویژگی	روش				
	GLRAM	GBAAM	چوی و همکاران	روی‌چاودری و همکاران	روش پیشنهادی
مقاوم در برابر حمله جعل	√	√	√	√	√
مقاوم در برابر حمله تکرار	√	√	√	ندارد	√
مقاوم در برابر حمله تسخیر	√	√	√	√	√
مقاوم در برابر حمله عامل درونی	√	√	ندارد	ندارد	√
قابلیت گمنامی	ندارد	ندارد	ندارد	ندارد	√
قابلیت محرمانگی رو به جلو	√	√	ندارد	√	√
قابلیت حذف و اضافه اعضا	√	ندارد	√	ندارد	√
قابلیت غیرقابل پیگیری بودن	ندارد	ندارد	ندارد	ندارد	√
مقاوم در برابر نشت پارامتر مخفی	ندارد	√	√	ندارد	√
مقاوم در برابر حمله استراق سمع	√	√	√	√	√
مقاوم در برابر حمله شخصی در میان	√	√	√	√	√
مقاوم در برابر حمله انکار سرویس	√	√	√	√	√

۴-۳- ارزیابی کارایی

در اینجا مقایسه کارایی پروتکل پیشنهادی با روش‌های مشابه از منظر سربار ارتباطی و هزینه محاسباتی انجام شده است. از رویکردهای موجود در [۷] و [۳۱] برای ارزیابی عملکرد تعداد پیام‌های مبادله شده در شبکه استفاده نموده‌ایم. MTCDها درون g گروه دسته‌بندی می‌شوند که هر گروه به میزان (n/g) عضو دارد. جدول ۳ سربار ارتباطی برای n عضو MTCD درون شبکه برای طرح‌های متفاوت را نشان می‌دهد. SE-AKA [۲۰] بر روی کاهش تعداد پیام‌های ارتباطی در هسته شبکه (سرور) تمرکز دارد. درحالی‌که در GLARM [۷]، GBAAM [۲۲] و Chio-AKA[۲۳]، سربار ارتباطی در ترافیک‌های لبه شبکه (دستگاه‌های انتهایی MTCD) کاهش داده شده است. شکل ۶ و ۷ مقایسه پروتکل پیشنهادی با تعدادی از پروتکل‌های دیگر را نشان می‌دهد. پروتکل پیشنهادی و روی‌چاودری و همکاران [۳۱]، از طریق پخش همگانی پیام‌ها، ترافیک را در لبه شبکه و سرور شبکه کاهش می‌دهند. در سرور احرازهویت، ارتباطات تنها با رهبر گروه شکل می‌گیرد. در نتیجه در هر دو مورد کاهش سربار ارتباطی را خواهیم داشت. طول بیتی تابع هش و چبیشف برابر ۱۶۰ بیت، نانس و شناسه برابر ۱۲۸ بیت و مهرزمانی برابر ۳۲ بیت در نظر گرفته شده است. شکل ۶، مقایسه تعداد پیام‌های مبادله شده بین روش پیشنهادی و دیگر روش‌ها را به ازای تعداد گروه‌های مختلف نشان می‌دهد که روش پیشنهادی نسبت Chio-AKA [۲۳] و روی‌چاودری و همکاران [۳۱] کاهش ناچیز و نسبت به سایر روش‌ها کاهش چشم‌گیر دارد.

جدول۳: مقایسه تعداد پیام‌های مبادله شده برای n عضو

پروتکل	لبه شبکه	نقطه دسترسی	هسته شبکه	مجموع
SE-AKA [۲۰]	-	3n+3	2	3n+5
GLRAM [۷]	2n	3	2	2n+5
GBAAM [۲۲]	2n	3	2	2n+5
Choi-AKA [۲۳]	n-1	4	2	n+5
روی‌چاودری [۳۱]	n	2	2	n+4
روش پیشنهادی	n	2	2	n+4

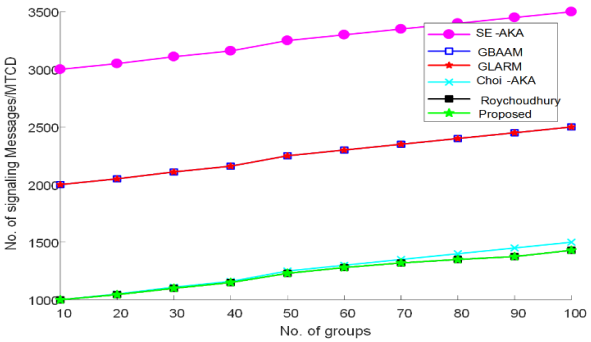
سربار محاسباتی برای XOR در نظر گرفته نشده است. زمان تخمینی برای عملیات هش $T_{hash} = 0.0005$ ms ، چندجمله‌ای $T_{chev} = 0.021025\ ms$، ضرب اسکالر در رمزنگاری خم بیضوی $T_{mul} = 0.063075\ ms$، محاسبات رمزنگاری متقارن $T_{enc} = 0.0087\ ms$، جفت‌سازی خطی $T_{pair} = 1.537\ ms$ و $T_{ptm} = T_{mul} = 0.063075\ ms$ در نظر گرفته شده است. زمان محاسبات برای عملیات هایی که MTCDها، رهبر گروه و سرور شبکه باید انجام دهند در جدول ۵ نشان داده شده است. نمودار شکل ۸ زمان محاسبات برای پروتکل‌های مختلف را نشان می‌دهد. در رویکرد روی‌چاودری و همکاران [۳۱] قابلیت حذف و اضافه اعضای گروه وجود ندارد و TA در فاز ثبت‌نام، کلید گروه را تولید و در اختیار آنها قرار می‌دهد اما در Chio-AKA [۲۳] و روش پیشنهادی ما این قابلیت در نظر گرفته شده است.

جدول ۴: مقایسه طول بیتی پسربار ارتباطی در روش پیشنهادی و روش روی‌چاودری و همکاران

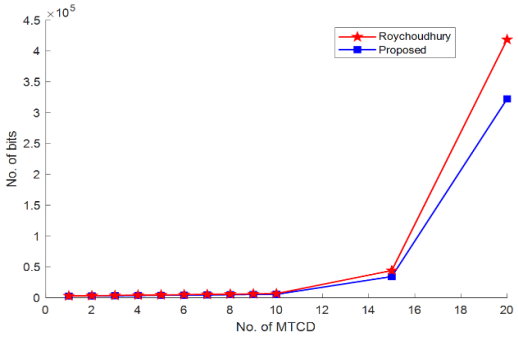
پروتکل	MTCD	GL	TA
روش پیشنهادی	$3\ \|hash\| + \|Cheb\| + \|time\| = 672$	$n(\ 2\|hash\| + \|Cheb\|) + 4\|hash\| + \|ID\| + 2\|time\| + 2\|Cheb\| = 320n + 1152$	$(n+1)\|hash\| + 2\|Cheb\| + \|time\| = 160n + 512$
روی‌چاودری	$\|hash\| + \|nonce\| + 2\ \|ID\| + 2\|Cheb\| + time = 896$	$n(\ 2\|ID\| + \|Cheb\| + \|nonce\| + \|hash\|) + 3\|hash\| + 2\|ID\| + \|nonce\| + \|Cheb\| = 704n + 1024$	$n(\|Hash\| + \|ID\|) + \|Cheb\| + \|hash\| + \|nonce\| + \|ID\| = 288\ n + 576$

جدول ۵: مقایسه سربار محاسباتی

پروتکل	MTCD	GL	TA
SE-AKA [۲۰]	$4T_{hash} + T_{mul} + T_{enc}$	$5T_{hash} + 2T_{mul} + T_{enc}$	$(3n+2)T_{hash} + 2nT_{mul} + nT_{enc}$
GLRAM [۷]	$8\ T_{hash}$	$8\ T_{hash}$	$(5\ n+4)T_{hash}$
GBAAM [۲۲]	$4\ T_{mul}$	$4\ T_{mul}$	$n\ T_{ptm} + 2nT_{mul} + 2T_{pair} + T_{mul}$
Choi-AKA [۲۳]	$5T_{hash} + T_{enc}$	$(2n+5)T_{hash} + nT_{enc}$	$(n+5)\ T_{hash}$
Roychoudhury-AKA [۳۱]	$5T_{chev} + 4T_{hash} + T_{KDF}$	$5T_{chev} + 4T_{hash} + T_{KDF}$	$+(n+3)T_{chev} + (2n+1)T_{hash} + nT_{KDF}$
روش پیشنهادی	$6T_{cheb} + 10T_{hash}$	$6T_{cheb} + 11T_{hash}$	$(2n+4)T_{chev} + (5n+5)T_{hash}$

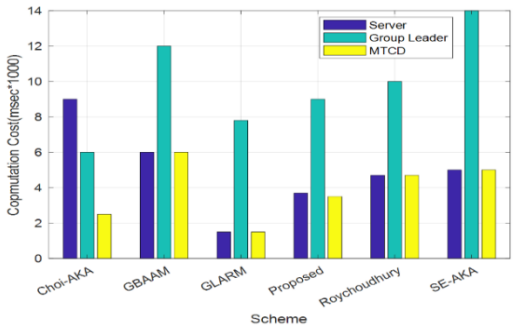


شکل ۶: مقایسه سربار ارتباطی



شکل ۷: مقایسه سربار ارتباطی روش پیشنهادی و [۳۱]

پروتکل پیشنهادی نسبت به پروتکل‌های سبک‌وزن مبتنی بر رمزنگاری هش مشابه GLRAM [۷] و Chio-AKA [۲۳] سربار محاسباتی بالاتری دارد. اما نسبت به روش‌های SE-AKA [۲۰] و GBAAM [۲۲] که از محاسبات سنگین ECC استفاده می‌کنند عملکرد بهتری دارد. پروتکل پیشنهادی، همچنین از نظر سربار ارتباطات نسبت به روش‌های GLARM و SE-AKA بهتر عمل کرده است؛ و کمی نسبت به Chio-AKA و روی‌چاودری بهتر است.



شکل ۸: مقایسه سربار محاسباتی

بااین‌حال، مشکلاتی که طرح‌های آنها داشتند را برطرف نموده است. انتخاب رهبر گروه به‌صورت تصادفی در صرفه‌جویی سربار محاسباتی می‌تواند نقش بزرگ‌تری را ایفا کند. Chio-AKA در قسمت محاسبات رهبر گروه سربار بالایی دارد. دلیل این امر قابلیت حذف و اضافه اعضای گروه است. پروتکل پیشنهادی مشابه روی‌چاودری [۳۱] از رمزنگاری چیبشف استفاده می‌کند؛ اما سربار محاسباتی کمتری نسبت به آن دارد. با توجه به مطالب گفته شده، پروتکل پیشنهادی نسبت به پنج روش مقایسه شده مزایای بسیاری دارد.

۵- نتیجه‌گیری

احرازهویت گروهی جایگزین مناسبی برای کاهش میزان داده‌های ارسالی و دریافتی در شبکه است. با این حال، چالش‌های امنیتی بیشتری در مقابل عاملین غیرمجاز، حمله شخصی میانی (MITM)، حمله تسخیر و مانند آن دارند. پروتکل‌های احرازهویت گروهی موجود، نیازهای امنیتی مناسب برای ارتباطات گروهی در شبکه IoT را فراهم نکرده‌اند. در این پژوهش از مفهوم نقشه آشفته چبیشف برای طراحی پروتکل احرازهویت گروهی و پروتکل توافق کلید استفاده نمودیم که سربار ارتباطی را به‌طور قابل توجهی کاهش و سربار محاسباتی آن معقول است. در پروتکل پیشنهادی از ایده ساختار درخت باینری مجازی استفاده کردیم چرا که امکان حذف و اضافه شدن گره‌ها را پشتیبانی می‌کند و مکانیزم حذف و اضافه گره‌های عضو در آن در نظر گرفته شده است. ارزیابی‌های صورت گرفته برتری طرح پیشنهادی را نسبت به سایر روش‌های مشابه نشان می‌دهد. به‌منظور ادامه کار حاضر به پژوهشگران علاقمند در این حوزه، توافق کلید گروهی مبتنی بر بلاکچین توصیه می‌شود.

مراجع

[1] R. Yugha and S. Chithra, “A survey on technologies and security protocols: Reference for future generation IoT”, Journal of Network and Computer Applications, 102763, 2020.

[2] M. Kanellos, “smart devices every minute in (2025): Idc outlines the future”, Forbes, 2016.

[3] S. R. Islam, D. K. wak, M. H. Kabir, M. Hossain and K. S. Kwak, “The internet of things for health care: a comprehensive survey”, IEEE access, No. 3, pp. 678-708, 2015.

[۴] مرتضی عریفی، محمود گردشی "ارائه یک پروتکل کارآمد توافق کلید گروهی تصدیقی پویا مبتنی بر شناسه"، مجله علوم و فناوری های پدافند نوین، شماره ۲، ۱۳۹۰.

[۵] سیدعباس کاظمی، مهدی جوانمرد، سید علی رضوی ابراهیمی "رمزنگاری توسط ابرخم های بیضوی و پیشنهاد پروتکل توافق کلید گروهی برای شبکه های موردی مبتنی برناحیه با استفاده از ابرخم های بیضوی"، اولین همایش ملی فناوری اطلاعات و شبکه های کامپیوتری دانشگاه پیام نور، طبس، دانشگاه پیام نور طبس، ۱۳۹۱.

[6] Y. Aydin, G. K. Kurt, E. Ozdemir and H. Yanikomeroglu, “A Flexible and Lightweight Group Authentication Scheme”, IEEE Internet of Things Journal, 2020.

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

[8] S. S. Al-Riyami and K. G. Paterson, “Certificateless public key cryptography”, In International conference on the theory and application of cryptology and information security, Springer, Berlin, Heidelberg, pp. 452-473, November 2003.

[9] Z. Xia, Y. Liu, C. F. Hsu and C. C. Chang, "Cryptanalysis and Improvement of a Group Authentication Scheme with Multiple Trials and Multiple Authentications", Security and Communication Networks, 2020.

[10] H. Y. Chien, "Group authentication with multiple trials and multiple authentications", Security and Communication Networks, 2017.

[11] O. El Mouaatamid, M. Lahmer and M. Belkasmi, "A Scalable Group Authentication Scheme Based on Combinatorial Designs with Fault Tolerance for the Internet of Things", SN Computer Science, Vol. 1, No. 4, pp. 1-13, 2020.

[12] W. Li, Y. Dai, W. Miao, M. Zhang, J. Fan, R. Liu and Y. Li, "A Group-based End-to-end Identity Authentication Method for Massive Power Wireless Private Network", In 10th International Conference on Electronics Information and Emergency Communication (ICEIEC), pp. 14-17, July 2020.

[13] J. Zhang, H. Zhong, J. Cui, Y. Xu and L. Liu, "An Extensible and Effective Anonymous Batch Authentication Scheme for Smart Vehicular Networks", IEEE Internet of Things Journal, Vol. 7, No. 4, pp. 3462-3473, 2020.

[14] B. L. Parne, S. Gupta and N. S. Chaudhari, "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network", IEEE Access, Vol. 6, pp. 3668-3684, 2018.

[15] P. Cirne, A. Zúquete and S. Sargento, "TROPHY: Trustworthy VANET routing with group authentication keys", Ad Hoc Networks, Vol. 71, pp. 45-67, 2018.

[16] Al-Shareeda, Mahmood A., Selvakumar Manickam, Badiea Abdulkarem Mohammed, Zeyad Ghaleb Al-Mekhlafi, Amjad Qtaish, Abdullah J. Alzahrani, Gharbi Alshammari, Amer A. Sallam, and Khalil Almekhlafi. "Chebyshev polynomial-based scheme for resisting side-channel attacks in 5g-enabled vehicular networks." *Applied Sciences* 12, no. 12 ,2022.

[17] G. Xu, X. Li, L. Jiao, W. Wang, A. Liu, C. Su, ... and X. Cheng, "BAGKD: a batch authentication and group key distribution protocol for VANETs", IEEE Communications Magazine,Vol. 58, No. 7, pp. 35-41, 2020.

[18] Y. Yao, X. Chang, J. Mišić and V. B. Mišić, "Lightweight Batch AKA Scheme for User-Centric Ultra-Dense Networks", IEEE Transactions on Cognitive Communications and Networking, 2020.

[19] Y. Sun, J. Cao, M. Ma, Y. Zhang, H. Li and B. Niu, "EAP-DDBA: Efficient Anonymity Proximity Device Discovery and Batch Authentication Mechanism for Massive D2D Communication Devices in 3GPP 5G HetNet", IEEE Transactions on Dependable and Secure Computing, 2020.

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

[21] S. Wang, K. Mao, F. Zhan and D. Liu, "Hybrid conditional privacy-preserving authentication scheme for VANETs", Peer-to-Peer Networking and Applications, pp. 1-16, 2020.

[22] J. Cao, M. Ma and H. Li, "GBAAM: group-based access authentication for MTC in LTE networks", Security and communication networks, Vol. 8, No. 17, pp. 3282-3299, 2015.

[23] D. Choi, H. K. Choi and S. Y. Lee, "A group-based security protocol for machine-type communications in LTE-advanced", Wireless networks, Vol. 21, No. 2, pp. 405-419, 2015.

[24] J. Yang, J. Deng, T. Xiang and B. Tang, "A Chebyshev polynomial-based conditional privacy-preserving authentication and group-key agreement scheme for VANET", Nonlinear Dynamics, Vol. 106, No. 3, pp. 2655-2666, 2021.

[25] Q. Zhang, L. Zhu, Y. Li, Z. Ma, J. Yuan, J. Zheng and S. Ai, "A group key agreement protocol for intelligent internet of things system", International Journal of Intelligent Systems, Vol. 37, No. 1, pp. 699-722, 2022.

[26] Y. Xia, R. Qi, S. Ji, J. Shen, T. Miao and H. Wang, "PUF-Assisted Lightweight Group Authentication and Key Agreement Protocol in Smart Home", Wireless Communications and Mobile Computing, 2022.

[27] A. Braeken, "Pairing free asymmetric group key agreement protocol", Computer Communications, Vol. 181, pp. 267-273, 2022.

[28] P. Bergamo, P. D'Arco, A. De Santis and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials", IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 52, No. 7, pp. 1382-1393, 2005.

[29] L. Kocarev and S. Lian, "Chaos-based cryptography: Theory, algorithms and applications", Springer Science & Business Media, Vol. 354, 2011.

[30] S. H. Islam, M. K. Khan, M. S. Obaidat and F. T. B. Muhaya, "Provably secure and anonymous password authentication protocol for roaming service in global mobility networks using extended chaotic maps", Wireless Personal Communications, Vol. 84, No. 3, pp. 2013-2034, 2015.

[31] P. Roychoudhury, B. Roychoudhury and D. K. Saikia, "Provably secure group authentication and key agreement for machine type communication using Chebyshev's polynomial", Computer Communications, Vol. 127, pp. 146-157, 2018.

[32] U. D. D. Mills, J. Martin, J. Burbank and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", Technical Report, 2010.

[33] Y. Liu, Y. Wang and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm", IEEE Transactions on Intelligent Transportation Systems, Vol. 18, No. 10, pp. 2740-2749, 2017.

[34] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols", In Proceedings of the 1st ACM conference on Computer and communications security, pp. 62-73, December 1993.

[35] V. Shoup, "Sequences of games: a tool for taming complexity in security proofs", IACR Cryptol. ePrint Arch., 2004.

[36] I. Shparlinski, "Computational Diffie-Hellman problem", encyclopaedia entry, 2011.

[37] R. Canetti,"Decisional Diffie-Hellman Assumption", 2005.

[38] T. Zhou and J. Xu, "Provable secure authentication protocol with anonymity for roaming service in global mobility networks", Computer Networks, Vol. 55, No. 1, pp. 205-213, 2011.

پاورقی‌ها:

[1] Internet of Things (IoT)

[2] Machine-to-Machine (M2M)

[3] Device-to-Device (D2D)

[4] CertificateLess Batch Signature (CLBS)

[5] Bilinear Paring

[6] Chebyshev polynomials

[7] Elliptic-Curve Cryptography (ECC)

[8] Certificate Revocation Lists (CRL)

[9] Trusted Authority (TA)

[10] Long Term Evolution (LTE)

[11] Vehicular Ad hoc Network (VANET)

[12] Ultra-Dense Networks (UND)

[13] Chaotic Maps based Decisional Diffie Hellman Problem

[14] Machine type communication (MTC)

[15] Vehicle to everything (V2X)

[16] Network Time Protocol (NTP)

[17] Partnering

[18] Accept state

[19] Query

[20] Semantic security