مقاله پژوهشی

ارائه یک احراز هویت متقابل سبک‌وزن گروهی دستگاه‌ها در اینترنت اشیا

رضا سرابی میانجی، سام جبه‌داری و ناصر مدیری

چکیده: اینترنت اشیا در حال تبدیل‌شدن به بزرگ‌ترین پلتفرم محاسباتی است و هر روزه شاهد افزایش تعداد دستگاه‌های این محیط هستیم. علاوه بر این، بیشتر اشیای این زیرساخت دارای محدودیت‌های محاسباتی و حافظه می‌باشند و قادر به انجام عملیات پیچیده محاسباتی نیستند. این محدودیت‌ها در بیشتر روش‌های احراز هویت سنتی نادیده گرفته شده‌اند. در ضمن در روش‌های جدید احراز هویت این محیط، به مسأله مقیاس‌پذیری توجه زیادی نشده و بنابراین نیاز به یک احراز هویت سبک‌وزن، مقیاس‌پذیر احساس می‌شود. در این مقاله یک پروتکل احراز هویت سبک‌وزن ارائه شده که اشیا در گروه‌های مختلف قرار می‌گیرند و در هر گروه یک گره مدیر در نظر گرفته می‌شود و به عنوان نماینده از طرف بقیه گروه، عملیات احراز هویت را انجام می‌دهد. بنابراین به صورت گروهی احراز هویت انجام می‌گردد و پروتکل مقیاس‌پذیری بالای دارد. روش پیشنهادی هزینه محاسباتی گره و سرور را کاهش می‌دهد و حریم خصوصی را از طریق گمنامی گره‌ها فراهم می‌آورد. رازداری رو به جلو را بدون استفاده از رمزگذاری آسنکرون و همچنین توافق بر روی کلید جلسه را دارد. از ابزار AVISPA برای تأیید امنیتی روش پیشنهادی استفاده شده است. در روش ما، هزینه زمانی احراز هویت در گره و سرور نسبت به روش‌های بررسی‌شده به ترتیب ۷٫۸٪ و ۳٫۵٪ کاهش یافته است.

کلیدواژه: **احراز هویت سبک‌وزن، احراز هویت گروهی، اینترنت اشیا، توافق کلید.**

۱- مقدمه

اینترنت اشیا نقش بسیار مهمی در زندگی روزمره ما بازی می‌کند. از این تکنولوژی در مراقبت‌های سلامتی، اتومبیل‌ها، سرگرمی‌ها، تجهیزات صنعتی، ورزش‌ها، خانه‌های هوشمند و غیره استفاده می‌شود [۱].

تا سال ۲۰۲۰، بیش از ۵۰ میلیارد دستگاه به اینترنت اشیا متصل شدند. سرعت اتصال دستگاه‌های مختلف به اینترنت بسیار زیاد و شباهت همه این دستگاه‌ها توانایی اتصال به اینترنت و تبادل اطلاعات است. با استفاده از این دستگاه‌ها داده‌ها از دنیای فیزیکی جمع‌آوری می‌شوند و با آنالیز داده‌های جمع‌شده، دنیای هوشمند ایجاد می‌گردد و تصمیم‌گیری بهتر برای مدیریت انجام می‌گیرد [۲].

این مقاله در تاریخ ۲۷ مهر ماه ۱۳۹۹ دریافت و در تاریخ ۱۶ شهریور ماه ۱۴۰۰ بازنگری شد.

رضا سرابی میانجی، گروه مهندسی کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران، (email: reza.sarabi@gmail.com).

سام جبه‌داری (نویسنده مسئول)، گروه مهندسی کامپیوتر، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران، (email: s_jabbehdari@iau-tnb.ac.ir).

ناصر مدیری، گروه مهندسی کامپیوتر، دانشکده مهندسی برق و کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران، (email: nassermodiri@chmail.ir).

از آنجایی که بیشتر حسگرها در محیط اینترنت اشیا در دسترس مهاجمان قرار دارند، امنیت فیزیکی سخت‌افزارها و امنیت اطلاعات برای ارتباطات دستگاه‌ها به نگرانی‌های جدی برای توسعه زیرساخت اینترنت اشیا تبدیل شده است. همچنین در اینترنت اشیا از سخت‌افزارهای ناهمگن با قابلیت‌های متفاوت استفاده می‌شود. این موضوعات باعث به وجود آمدن انواع مشکلات پیچیده امنیتی می‌گردد که اگر مورد توجه قرار نگیرند، می‌توانند جلوی استفاده از برنامه‌های کاربردی اینترنت اشیا را بگیرند. به عنوان مثال می‌توان به دو حوزه کاری خانه‌های هوشمند و سیستم‌های مراقبت پزشکی هوشمند اشاره کرد که در آنها حفاظت از اطلاعات بسیار ضروری و حیاتی است.

احراز هویت فرایندی است برای تشخیص این که یک موجودیت واقعاً همان کسی یا چیزی می‌باشد که ادعا می‌کند و یکی از مهم‌ترین فرایندها در زنجیره کنترل دسترسی است، زیرا سایر عملیات انتقال داده و امنیت پس از فرایند احراز هویت انجام می‌شوند. بنابراین احراز هویت اصلی‌ترین مکانیزم امنیتی در اینترنت اشیا است و هدف آن مشخص‌کردن درستی هر موجودیت مثل دستگاه یا کاربر است [۳].

اما احراز هویت در اینترنت اشیا با چالش‌هایی همراه است که می‌توان به موارد زیر اشاره نمود:

- دستگاه‌های اینترنت اشیا دارای محدودیت منابع هستند و به صورت مداوم داده‌های حساسی را انتقال می‌دهند [۴].
- دستگاه‌ها دارای قدرت محاسباتی محدود بوده و فضای ذخیره‌سازی کمی دارند و توانایی رمزنگاری و رمزگشایی نامتقارن را ندارند [۳].
- دستگاه‌های اینترنت اشیا در کانال ناامن، اطلاعات مبادله می‌کنند و مهاجمان به راحتی به این کانال دسترسی دارند [۴].
- با به خطر افتادن یک کلید جلسه، امکان استنباط کلیدهای جلسه قبلی وجود دارد و بیشتر روش‌های احراز هویت، قابلیت رازداری رو به جلو را پشتیبانی نمی‌کنند [۴].
- به دلیل بازبودن و تحرک شبکه‌های بی‌سیم محیط اینترنت اشیا، مهاجم می‌تواند به راحتی اطلاعات مبادله‌شده در کانال را سرقت یا جعل کند و باعث نقض حریم خصوصی کاربر گردد. در سیستم‌هایی از قبیل مراقبت پزشکی، سرقت یا جعل اطلاعات می‌تواند عواقب بسیار جدی به همراه داشته باشد و حتی می‌تواند باعث به خطر انداختن جان بیمار گردد [۵].
- دستگاه‌های اینترنت اشیا ناهمگن هستند و از پروتکل‌های مختلف استفاده می‌نمایند.
- به علت محدویت منابع، دستگاه‌ها از روش‌های قدیمی احراز هویت نمی‌توانند استفاده کنند.

احراز هویت گروهی یکی از بهترین راه حل‌ها برای به حداقل رساندن

بار کاری در سرور و شبکه است. میلیون‌ها گره در اینترنت اشیا می‌توانند در گروه‌هایی قرار گیرند و به جای ارسال تمام درخواست‌های احراز هویت به سرور، می‌توان از احراز هویت گروهی استفاده نمود که باعث کاهش بار کاری سرور و شبکه می‌شود. ایده احراز هویت گروهی توسط Harn در [۶] پیشنهاد شد و توسط Chien توسعه یافت. این تحقیقات، محدودیت منابع را در نظر نمی‌گیرند و در اینترنت اشیا قابل استفاده نیستند.

بنابراین در این مقاله یک احراز هویت متقابل سبک‌وزن گروهی برای اینترنت اشیا پیشنهاد می‌شود که باعث افزایش سرعت احراز هویت خواهد شد. برای این منظور، اشیا در گروه‌هایی قرار می‌گیرند و در هر گروه به جای احراز هویت تک‌تک گره‌ها، فقط گره اصلی اقدام به احراز هویت می‌کند و پس از احراز هویت به پخش کلید جلسه بین اعضای گروه اقدام می‌نماید. این امر باعث کاهش تعداد احراز هویت‌ها و در نتیجه کاهش مدت زمان احراز هویت کل گره‌ها می‌شود. همچنین در احراز هویت از عملگرهای رمزنگاری آسنکرون استفاده نشده و فقط از عملگرهای XOR و Hash استفاده می‌شود. بنابراین این روش، یک پروتکل احراز هویت سبک‌وزن است. روش پیشنهادی ما دارای قابلیت‌های زیر است:

- امکان احراز هویت گروهی دستگاه‌ها را فراهم می‌آورد. برای این منظور اشیا در گروه‌های متفاوت قرار می‌گیرند و به صورت گروهی احراز هویت انجام می‌شود که این امر باعث مقیاس‌پذیری بالای پروتکل پیشنهادی می‌گردد.
- رازداری رو به جلو را بدون استفاده از رمزگذاری آسنکرون فراهم می‌آورد.
- احراز هویت متقابل سبک‌وزن و توافق کلید در این روش وجود دارد. هر زوج دستگاه می‌توانند در صورت نیاز، یکدیگر را احراز هویت نمایند و بر سر کلید جلسه توافق کنند.
- برای آن که از این روش احراز هویت بتوان در دستگاه‌ها با منابع محدود استفاده کرد فقط از عملگرهای محاسباتی سبک Hash و XOR استفاده شده است.
- طرح ما دارای ریسک امنیتی پایینی بوده و هزینه محاسباتی کمی دارد.
- از ابزار AVISPA برای تأیید امنیتی طرح و آنالیز امنیتی استفاده شده است.
- هزینه زمانی احراز هویت در گره و سرور نسبت به روش‌های بررسی‌شده به ترتیب ۷/۸٪ و ۳/۵٪ کاهش یافته است.

این مقاله شامل این مفاهیم است: ادبیات احراز هویت اینترنت اشیا در بخش ۲ بیان می‌گردد و مدل‌های سیستم در بخش ۳ ارائه می‌شود. در بخش ۴ روش پیشنهادی آمده و شبیه‌سازی مقاله در بخش ۵ است. ارزیابی زمان اجرای پروتکل پیشنهادی در بخش ۶ و در بخش ۷ ارزیابی امنیتی در مقابل حملات بیان می‌گردد. در ادامه، در بخش ۸ مقایسه با روش‌های دیگر ارائه می‌شود و نتیجه‌گیری نهایی در بخش ۹ قرار دارد.

۲- کارهای مرتبط

با توجه به این که محیط اینترنت اشیا تا حدودی ناامن است و تجهیزات موجود در این محیط دارای محدودیت منابع محاسباتی و حافظه می‌باشند، بنابراین نیاز به احراز هویت سبک‌وزن در این محیط احساس می‌شود. اخیراً کارهای زیادی در این زمینه انجام شده است. در این بخش کارهای احراز هویت موجود در اینترنت اشیا مورد بررسی قرار می‌گیرد.

در [۷] یک طرح احراز هویت متقابل سبک‌وزن با توافق کلید برای شبکه‌های WBAN با استفاده از عملگر XOR و تابع Hash ارائه شده است. هدف این طرح ایجاد احراز هویت بین گره‌های حسگر پوشیدنی و دستگاه ترمینال و کاربران است. در [۵] یک روش احراز هویت برای معماری WBAN ارائه شده است. این روش، یک پروتکل احراز هویت سبک‌وزن متقابل و توافق کلید برای معماری WBAN است. برای این منظور از عملگر XOR و توابع Hash استفاده می‌کند و بدون استفاده از رمزنگاری آسنکرون رازداری رو به جلو را گارانتی می‌کند. این روش در مقایسه با روش‌های رمزنگاری آسنکرون دارای هزینه محاسباتی کمی است.

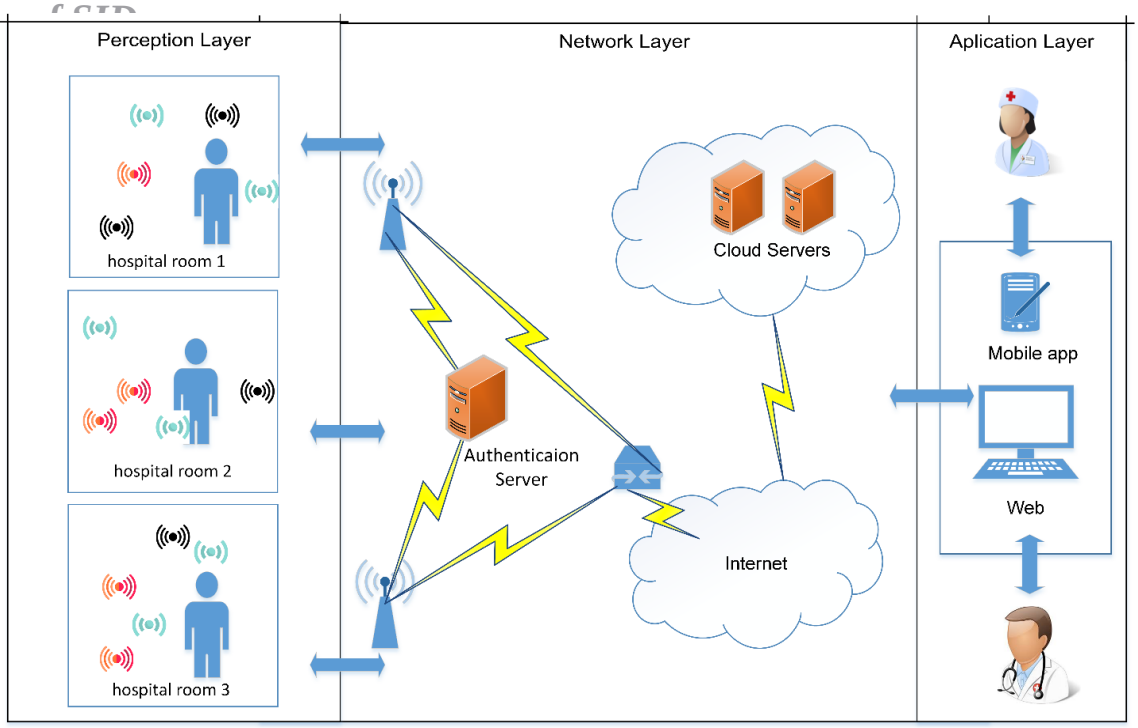
در [۴] یک روش احراز هویت سبک کاربر بر اساس توکن در محیط اینترنت اشیا ارائه شده که استفاده از توکن باعث افزایش قدرت احراز هویت می‌شود. در این روش از توکن‌های زمان‌دار برای رسیدن به هدف رازداری رو به جلو و همچنین عملگر ساده XOR و تابع Hash استفاده شده است. توکن، راه حلی مؤثر برای احراز هویت بین کاربر و دستگاه‌های هوشمند به وجود می‌آورد. استفاده از توکن ریسک دزدیده‌شدن فاکتور احراز هویت را کاهش می‌دهد و نسبت به نام کاربری و کلمه عبور نیاز به تلاش کمتری از جانب کاربر دارد. در [۸] روش احراز هویت متقابل سبک‌وزن و توافق کلید برای شبکه بی‌سیم بدن پیشنهاد شده است. برای این منظور در [۹] روشی با هزینه محاسباتی کمتر نسبت به [۸] ارائه شده که در مقابل حملات مختلف مقاوم است.

در [۱۰] یک چارچوب سبک‌وزن برای احراز هویت در محیط ابر ارائه شده که شبیه یک سیستم رمزنگاری است و چندین الگو می‌تواند از یک منبع بیومتریک ساده ایجاد گردد که هیچ یک از الگوها با هم ارتباطی ندارند. کاربر با استفاده از برنامه‌های کاربردی مختلف و الگوهای مختلف می‌تواند ثبت نام نماید و الگوی بیومتریک اصلی فاش نمی‌شود و عملیات باطل‌سازی بسیار راحتی دارد، فقط کافی است که الگوی جدید ایجاد گردد و جایگزین الگوی قدیمی شود.

در [۱۱] یک طرح احراز هویت برای برنامه‌های کاربردی مبتنی بر RFID اینترنت اشیا در موبایل‌های نسل ۵ ارائه شده که کلیدها در حافظه نهان ذخیره می‌گردند و برای احراز هویت استفاده می‌شوند و سرعت احراز هویت را بالا می‌برند و هزینه‌های محاسبات را کاهش می‌دهند و امنیت مخزن افزایش می‌یابد.

در [۱۲] طرح احراز هویت متقابل برای برنامه‌های کاربردی مبتنی بر NFC موبایل‌های نسل ۵ ارائه شده است. در این طرح از عملگرهای XOR و شیفت برای انجام و ذخیره ساختارهای برچسب‌های NFC استفاده شده است. آنها به جای شناسه واقعی از اسامی مستعار استفاده کرده‌اند تا ناشناس‌بودن برچسب‌ها را فراهم آورند. در [۱۳] یک طرح احراز هویت ناشناس اینترنت اشیا بر روی ECC سبک‌وزن ارائه شده که شامل دو مرحله اصلی است. این مراحل شامل ثبت نام و احراز هویت است. در این تحقیق، مقایسه‌ای بین ECC و RSA با استفاده از زمان مورد نیاز برای رمزگذاری و رمزگشایی با استفاده از اندازه کلیدهای متفاوت انجام شده است.

در [۱۴] یک احراز هویت سبک‌وزن کاربر برای سیستم مراقبت‌های پزشکی بر پایه ابر ارائه شده است. این روش در برابر حملات مختلف مقاوم است و هزینه محاسباتی مناسبی دارد. در [۱۵]، یک پروتکل احراز هویت دستگاه برای خانه هوشمند، با استفاده از تابع Hash و رمزگذاری ارائه شده که این روش دارای قابلیت‌های امنیتی بسیار بالایی است. در [۱۶] یک طرح احراز هویت برای اینترنت اشیای پزشکی پیشنهاد شده که



شکل ۱: معماری اینترنت اشیا برای سناریوی بیمارستان هوشمند.

جدول ۱: روش‌های پیشین احراز هویت در اینترنت اشیا.

ردیف	روش احراز هویت	معایب
۱	مبتنی بر صدور گواهینامه	نیاز به دست‌تکانی دارد. هزینه مصرف بالا است. فضای ذخیره‌سازی زیادی نیاز دارد. توجهی به محدودیت منابع ندارد. نیاز به گواهی‌نامه احراز هویت دارد. نیاز به زمان زیادی برای ایجاد نشست دارد. احراز هویت اضافی برای کاربران ایجاد می‌شود.
۲	مبتنی بر رمزنگاری	دستگاه‌ها نیاز به توانایی انجام پیچیده رمزنگاری دارند. فرایندهای پیچیده محاسباتی انجام می‌گیرد.
۳	مبتنی بر روش‌های غیر رمزنگاری	نیاز به جمع‌آوری مداوم اطلاعات از محیط دارد.

در برابر حملات جعل هویت، حدس‌زدن رمز عبور، مرد میانی[1] و پخش مجدد مقاوم است. هزینه محاسباتی گره و سرور در این روش بالا است.

در [۱۷] یک پروتکل برای احراز هویت بین کاربر و سرور ارائه شده که یک احراز هویت دومرحله‌ای برای دستگاه‌های اینترنت اشیا است. کلمه عبور به عنوان فاکتور اول احراز هویت استفاده می‌شود و PUF به عنوان فاکتور دوم احراز هویت مورد استفاده قرار می‌گیرد. در [۱۸] یک طرح احراز هویت برای سیستم‌های اینترنت اشیا با استفاده از بلاک‌چین به نام Bubbles-of-Trust و در [۱۹] یک طرح احراز هویت دو فاکتور سبک‌وزن ارائه شده است. این طرح بر پایه تابع Hash و عملگر XOR است. در [۲۰] یک پروتکل سبک‌وزن احراز هویت و حفظ حریم خصوصی برای پرداخت تلفن همراه در اینترنت اشیا ارائه گردید. در این پروتکل با قراردادن محاسبات بر روی پلتفرم پرداخت با قدرت محاسباتی بالا، کارایی بهبود یافته است.

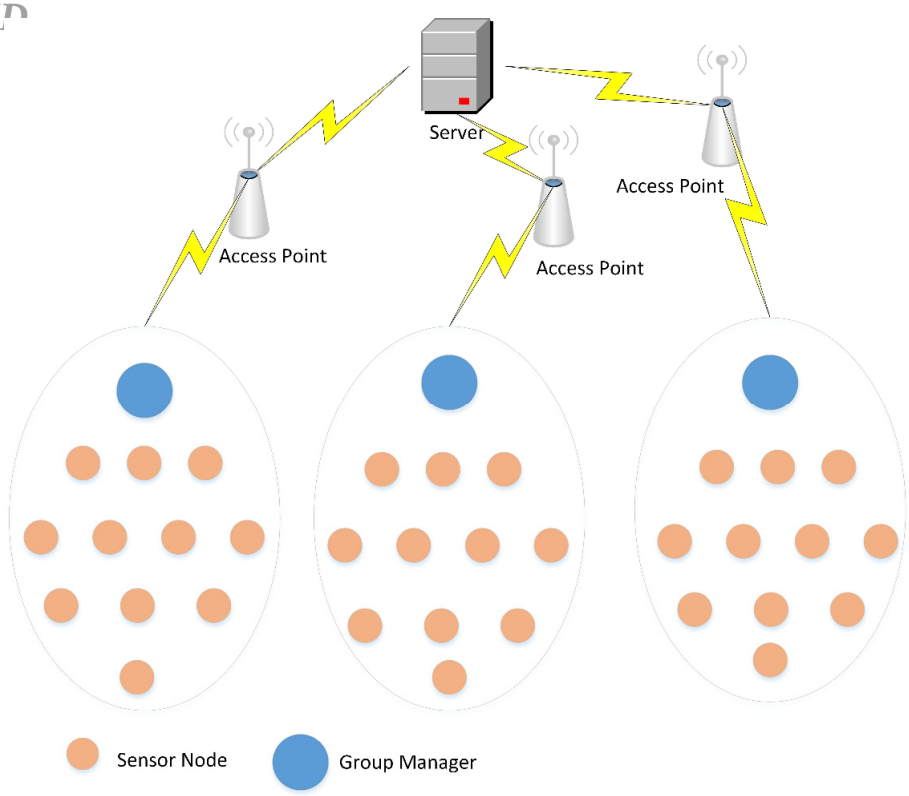
در جدول ۱ گروه‌بندی از روش‌های احراز هویت در اینترنت اشیا، ارائه و معایب هر روش احراز هویت نیز بیان شده است. با توجه به معایب دو روش مبتنی بر صدور گواهی‌نامه و مبتنی بر رمزنگاری در اینترنت اشیا، تمایل به استفاده از روش غیر رمزنگاری زیاد است و اخیراً تحقیقات زیادی در این روش انجام گرفته است.

۳- مدل‌های سیستم

۳-۱ مدل شبکه پیشنهادی

به منظور بررسی روش پیشنهادی، یک سناریو از محیط‌های اینترنت اشیا ارائه شده تا تقاضای احراز هویت سبک‌وزن نشان داده شود. این سناریو (شکل ۱) مرتبط با سیستم بیمارستان هوشمند است. برای پیاده‌سازی سیستم بیمارستان هوشمند باید حسگرها در بخش‌های مختلف بیمارستان و حتی متصل به بدن بیماران وجود داشته باشند. گره‌های حسگر می‌توانند داده‌های بااهمیت مانند دمای بدن، نوار قلب، فشار خون و سایر اطلاعات زیست‌محیطی بیمار را به دست آورند. تمام داده‌های حس‌شده در یک سرور در محیط ابری و یا سرور محلی جمع‌آوری می‌شوند. پزشکان و پرستاران می‌توانند به صورت بلادرنگ وضعیت بیماران و اطلاعات محیطی هر بخش را از طریق سیستم مشاهده و بررسی کنند. در این سناریو داده‌های حس‌شده نیز باید در یک بازه زمانی کوتاه به صورت دوره‌ای به سرور منتقل شوند. در این سناریو فرض شده که حسگرها دارای منابع محدودی هستند که از یک یا چند باتری تغذیه می‌شوند و از قدرت محاسباتی و فضای ذخیره‌سازی کمی برخوردار هستند. هر حسگر قادر به انجام عملیات XOR و تابع Hash است و از یک تولیدکننده عدد تصادفی برای تولید اعداد تصادفی برخوردار است. همچنین دروازه‌ها و سرورها دارای منابع نامحدود و توانایی محاسبات کافی برای انجام عملیات Hash و تولید اعداد تصادفی هستند و حافظه ذخیره‌سازی برای ذخیره مقادیر موقتی و جداول داده را دارند.

1. Man-in-the-Middle Attacks



شکل ۲: گروه‌بندی گره‌های سنسور به سه گروه.

جدول ۲: نمادها و تعاریف.

نماد	توضیحات
GMa	گره مدیر گروه
GMe	گره عضو گروه
ID_{ser}	شناسه سرور
ID_{Gma}	شناسه گره مدیر گروه
$H(.)$	تابع یک‌طرفه Hash
tc, ts	مهر زمانی
xor	عملگر XOR
$.$	الحاق دو رشته
Tk	توکن
Ks	کلید جلسه
$Kser$	کلید اصلی سرور

۳-۲ مدل تهدید

در این مقاله مدل تهدید Dolev-Yao [۲۱] استفاده می‌شود که فرض می‌کند گره‌های حسگر و سرورها در یک کانال ناامن ارتباط برقرار می‌کنند. سرور به عنوان گره قابل اعتماد است اما مهاجم می‌تواند به پایگاه داده سرور نفوذ کند و تمام داده‌های موجود در آن را به جز کلید اصلی سرور به دست آورد.

همچنین مهاجم توانایی به دست آوردن تمام داده‌های مبادله‌شده در کانال ارتباطی را دارد و می‌تواند داده‌های جدیدی در کانال تزریق کند. در ضمن داده‌های ارسالی موجود در کانال را می‌تواند با مقادیر جدید جایگزین کرده و از نو در کانال ارتباطی ارسال نماید. حسگرها به دلیل محدودیت هزینه مالی از نظر فیزیکی محافظت نمی‌شوند و در نتیجه مهاجم می‌تواند داده‌های ذخیره‌شده در حافظه گره حسگر را استخراج کند و از آنها برای انجام کارهای مخرب استفاده نماید.

٤- طرح پیشنهادی

با توجه به محدودیت دستگاه‌های اینترنت اشیا، از احراز هویت قدیمی و سنتی مبتنی بر کلید عمومی- خصوصی و گواهی‌نامه نمی‌توان در این محیط استفاده نمود. در ضمن بایستی احراز هویت را با حداقل هزینه محاسباتی و ارتباطی انجام داد. روش‌های احراز هویت ارائه‌شده دارای مشکلاتی از قبیل هزینه محاسبات بالا، نیاز به حافظه بالا، هزینه ارتباطات بالا، عدم حفظ حریم خصوصی و ضعف در برابر حملات امنیتی هستند.

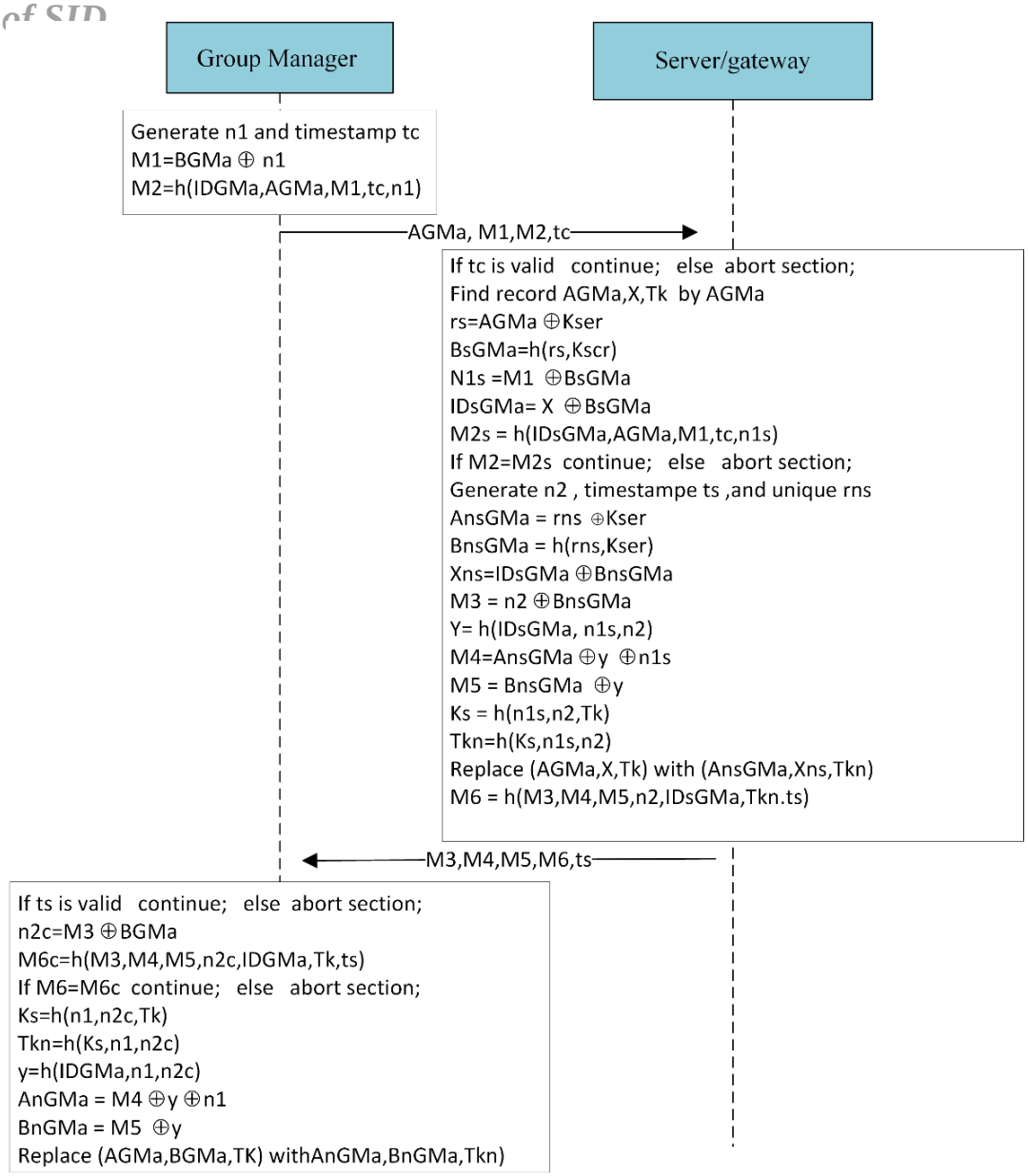
در طرح ارائه‌شده گره‌های حسگر به سه گروه مطابق شکل ۲ تقسیم می‌شوند. حال در هر گروه یک گره مدیر داریم که برای کل گروه عملیات احراز هویت را انجام می‌دهد و پس از احراز هویت، کلید جلسه را بین گره‌های عضو گروه پخش می‌کند. این امر باعث کاهش تعداد و مدت زمان اجرای احراز هویت می‌شود. بنابراین هزینه زمانی و هزینه ارتباطات برای گره‌های سرور و سنسور کاهش می‌یابد.

در هر گروه به جای احراز هویت تک‌تک گره‌ها فقط گره مدیر اقدام به احراز هویت می‌نماید و پس از احراز هویت نسبت به پخش کلید جلسه بین اعضای گروه اقدام می‌کند. این امر باعث کاهش تعداد احراز هویت‌ها و در نتیجه کاهش مدت احراز هویت کل گره‌ها می‌شود. همچنین در این احراز هویت از عملگرهای رمزنگاری استفاده نشده و فقط از عملگر XOR و تابع Hash استفاده شده است. بنابراین این روش یک پروتکل احراز هویت سبک‌وزن است. برای بیان احراز هویت از نمادهای جدول ۲ استفاده می‌شود. در ادامه، فازهای طرح ارائه شده است.

٤-۱ فاز مقداردهی اولیه

این مرحله توسط مدیر سیستم انجام می‌گیرد:

- مدیر سیستم یک کلید اصلی (K_{ser}) برای سرور در نظر می‌گیرد.
- این کلید در حافظه سرور ذخیره می‌گردد.



شکل ۳: فاز احراز هویت.

- در ضمن برای هر گروه، گره مدیر گروه و گره‌های عضو گروه مشخص می‌شوند.

٤-۲ فاز ثبت نام گره مدیر گروه

توسط سرور برای هر گروه یک شناسه یکتا ID_{GMa}، مقدار یکتای r و مقدار تصادفی Tk در نظر گرفته می‌شود.

- توسط مدیر سیستم مقادیر زیر محاسبه می‌گردد

$$AGMa = r \oplus Kser$$
$$BGMa = h(r.Kser)$$
$$X = IDGMa \oplus h(r.Kser)$$

- رکورد $IDGMa, AGMa, BGMa, Tk$ در حافظه گره مدیر گروه ذخیره می‌گردد.
- رکورد $AGma, X, Tk$ در حافظه سرور ذخیره می‌گردد.

٤-۳ فاز احراز هویت

در مرحله احراز هویت (شکل ۳)، گره مدیر گروه و سرور به طور متقابل یکدیگر را احراز هویت می‌کنند.

٤-٤ فاز پخش کلید بین گره مدیر و گره‌های عضو گروه

پس از آن که احراز هویت توسط گره مدیر گروه انجام گردید، کلید جلسه توسط مدیر گروه بین بقیه اعضای گروه پخش می‌شود. اعضای گروه تا زمان اعتبار کلید جلسه می‌توانند بدون انجام احراز هویت از آن استفاده نمایند. در ضمن برای پخش کلید از روش الگوی اشتراک رمز[1] استفاده شده است.

٥- شبیه‌سازی

در این بخش، شبیه‌سازی با استفاده از AVISPA ارائه شده و نشان می‌دهد که پروتکل در مقابل حملات امنیتی مقاوم است.

توضیحات و اطلاعات بیشتر در این خصوص را در [۲۱] تا [۲۳] می‌توانید پیدا نمایید. برای روش ارائه‌شده، جلسه‌های groupmanager، server، goal و environment در زبان HLPS مطابق شکل ۴ پیاده‌سازی شده‌اند.

1. Secret Sharing Scheme

```
role groupmanager(G,S: agent,
   Kser,IdGMa,R,Tok:message,
   Hash: hash_func,
   SND, RCV: channel(dy))
played_by G
def=
local State:nat,
 IDGMa,AGMa,BGMa,Tk,N1,Tc,M1,
 M2,M3,M4,M5,M6,Ts,N2c,M6c,M6N,
 Ks,Tkn,Y,AnGMa,BnGMa:message
init State:= 0
 /\ AGMa:= xor(R,Kser)
 /\ BGMa:= Hash(R.Kser)
 /\ Tk:= Tok
 /\ IDGMa:= IdGMa
transition
1. State = 0 /\ RCV(start)  =|>
 State' := 2
 /\ N1':= new()
 /\ Tc':= new()
 /\ M1':= xor(BGMa,N1')
 /\ M2':= Hash(IDGMa.AGMa.M1'.Tc'.N1')
 /\ secret(N1',sec1,{G,S})
 /\ SND(AGMa,M1',M2',Tc')
 /\ witness(G,S,server_groupmanager_nc,N1')
 /\ request(S,G,server_groupmanager_nc,N1')
2. State = 2 /\ RCV(M3,M4,M5,M6,Ts) =|>
 State' :=4
 /\ N2c' := xor(M3,BGMa)
 /\ M6N' := M6
 /\ M6c':=Hash(M3.M4.M5.N2c'.IDGMa.Tk.Ts)
3. State = 4 /\ M6c'=M6N' =|>
 State' :=6
 /\ Ks' := Hash(N1.N2c.Tk)
 /\ Tkn' := Hash(Ks'.N1.N2c)
 /\ Y' := Hash(IDGMa.N1.N2c)
 /\ AnGMa' := xor(xor(M4,Y'),N1)
 /\ BnGMa' := xor(M5,Y')
 /\ AGMa' := AnGMa'
 /\ BGMa' := BnGMa'
 /\ Tk' := Tkn'
end role
```

```
role server(G,S: agent,
    Kser,IdGMa,R,Tok:message,
    Hash:hash_func,
    SND, RCV: channel(dy))
played_by S
def=
 local State:nat,
AGMa,BGMa,X,Tk,M1,M2,Tc,Rs,BsGMa,N1s,
 IDsGMa,  M2s,M2S,N2,Ts,Rns, AnsGMa,BnsGMa,
Xns,M3,Y,M4,M5,Ks,Tkn,M6:message
 init State:= 1
  /\  AGMa:=  xor(R,Kser)
  /\ X:= xor(IdGMa,Hash(R,Kser))
  /\ Tk:=Tok
 transition
   1. State = 1 /\ RCV(AGMa,M1,M2,Tc) =|>
    State':=3
    /\ Rs' := xor(AGMa,kser)
    /\ BsGMa' := Hash(Rs',Kser)
    /\ N1s' := xor(M1,BsGMa')
    /\ IDsGMa' :=  xor(X,BsGMa')
    /\ M2S' := M2
    /\ M2s' := Hash(IDsGMa',AGMa,M1,Tc,N1s')
   2. State = 3   /\ M2S'=M2s' =|>
    State' := 5
    /\ N2' := new()
    /\ Ts' := new()
    /\ Rns' := new()
    /\ AnsGMa' := xor(Rns',Kser)
    /\ BnsGMa' := Hash(Rns',Kser)
    /\ Xns' := xor(IDsGMa,BnsGMa')
    /\ M3' := xor(N2',BnsGMa')
    /\ Y' := Hash(IDsGMa.N1s.N2')
    /\ M4' := xor(xor(AnsGMa',Y'),N1s)
    /\ M5' := xor(BnsGMa',Y)
    /\ Ks' := Hash(N1s,N2,Tk)
    /\ Tkn' := Hash(Ks'.N1s.N2')
    /\ AGMa' := AnsGMa'
    /\ X' := Xns'
    /\ Tk' := Tkn'
    /\ M6' := Hash(M3.M4.M5.N2'.IDsGMa.Xns'.Tkn')
    /\ secret(Ks',sec2,{G,S})
    /\ witness(G,S,server_groupmanager_ns,Ks')
    /\ request(S,G,server_groupmanager_ns,Ks')
    /\ SND(M3,M4,M5,M6,Ts)
end role
```

```
role session(G,S:agent,Kser,IdGMa,R,
     Tok:message,Hash:hash_func)
def=
 local SA,SB,RA,RB:channel(dy)
 composition

groupmanager(G,S,Kser,IdGMa,R,Tok,Hash,SA,RA)
/\ server(G,S,Kser,IdGMa,R,Tok,Hash,SB,RB)
 end role

 role environment()
 def=
  local
  Snd, Rcv: channel(dy)
  const g,s: agent,
  idGMa,r,tk,kser:message,
  h : hash_func,
  server_groupmanager_nc,
  server_groupmanager_ns,
  sec1,sec2: protocol_id
  intruder_knowledge = {g,s}
  composition
   session(g,s,kser,idGMa,r,tk,h)
   /\ session(s,g,kser,idGMa,r,tk,h)
 end role

 goal
  authentication_on server_groupmanager_nc
  authentication_on server_groupmanager_ns
  secrecy_of sec1 , sec2
 end goal
environment()
```

شکل ۴: کد احراز هویت با HLPSL.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/Auth.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.02s
  searchTime: 0.11s
  visitedNodes: 92 nodes
  depth: 11 plies
```

شکل ۵: نتیجه OFMC.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/Auth.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 37 states
  Reachable  : 33 states
  Translation: 0.02 seconds
  Computation: 0.01 seconds
```

شکل ۶: نتیجه CL-AtSe.

نتایج شبیه‌سازی ابزار AVISPA برای مدل OFMC و CL-AtSe نشان می‌دهد که طرح پیشنهادی تحت مدل OFMC (شکل ۵) و مدل CL-AtSe (شکل ۶) امن است و در برابر حملات فعال و غیر فعال از جمله حملات پخش مجدد و مرد میانی مقاوم است و روش ارائه‌شده را از نظر امنیتی تأیید می‌نماید.

٦- ارزیابی زمان اجرای پروتکل پیشنهادی

یکی از مهم‌ترین اهداف در انجام این پژوهش، کاهش زمان اجرای احراز هویت در گروه‌ها است و بنابراین در ادامه متوسط زمان اجرای احراز هویت به صورت دقیق بیان می‌شود. برای این منظور جدول ۳ شامل نمادها و توضیحات مربوط در نظر گرفته می‌شود تا با استفاده از آنها متوسط زمان اجرای احراز هویت گروه به دست آید.

متغیرهای تصادفی X_i برای $i=1,2,3$ از یکدیگر مستقل بوده و دارای توزیع پواسون با میانگین λ_i به ازای $i=1,2,3$ هستند. بنابراین برای احراز هویت در گروه اول، برآورد زمان انجام کار در سیستم به

جدول ۳: نمادها و توضیحات برای به دست آوردن متوسط زمان احراز هویت در گروه.

نماد	ویژگی	توضیحات
t_1	عدد ثابت مشخص	مدت زمان احراز هویت
$td1$	عدد ثابت مشخص	مدت زمان پخش کلید جلسه در گروه اول
$td2$	عدد ثابت مشخص	مدت زمان پخش کلید جلسه در گروه دوم
$td3$	عدد ثابت مشخص	مدت زمان پخش کلید جلسه در گروه سوم
T_1	عدد ثابت مشخص	بازه زمانی بین هر احراز هویت گروه اول
T_2	عدد ثابت مشخص	بازه زمانی بین هر احراز هویت گروه دوم
T_3	عدد ثابت مشخص	بازه زمانی بین هر احراز هویت گروه سوم
n_1	عدد ثابت مشخص	تعداد احراز هویت گروه اول که برابر تعداد T_1 است
n_2	عدد ثابت مشخص	تعداد احراز هویت گروه دوم که برابر تعداد T_2 است
n_3	عدد ثابت مشخص	تعداد احراز هویت گروه سوم که برابر تعداد T_3 است
X_1	متغیر تصادفی	تعداد گره‌هایی که در بازه T_1 در گروه اول عملیات احراز هویت انجام می‌دهند
X_2	متغیر تصادفی	تعداد گره‌هایی که در بازه T_2 در گروه دوم عملیات احراز هویت انجام می‌دهند
X_3	متغیر تصادفی	تعداد گره‌هایی که در بازه T_3 در گروه سوم عملیات احراز هویت انجام می‌دهند
λ_1	عدد ثابت مشخص	متوسط تعداد نیاز به احراز هویت گره‌ها در گروه اول در بازه T_1
λ_2	عدد ثابت مشخص	متوسط تعداد نیاز به احراز هویت گره‌ها در گروه دوم در بازه T_2
λ_3	عدد ثابت مشخص	متوسط تعداد نیاز به احراز هویت گره در گروه سوم در بازه T_3

صورت (۱) است

$$p_1 = n_1(t_1 + td_1) \quad (۱)$$

برای احراز هویت در گروه دوم برآورد زمان انجام کار در سیستم به صورت (۲) خواهد بود

$$p_2 = n_2(t_2 + td_2) \quad (۲)$$

همچنین برای احراز هویت در گروه سوم برآورد زمان انجام کار در سیستم به صورت (۳) است

$$p_3 = n_3(t_3 + td_3) \quad (۳)$$

پس از به دست آوردن ماکسیمم مقادیر p_i (فرمول (۴))، میانگین نهایی زمان اجرای احراز هویت با استفاده از (۵) به دست می‌آید

$$p = \max(p1, p2, p3) \quad (۴)$$

$$m = \frac{n_i(t_1 + td_i)}{\lambda_i} \Big/ p = p_i \quad (۵)$$

بر اساس نظر افراد خبره مقدار λ_i برای بزرگ‌ترین p_i بین ۳ تا ۸ می‌تواند باشد. اگر بدترین مقدار (۳) را در نظر بگیریم مقدار میانگین زمانی به صورت (۶) است

$$m = \frac{n_i(t_1 + td_i)}{3} \quad (۶)$$

۷- ارزیابی امنیتی در مقابل حملات

۷-۱ حمله جعل هویت گره

مهاجمان همواره در صدد نفوذ به گره‌های مختلف می‌باشند. در صورتی که مهاجم به هر نحوی بتواند به گره نفوذ کند و اطلاعات $IDGMa$، GMa، $BGMa$ و Tk موجود در حافظه آن را به دست آورد. از آنجایی که تمام این مقادیر Hash هستند، مهاجم اطاعات مفیدی از $BGMa$ و Tk نمی‌تواند به دست آورد. همچنین مهاجم نمی‌تواند r یا $Kser$ را از $AGMa = r \oplus Kser$ به دست آورد زیرا r تصادفی و تازه است. همچنین مقادیر $IDGMa$ و Tk در گره‌های مختلف متفاوت است. بنابراین مهاجم نمی‌تواند $AGMa$، $BGMa$، $IDGMa$ و Tk یا $AGMa$، $M1$، $M2$ و Tc را ایجاد نماید. در نتیجه طرح پیشنهادی ما، مقابله با حمله جعل هویت گره را تضمین می‌کند.

۷-۲ رازداری رو به جلو و رازداری رو به عقب

با توجه به افزایش قدرت نفوذ مهاجمان، رازداری رو به جلو و رازداری رو به عقب اخیراً مورد توجه زیادی قرار گرفته است. در روش ما، کلید جلسه به صورت $Ks = h(N1, N2, Tk)$ به دست می‌آید که $N1$ و $N2$ مقدار تصادفی تولیدشده در احراز هویت‌ها می‌باشند و $Tkn = h(Ks, N1, N2)$ را داریم که در آن مقادیر Ks، $N1$ و $N2$ در هر احراز هویت ایجاد می‌شوند. این وابستگی به مقادیر لحظه‌ای باعث می‌شود که اگر به هر نحوی کلید جلسه توسط مهاجم کشف شود، او نتواند کلیدهای جلسه قبلی یا بعدی را حدس بزند. پس با توجه به این که مقادیر $N1$ و $N2$ در هر احراز هویت به صورت تصادفی و جدید هستند، بنابراین Ks در هر احراز هویت متفاوت خواهد بود. حتی اگر مهاجم تمام داده‌های قبلی کانال را به دست آورد و کلید اصلی $Kser$ را کشف کند، در این صورت او می‌تواند $N1$ و $N2$ همان احراز هویت را به دست آورد و نمی‌تواند کلیدهای جلسه قبلی را به دست آورد، زیرا Tk هرگز در کانال منتقل نمی‌شود. فقط یک راه برای به دست آوردن Tk وجود دارد و آن مشاهده اطلاعات گره است. با وجود این، در صورت مشاهده و ضبط اطلاعات گره، مهاجم فقط می‌تواند آخرین Tk را به دست آورد و تمام Tkها را نمی‌تواند به دست آورد زیرا مقدار پارامتر دور قبلی Tk توسط تابع Hash رمزگذاری شده‌اند. بنابراین طرح ما دارای رازداری کامل است.

۷-۳ حمله جعل سرور

برای این حمله، مهاجم باید یک رکورد معتبر Ts، $M4$، $M5$، $M6$ و $M3$ را ایجاد کند. در این احراز هویت، مهاجم نمی‌تواند این رکورد معتبر را ایجاد نماید زیرا مهاجم نمی‌تواند $Kser$ را به دست آورد و همچنین از آنجایی که $M3 = N2 \oplus h(r, Kser)$ است، پس به هیچ وجه نمی‌تواند $M3$ معتبر نیز تولید کند. همچنین مهاجم

جدول ۴: مقایسه ویژگی‌های امنیتی و قابلیت‌ها.

طرح	الف	ب	ج	د
[۸]	×	×	×	×
[۹]	×	√	×	×
[۱۴]	√	×	×	×
[۱۵]	√	√	×	×
[۱۶]	√	√	×	×
[۵]	√	√	×	×
طرح ما	√	√	√	√

الف) رازداری رو به جلو و رازداری رو به عقب
ب) مقاوم در برابر حمله Jamming/desynchronization
ج) احراز هویت گروهی
د) مقیاس‌پذیری

نمی‌تواند $IDGMa$، Tk و $N1$ و در نتیجه $M4$، $M5$ یا $M6$ معتبر ایجاد کند، زیرا مقادیر آنها برابر $M4 = AGMa \oplus Y \oplus N1$، $M5 = BGMa \oplus Y$ و $M6 = h(M3, M4, M5, N2, IDGMa, TKn, Ts)$ هستند. با این شرایط مهاجم رکورد معتبر از Ts، $M4$، $M5$، $M6$ و $M3$ نمی‌تواند ایجاد نماید. پس طرح ما، مقابله با حمله جعل سرور را تضمین می‌کند.

۷-٤ حفظ حریم خصوصی

روش ما حریم خصوصی را از طریق گمنامی گره فراهم می‌آورد. در روش ما، شناسه گره ($IDGMa$) به طور مستقیم در کانال جابه‌جا نمی‌شود و ضمناً مهاجم نمی‌تواند $IDGMa$ را از طریق حمله استراق سمع به دست آورد. مقادیر r، $N1$، $N2$، Tc و Ts در هر احراز هویت کاملاً تصادفی انتخاب می‌شوند. بنابراین مقادیر $AGMa$، $M1$، $M2$، $M3$، $M4$، $M5$ و $M6$ در هر مرحله احراز هویت متفاوت می‌باشند و امکان به دست آوردن $IDGMa$ از طریق این اطلاعات وجود ندارد. این امر باعث می‌شود تا طرح ما حریم خصوصی از نوع گمنامی داشته باشد.

۸- مقایسه با روش‌های دیگر

در [۸] یک پروتکل احراز هویت متقابل سبک‌وزن در شبکه بی‌سیم بدن پیشنهاد شده که در مرحله احراز هویت، پارامترها به صورت پیوسته در گره و سرور به روز می‌شوند و چنانچه مهاجم در حین احراز هویت، کانال ارتباطی را قطع کند، امکان احراز هویت‌های بعدی برای این روش وجود ندارد. بنابراین در مقابل حمله jamming/desynchronization مقاوم نیست. در ضمن بین کلیدهای متوالی، وابستگی وجود دارد و در صورتی که یک کلید جلسه کشف شود، امکان کشف کلیدهای جلسه قبلی و بعدی برای مهاجم امکان‌پذیر است. پس این روش فاقد قابلیت رازداری رو به جلو می‌باشد. در [۹] روش احراز هویت سبک‌وزنی ارائه شده که در مقابل حملات jamming/desynchronization مقاوم است. در این روش نیز وابستگی بین کلیدها وجود دارد و فاقد قابلیت رازداری رو به جلو است. هر دو روش [۸] و [۹] مقیاس‌پذیر نبوده و امکان احراز هویت گروهی را ندارند.

در [۱۵]، یک پروتکل احراز هویت دستگاه برای خانه‌های هوشمند با استفاده از عملگرهای Hash و رمزگذاری ارائه شده است. این روش قابلیت‌های امنیتی بسیار بالایی دارد و رازداری رو به جلو و رازداری رو به عقب را پشتیبانی می‌کند. در [۱۶] یک طرح احراز هویت برای مراقبت‌های پزشکی پیشنهاد شده که در برابر حملات جعل هویت، حدس‌زدن رمز عبور، مرد میانی، jamming/desynchronization و پخش مجدد مقاوم است و همچنین رازداری رو به جلو و رازداری رو به عقب را پشتیبانی می‌کند. در هر دو روش [۱۵] و [۱۶] بین کلیدهای تولیدشده وابستگی وجود ندارد و بنابراین رازداری رو به جلو و رازداری رو به عقب را فراهم می‌آورند. در این دو روش، در هر مرحله از احراز هویت، گره‌ها مقادیر جدید و قدیمی پارامترهای احراز هویت را نگه می‌دارند. در صورتی که در حین احراز هویت، مهاجم اقدام به قطع ارتباط بین گره‌ها نماید، هر دو گره با استفاده از مقادیر قدیمی، پارامترها را مقداردهی مجدد می‌کنند و عملیات احراز هویت بعدی بدون مشکل انجام می‌شود. بنابراین این دو روش در مقابل حمله jamming/desynchronization مقاوم هستند. در ضمن [۱۵] و [۱۶] قابلیت احراز هویت گروهی را ندارند و مقیاس‌پذیر نیستند.

در [۱۴] یک احراز هویت سبک‌وزن کاربر برای سیستم مراقبت‌های پزشکی بر پایه ابر ارائه گردیده است که این روش در مقابل حمله jamming/desynchronization مقاوم نیست. در ضمن در این احراز هویت، بین کلیدهای تولیدشده ارتباطی وجود ندارد و کشف یکی از کلیدها منجر به کشف کلیدهای دیگر نمی‌شود، پس رازداری رو به جلو و رازداری رو به عقب را پشتیبانی می‌کند. در [۵] یک روش احراز هویت متقابل ارائه شده که از عملگرهای XOR و تابع Hash برای احراز هویت استفاده می‌کند. این روش در مقابل بیشتر حملات از جمله حمله jamming/desynchronization مقاوم است و حریم خصوصی را فراهم آورده و همچنین رازداری رو به جلو را نیز پشتیبانی می‌کند. در این روش، هیچ وابستگی بین کلیدهای جلسه وجود ندارد. در ضمن [۵] و [۱۴] امکان احراز هویت گروهی را ندارند و مقیاس‌پذیر نیستند.

در طرح ما یک احراز هویت متقابل گروهی ارائه شده و گره مدیر گروه به نمایندگی از طرف بقیه اعضای گروه اقدام به احراز هویت می‌کند و این امر باعث بالارفتن قابلیت مقیاس‌پذیری روش می‌گردد. روش ما در مقابل انواع حملات احراز هویت عملکرد خوبی دارد و در مقابل آنها مقاوم است. در هر مرحله از احراز هویت، گره حسگر و گره سرور مقادیر جدید و قدیمی پارامترهای احراز هویت را دارند. در صورتی که در حین احراز هویت، مهاجم اقدام به قطع ارتباط بین گره سرور و گره حسگر نماید، هر دو گره با استفاده از مقادیر قدیمی، پارامترها را مقداردهی می‌کنند و عملیات احراز هویت بعدی بدون مشکل انجام می‌شود. بنابراین طرح ما در مقابل حمله jamming/desynchronization مقاوم است. همچنین قابلیت رازداری رو به جلو و حریم خصوصی را از طریق گمنامی گره‌ها فراهم می‌آورد. در ضمن از عملگرهای XOR و تابع Hash برای احراز هویت استفاده می‌کند که این عملگرها بسیار سبک‌وزن هستند. در جدول ۴ مقایسه ویژگی‌های امنیتی و قابلیت روش‌ها ارائه شده است.

به طور کلی روش ما دارای مقیاس‌پذیری بالایی بوده و احراز هویت گروهی را فراهم می‌آورد و در مقابل حملات احراز هویت بسیار مقاوم است. در ادامه به بررسی هزینه اجرا و زمان اجرای روش‌ها می‌پردازیم. برای نشان‌دادن هزینه اجرای روش‌های مختلف از نمادهای زیر استفاده می‌شود:

- T_{Hash}: هزینه اجرای تابع Hash
- T_{XOR}: هزینه اجرای عملگر XOR
- $T_{Symmetric}$: هزینه اجرای عملیات رمزگذاری

در [۸] هزینه اجرای گره $5T_{Hash} + 2T_{XOR}$ و هزینه اجرای گره هاب $8T_{Hash} + 4T_{XOR}$ است. در [۹] هزینه اجرای گره مقدار $5T_{Hash} + 5T_{XOR}$

جدول ۵: مقایسه زمان اجرای احراز هویت بین روش ما و روش‌های قبلی.

طرح	هزینه اجرای حسگر/ کاربر	هزینه اجرای سرور/ هاب/ دروازه	زمان اجرای حسگر/ کاربر	زمان اجرای سرور/ هاب/ دروازه
[۸]	$5T_{Hash}+2T_{XOR}$	$8T_{Hash}+4T_{XOR}$	۰/۰۲۸ میلی‌ثانیه	۰/۰۴۲۸ میلی‌ثانیه
[۹]	$5T_{hash}+5T_{XOR}$	$8T_{Hash}+11T_{XOR}$	۰/۰۳۱ میلی‌ثانیه	۰/۰۴۳۵ میلی‌ثانیه
[۱۴]	$5T_{Hash}+6T_{XOR}$	$7T_{Hash}+4T_{XOR}$	۰/۰۳۲ میلی‌ثانیه	۰/۰۳۶۸ میلی‌ثانیه
[۱۵]	$4T_{Hash}+1T_{Symmetric}$	$5T_{Hash}+1T_{Symmetric}$	۰/۱۵۱۱ میلی‌ثانیه	۰/۱۵۶۳ میلی‌ثانیه
[۱۶]	$6T_{Symmetric}+8T_{Hash}$	$8T_{Symmetric}+6T_{Hash}$	۰/۸۲۴۴ میلی‌ثانیه	۰/۰۷۳۶ میلی‌ثانیه
[۵]	$5T_{hash}+5T_{XOR}$	$7T_{Hash}+9T_{XOR}$	۰/۰۳۱ میلی‌ثانیه	۰/۰۳۷۳ میلی‌ثانیه
طرح ما	$4T_{Hash}+5T_{XOR}$	$6T_{Hash}+9T_{XOR}$	۰/۰۲۵۸ میلی‌ثانیه	۰/۰۳۵۵۲ میلی‌ثانیه

و هزینه اجرای گره هاب $8T_{Hash}+11T_{XOR}$ است. در [۱۴] هزینه اجرای گره حسگر $5T_{Hash}+6T_{XOR}$ و هزینه اجرای گره دروازه $7T_{Hash}+4T_{XOR}$ است. در [۱۵] هزینه اجرای دستگاه برابر $4T_{Hash}+1T_{Symmetric}$ و هزینه اجرای گره دروازه برابر $5T_{Hash}+1T_{Symmetric}$ است. در [۱۶] هزینه اجرای گره کاربر برابر $6T_{Symmetric}+8T_{Hash}$ و هزینه اجرای گره دروازه برابر $8T_{Symmetric}+6T_{Hash}$ است. در [۵] هزینه اجرای گره $5T_{Hash}+5T_{XOR}$ و هزینه اجرای گره سرور $7T_{Hash}+9T_{XOR}$ است. در طرح ما هزینه اجرای گره $4T_{Hash}+5T_{XOR}$ می‌باشد و هزینه اجرای گره سرور برابر با $5T_{Hash}+9T_{XOR}$ است.

برای مقایسه زمان اجرای احراز هویت، می‌توان از زمان اجرای عملگر XOR صرف نظر نمود چون در مقایسه با تابع Hash و رمزگذاری، زمان اجرای ناچیزی دارد. با در نظر گرفتن محیط و پلتفرم تست به شرح پردازنده Intel(R) Core TM i۷ – ۴۷۱۰HQ ۲/۵۰GHz، حافظه ۸ GB و ویندوز ۸ نسخه ۶۴بیتی، زمان اجرای عملیات SHA –۲۵۶ برابر با ۰/۰۰۵۲ میلی‌ثانیه و زمان اجرای رمزگذاری، ۰/۱۳۰۳ میلی‌ثانیه است. بنابراین بر اساس این مقادیر زمان اجرای احراز هویت برای روش‌های مرتبط به دست می‌آید. هزینه اجرا و زمان اجرای احراز هویت‌های مرتبط در جدول ۵ ارائه شده است. در روش ما، هزینه زمانی احراز هویت در گره و سرور نسبت به روش‌های بررسی‌شده به ترتیب ۷/۸٪ و ۳/۵٪ کاهش یافته است. روش ما دارای زمان اجرای کمتری نسبت به روش‌های دیگر است.

۹- نتیجه‌گیری

در این مقاله، یک احراز هویت متقابل سبک‌وزن گروهی برای اینترنت اشیا پیشنهاد شد که باعث افزایش سرعت احراز هویت شده است. اشیا در گروه‌هایی قرار می‌گیرند و در هر گروه به جای احراز هویت تک‌تک گره‌ها فقط گره مدیر گروه اقدام به احراز هویت می‌کند و پس از احراز هویت، نسبت به پخش کلید جلسه بین اعضای گروه اقدام می‌کند. احراز هویت گروهی، مقیاس‌پذیری پروتکل پیشنهادی را بالا می‌برد. از طرفی، این امر باعث کاهش تعداد احراز هویت‌ها و در نتیجه کاهش مدت احراز هویت کل گره‌ها می‌شود و امکان استفاده از آن، در محیط‌های با گره‌های زیاد را بالا می‌برد. همچنین در احراز هویت از عملگرهای رمزنگاری آسنکرون استفاده نشده و فقط از عملگرهای XOR و Hash استفاده شده است. بنابراین این روش احراز هویت، یک پروتکل احراز هویت سبک‌وزن است. همچنین یک احراز هویت متقابل بین دو دستگاه ایجاد می‌کند که دو طرف همدیگر را اعتبارسنجی کرده و بر روی کلید جلسه به توافق می‌رسند. از آنجایی که شناسه گره‌ها بر روی کانال ارتباطی جابه‌جا نمی‌شود، حریم خصوصی از طریق گمنام گره فراهم می‌گردد. در ضمن طرح ما مشکلات امنیتی کمتری نسبت به طرح‌های قبلی دارد. در این مقاله از ابزار AVISPA برای تأیید امنیتی طرح استفاده کردیم. در روش ما، هزینه زمانی احراز هویت در گره و سرور نسبت به روش‌های بررسی‌شده به ترتیب ۷/۸٪ و ۳/۵٪ کاهش یافته است.

از محدودیت‌های روش ما ثابت‌بودن تعداد گروه‌ها و اعضای آنها است. در طرح ما تعداد گروه‌ها سه تا در نظر گرفته شده است، در حالی که تعداد گروه می‌تواند بر اساس نیاز تغییر کند. در ضمن گره‌ها توسط مدیر سیستم عضو گروه‌ها می‌شوند و امکان جابه‌جایی گره بین گروه‌ها وجود ندارد. در حالی که گره‌ها می‌توانند جابه‌جا شوند و باید قابلیت جابه‌جایی بین گروه‌ها برای اعضای آنها فراهم گردد.

ایجاد پویایی در تعداد گروه‌ها و امکان جابه‌جایی اعضای گروه‌ها می‌تواند جزء کارهای پژوهشی آتی باشد. در ضمن ارائه یک الگوریتم بهینه و امن برای توزیع کلید در فاز ۴ احراز هویت در پژوهش‌های آتی می‌تواند انجام گیرد.

مراجع

[1] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: a survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8-27, Feb. 2018.

[2] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, and W. Shi, "On security challenges and open issues in Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 83, pp. 326-337, Jun. 2018.

[3] Y. H. Chuang, N. W. Lo, C. Y. Yang, and S. W. Tang, "A lightweight continuous authentication protocol for the Internet of Things," *Sensors*, vol. 8, no. 4, Article No. 4, 26 pp., 2018.

[4] M. Dammak, O. Rafik, M. Boudia, M. A. Messous, S. M. Senouci, and C. Gransart, "Token-based lightweight authentication to secure IoT networks," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf.*, 4 pp., Las Vegas, NV, USA, 11-14 Jan. 2019.

[5] Z. Xu, C. Xu, W. Liang, J. Xu, and H. Chen, "A lightweight mutual authentication and key agreement scheme for medical Internet of Things," *IEEE Access*, vol. 7, pp. pp. 53922-53931, 2019.

[6] L. Harn, "Group authentication," *IEEE Trans. Comput.*, vol. 62, no. 9, pp. 1893-1898, Sept. 2013.

[7] A. Gupta, "A lightweight mutually authenticated key-agreement scheme for wireless body area networks in Internet of things environment," in *Proc. of the 24th Annual Int. Conf. on Mobile Computing and Networking*, pp. 804-806, New Delhi, India, 29 Oct.-2 Nov. 2018.

[8] M. Hamada, S. Kumari, and A. Kumar, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Comput. Methods Programs Biomed.*, vol. 135, pp. 37-50, Oct. 2016.

[9] C. Chen, B. Xiang, T. Wu, and K. Wang, "An anonymous mutual authenticated key agreement scheme for wearable sensors in wireless body area networks," *Appl. Sci.*, vol. 8, no. 7, Article No.: 1074, 2018.

[10] P. Punithavathi, S. Geetha, M. Karuppiah, S. K. H. Islam, M. M. Hassan, and K. R. Choo, "A lightweight machine learning-based authentication framework for smart IoT devices," *Inf. Sci.*, vol. 84, pp. 255-268, May 2019.

[11] K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," *Secur. Commun. Networks*, vol. 9, pp. 3095-3104, 2016.

[12] K. Fan, P. Song, and Y. Yang, "ULMAP: ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G," *Mob. Inf. Syst.*, vol. 2017, Article No.: 2349149, 7 pp., 2017.

[13] M. Durairaj and K. Muthuramalingam, "A new authentication scheme with elliptical curve cryptography for Internet of Things (IoT) environments," *Int. J. Eng. Technol.*, vol. 7, no. 2.26, pp. 119-124, 2018.

[14] G. Sharma and S. Kalra, "A lightweight user authentication scheme for cloud-IoT based healthcare services," *Iranian J. of Science and Technology-Trans. of Electrical Engineering*, vol. 43, pp. 619-636, 2019.

[15] A. Xiang and J. Zheng, "A situation-aware scheme for efficient device authentication in smart grid-enabled home area networks," *Electronics*, vol. 9, no. 6, Article No.: 989, 2020.

[16] P. Kumar and L. Chouhan, "A privacy and session key based authentication scheme for medical IoT networks," *Comput. Commun.*, vol. 166, pp. 154-164, 15 Jan. 2021.

[17] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327-1340, Oct. 2017.

[18] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: a decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126-142, Sept. 2018.

[19] L. Zhou, X. Li, K. H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Futur. Gener. Comput. Syst.*, vol. 91, pp. 244-251, Feb. 2019.

[20] Y. Chen, W. Xu, L. Peng, and H. Zhang, "Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT," *IEEE Access*, vol. 7, pp. 15210-15221, 2019.

[21] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198-208, Mar. 1983.

[22] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, and L. Compagna, "The AVISPA Tool for the Automated Validation," pp. 281-285.

[23] R. Amin and G. P. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Networks*, vol. 36, pt. 1, pp. 58-80, Jan. 2016.

رضا سرابی میانجی کارشناسی و کارشناسی ارشد مهندسی کامپیوتر-نرم‌افزار را به ترتیب در سال ۱۳۷۹ و ۱۳۸۱ دریافت کرد. از سال ۱۳۹۵ در دکترای مهندسی کامپیوتر- سیستم‌های نرم‌افزاری دانشگاه آزاد اسلامی واحد تهران شمال مشغول تحصیل و تحقیق است. وی چندین کتاب در زمینه شبکه‌های کامپیوتری، برنامه‌نویسی و طراحی صفحات وب ترجمه و تألیف نموده است. ایشان از سال ۱۳۷۹ در دانشگاه مشغول تدریس است. همچنین از سال ۱۳۸۰ در تیم‌های مدیریت شبکه‌های کامپیوتری، توسعه نرم‌افزار و مدیریت پایگاه داده بانک مرکزی جمهوری اسلامی ایران مشغول به کار هست. علایق تحقیقاتی وی شامل اینترنت اشیا، امنیت سیستم‌های اطلاعاتی، مدیریت و امنیت شبکه‌های کامپیوتری و مدیریت سیستم‌های پایگاه داده است.

سام جبه‌داری به عنوان دانشیار گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد تهران شمال مشغول به کار است. او مدرک کارشناسی مهندسی برق مخابرات و کارشناسی ارشد مهندسی برق مخابرات خود را به ترتیب از دانشگاه صنعتی خواجه نصیر طوسی و دانشگاه آزاد اسلامی واحد تهران جنوب دریافت کرد. وی مدرک دکترای مهندسی کامپیوتر را از دانشگاه آزاد اسلامی واحد علوم و تحقیقات دریافت نمود. علایق تحقیقاتی ایشان زمان‌بندی، QoS، MANET، امنیت شبکه‌های کامپیوتری، شبکه‌های حسگر بی‌سیم، محاسبات ابری، اینترنت اشیا و محاسبات لبه و مه است.

ناصر مدیری در سال ۱۳۶۵ مدرک کارشناسی الکترونیک را از دانشگاه ساسیکس انگلستان و در سال ۱۳۶۶ مدرک کارشناسی ارشد الکترونیک را از دانشگاه ساوت‌همپتون انگلستان دریافت کرد. همچنین در سال ۱۳۶۸ مدرک دکترای مهندسی کامپیوتر را از دانشگاه ساسیکس انگلستان دریافت نمود. ایشان از سال ۱۳۷۱ هیأت علمی دانشگاه بوده و در حوزه‌های تخصصی امنیت شبکه‌های کامپیوتری، امنیت نرم‌افزارهای کاربردی و فرایند توسعه امن نرم‌افزار فعالیت می‌نماید. ایشان چندین کتاب تخصصی در حوزه امنیت شبکه‌های کامپیوتری، امنیت نرم‌افزارهای کاربردی و فرایندهای توسعه امن نرم‌افزار چاپ کرده‌اند. علایق تحقیقاتی وی توسعه امن نرم‌افزار، امنیت شبکه‌های کامپیوتری، اینترنت اشیا، ERP، RFID، ISO/IEC ۲۷۰۰۰ و ISO/IEC ۱۵۴۰۸ است.