دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۲، جلد ۲۱، شماره ۲ (۱–۱۵)
https://monadi.isc.org.ir

ارائه‌شده در بیستمین کنفرانس بین‌المللی انجمن رمز ایران در سازمان پژوهش‌های علمی و صنعتی ایران، ۸ و ۹ شهریور ۱۴۰۲

یک طرح احرازهویت و توافق کلید امن مناسب شبکه‌های LoRaWAN★

زهرا جعفری[۱]، سحر پلیمی[۲]، محمدامین صبائی[۱]، رحمان حاجیان[۱] و سید حسین عرفانی[۳،*]

[۱]گروه مهندسی فناوری اطلاعات، دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران
[۲]گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد یادگار امام خمینی (ره) شهرری، تهران، ایران
[۳]گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
امنیت
احرازهویت متقابل
توافق کلید
ابزار AVISPA
منطق BAN

dor: 20.1001.1.24763047.1402.12.2.1.7

نوع مقاله: پژوهشی

چکیده

در محیط‌های مبتنی بر اینترنت اشیا، موضوع حفظ امنیت و حریم خصوصی دو نگرانی اصلی در برنامه‌های کاربردی و حیاتی آن هستند. پروتکل LoRa بطور مؤثر امکان ارتباط دوربرد را برای دستگاه‌های انتهایی با محدودیت منابع در شبکه LoRaWAN فراهم می‌کند که توسط افراد مختلف و دنیای صنعت پذیرفته شده و مورد استفاده قرار گرفته است. به منظور تسهیل استفاده از این فناوری و جلب اعتماد کاربران، اطمینان از امنیت و حریم خصوصی اطلاعات جمع‌آوری شده توسط دستگاه‌های انتهایی ضروری است که پروتکل‌های احرازهویت و توافق کلید در این زمینه پیشگام هستند. در این مقاله، یک طرح جدید برای احرازهویت و توافق کلید خاص شبکه LoRaWAN معرفی کرده‌ایم که احرازهویت متقابل را در میان شرکت‌کنندگان آن فراهم می‌کند و برای کاربر/ دستگاه‌های انتهایی و سرور شبکه این امکان را فراهم می‌کند تا بدون اعتماد بی‌قید و شرط، یک کلید نشست امن برقرار کنند. امنیت طرح پیشنهادی در ابتدا با استفاده از ارزیابی غیررسمی و مبتنی بر دانش فرد تحلیل‌گر، سپس از طریق ابزار AVISPA و منطق BAN به صورت رسمی به اثبات رسیده است. علاوه بر این، ضمن مقایسه برخی از طرح‌های احراز هویت موجود، نشان داده‌ایم که پروتکل پیشنهادی از منظر هزینه‌های مربوط به سربارهای محاسباتی و ارتباطی کارآمدتر است.

۱ مقدمه

تکامل زیرساخت‌های ارتباطی، فراگیر شدن اتصال‌های بی‌سیم را نوید می‌دهد و فناوری‌های متنوع آنها سبب ایجاد زمینه‌های جدید در اینترنت اشیا (IoT[۱]) خواهند شد. IoT با پذیرش پروتکل‌های ارتباطی و استانداردهای مختلف، فعال‌سازی ارتباط دستگاه‌های ناهمگن و اغلب با محدودیت منابع را تسهیل می‌بخشد [۱، ۲]. پهنای باند مصرفی، مقرون به صرفه بودن، افزایش قابلیت‌های سنجش سخت‌افزارها و مانند این موارد در کنار حفظ محرمانگی و حریم خصوصی چالش‌های پیش روی این شبکه‌ها است. فناوری‌های مربوط به شبکه IoT به سمت انتهای پشته پروتکل از جمله شبکه‌های Ethernet، Wi-Fi و به‌طور اختصاصی‌تر به سمت شبکه‌های LPWAN، Bluetooth، ZigBee، NFC و RFID در حال حرکت هستند که هر یک ویژگی‌های منحصر به فرد خود را دارند.

[1] Internet of Thing (IoT)

★از کمیته علمی بیستمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: ms.zahraajafarii@gmail.com (زهرا جعفری)، Sahar.palimii@gmail.com (سحر پلیمی)، Mohamad.amin.s.sut@gmail.com (محمدامین صبائی)، Hajian.rh@gmail.com (رحمان حاجیان)، h_erfani@azad.ac.ir (سید حسین عرفانی)

در این پژوهش، بر روی شبکه‌های LPWAN به ویژه شبکه LoRaWAN تمرکز می‌کنیم؛ این فناوری‌ها به طور گسترده به دو دسته شبکه‌های سلولی و شبکه‌های LPWAN بدون مجوز تقسیم می‌شوند که فناوری شبکه‌های سلولی، اعتبار خود را از طریق زیرساخت‌های سازگار و استانداردشده تضمین می‌کنند و از داده‌های بزرگتر، عمر باتری کمتر و سخت‌افزار ارزان‌تر پشتیبانی می‌کنند. LPWANهای بدون مجوز برای شبکه‌های سفارشی با نرخ داده کم، عمر باتری و پوشش گسترده تا کیلومترها طراحی شده‌اند که مشابه WiFi در مقیاس بزرگتر هستند. از جمله فناوری‌های مهم LPWAN می‌توان به NB-IoT، LoRa و مانند آن اشاره کرد [۳]. LoRa پروتکل لایه فیزیکی برای ارتباط‌های بی‌سیم LPWAN، بر راهکارهای مدلاسیون مانند CSS [۱] و FSK [۲] متکی است [۴]. LoRaWAN [۳] یک فناوری WAN در بالای لایه فیزیکی LoRa است که به دلیل دارا بودن عملکردهای ذاتی مدیریت شبکه به‌عنوان پروتکل به این لایه تعلق دارد [۵، ۶]. LoRaWAN متناسب با ویژگی‌های همنام آن یعنی برد طولانی، توان پایین، نرخ داده کم و شبکه‌های گسترده طراحی شده است [۲]. معماری یک سیستم LoRaWAN، علاوه بر دستگاه‌های انتهایی (ED [۴])، دروازه (GW [۵])، سرور شبکه (NS [۶])، سرور کاربرد (AS [۷]) و در صورت بهره‌گیری از نسخه 1.1، یک سرور پیوستن به شبکه را نیز فراهم می‌کند. سرورها مسئول فعال کردن دستگاه‌ها و ذخیره داده‌ها هستند و در صورت عدم فعال‌سازی، سرور پیام‌های آن را نادیده می‌گیرد؛ پس گره زمانی فعال در نظر گرفته می‌شود که دارای نسخه معتبر از مقادیر آدرس دستگاه، کلید نشست شبکه یعنی کلید مورد استفاده برای محاسبه یکپارچگی بسته‌های MAC و کلید نشست سرور کاربرد برای رمزگذاری پیام‌ها باشد [۷]. این پروتکل دو مکانیزم را برای فعال‌سازی دستگاه‌های موجود ارائه می‌دهد یکی ABP [۸]، کلیدهای نشست دستگاه‌ها به‌صورت پیش فرض در دستگاه بارگذاری شده و نیازی به احرازهویت برخط ندارد و دیگری OTAA [۹]، نشان می‌دهد که گره از قبل با AppKey پیکربندی شده و باید با ارسال یک «درخواست پیوستن» با سرور شبکه ارتباط برقرار کند که برخی از پارامترهای خود را مشخص می‌کند. هنگامی که مقادیر دریافتی تأیید شوند، سرور اقدام به تولید کلیدها و ارسال «پذیرش درخواست پیوستن» می‌کند [۲]. خطر نقض امنیت و حریم خصوصی در LoRaWAN به دلیل ماهیت بی‌سیم پروتکل‌های ارتباطی باند فرکانسی آن همواره وجود دارد؛ فعالیت‌های مناسبی باید انجام شود تا از حمله‌های مخربی که باعث عدم دستیابی به الزام‌های اساسی نظیر احرازهویت، محرمانگی، یکپارچگی و مانند آن می‌شود جلوگیری و نسبت به آن واکنش نشان داده شود. برای پشتیبانی از محرمانگی عملیات‌های LoRaWAN در حوزه‌های کاربردی، تکامل مکانیزم‌های امنیتی باید با آسیب‌پذیری و تهدیدهای متغیر سازگار شود. این امر به ویژه با توجه به پیچیدگی استاندارد و اصلاح مداوم آن چالش‌انگیز است. در عمل، امنیت روش‌های استاندارد شده باید همراه با پیاده‌سازی باشد که شامل پیوند رادیویی لبه شبکه با دستگاه‌های انتهایی، دروازه‌ها و زیرساخت‌ها است. تاکنون کارهای بسیاری در خصوص مدیریت کلید در شبکه LoRaWAN صورت گرفته است؛ با این حال در خصوص احرازهویت و توافق کلید توسط دستگاه‌های انتهایی، دروازه و سرورها کارهای محدودی انجام شده است. در این پژوهش، نقاط ضعف پروتکل ضیا و همکاران [۸] از جمله آسیب‌پذیری در برابر حمله‌های شخص میانی، نشت پارامتر مخفی و مانند آن برای محیط شبکه‌های بی‌سیم اثبات گردیده است. همچنین یک پروتکل احرازهویت متقابل و امن برای LoRaWAN ارائه داده‌ایم که علاوه بر جلوگیری از حمله‌های رایج در شبکه، از سربار ارتباطی و محاسباتی معقولی برخوردار است. پروتکل پیشنهادی می‌تواند جایگزین مناسبی برای فرایند احرازهویت و توافق کلید در پروتکل LoRa در چارچوب LoRaWAN باشد.

۱.۱ ساختار پژوهش

ادامه پژوهش حاضر به این شرح است که بخش ۲و ۳ به ترتیب دانش پیشین در زمینه امنیت شبکه LoRaWAN و نقاط ضعف طرح ضیا و همکاران [۸] را ذکر می‌کند. مدل شبکه، طرح احراز هویت و توافق کلید پیشنهادی در بخش ۴ ارائه شده است. ارزیابی پروتکل پیشنهادی با استفاده از تحلیل غیررسمی، شبیه‌ساز AVISPA، منطق BAN و سپس مقایسه با برخی روش‌های موجود در بخش ۵ انجام گرفته است. در آخر، در بخش ۶، نتیجه‌گیری و کارهای پیشنهادی آتی گردآوری شده است.

۲ کارهای پیشین

موضوع امنیت LPWANها به‌خصوص LoRaWAN در محیط IoT یک موضوع چالش‌انگیز است؛ به همین دلیل توسط محققان زیادی مورد توجه قرار گرفته است؛ به طوری که بروزترین مشارکت‌ها را می‌توان در سه مسیر اصلی طبقه‌بندی کرد: ۱) شرح کلی جنبه‌های امنیتی و آسیب‌پذیری‌های احتمالی، ۲) مکانیزم‌های جدید برای بهبود امنیت و ۳) جلوگیری از حمله‌های رایج در شبکه. عبدالحکیم و همکاران [۹] معتقدند بحرانی‌ترین مشکلات امنیتی LoRaWAN شامل نقطه خرابی در سرور شبکه، عدم محرمانگی، حمله‌های فیزیکی و عدم به‌روزرسانی کلیدها در OTAA و ABP است. اخیراً، برای رفع آسیب‌پذیری‌های امنیتی، نویسندگان راه‌حل‌های مدیریتی مختلفی را پیشنهاد کرده‌اند. ریبیرو و همکاران [۱۰] یک معماری امن برای مدیریت کلید مبتنی بر قراردادهای هوشمند و زنجیره قالب‌ها [۱۰] برای افزایش امنیت و دسترسی‌پذیری در شبکه‌های LoRaWAN پیشنهاد دادند و برای نشان دادن امکان‌سنجی این معماری مبتنی بر زنجیره قالب‌ها، یک نمونه اولیه با استفاده از ابزارهای منبع باز و سخت‌افزاری ایجاد کردند. یک روش تولید کلید نشست توسط تسای و همکاران [۱۱] پیشنهاد شد که با ادغام رمزنگاری منحنی بیضوی و AES-128، کلیدهای نشست برای سرورها ایجاد می‌شوند. توماس و همکاران [۱۲] با توضیح حمله شخص میانی که در لایه فیزیکی LoRaWAN و در

[1] Chirp Spread Spectrum (CSS) [2] Frequency-Shift Keying (FSK) [3] Long Range Wide Area Network (LoRaWAN) [4] End Device (ED) [5] Gateway (GW) [6] Network Server (NS) [7] Application Server (AS) [8] Activation By Personalization (ABP) [9] Over-The-Air Activation (OTAA)

[10] Blockchain

طول ارتباطات رمزگذاری شده بین دو ماژول همتا از طریق شبکه بی‌سیم اتفاق می‌افتد، راهکاری جدید در برابر این حمله توسط الگوریتم‌های رمزنگاری ارائه کردند تا بتواند اثرات آن را کاهش دهد. برای شبکه LoRaWAN، جباری و باقرزاده [۱۳] یک مکانیزم برای استقرار کلیدهای تأییدشده توسط کاربر ایجاد کردند که به شرکت کنندگان اجازه می‌دهد تا هویت یکدیگر را تایید کنند. علاوه بر این، کاربران و دستگاه‌های انتهایی را قادر می‌سازد تا بدون اعتماد بی‌قید و شرط به سرور شبکه، یک کلید نشست امن بین خود برقرار کنند.

در سال‌های اخیر، طرح‌های احرازهویت و توافق کلید متعددی برای اطمینان از حفظ امنیت و حریم خصوصی موجودیت‌ها در محیط‌های IoT با منابع محدود مانند شبکه‌های حسگر بی‌سیم، خودرویی و شبکه‌های متحرک سراسری پیشنهاد شده‌اند. این پروتکل‌ها به‌گونه‌ای طراحی شده‌اند که قابلیت استفاده در دیگر کاربردها را با جایگزینی عامل‌های ارتباطی خود (بدون تغییر خاصی یا با کمی تغییر) دارند.

به دلیل نقص امنیتی طرح‌های احراز هویت دو عاملی مبتنی بر رمز عبور، نویسندگان مختلفی [۱۴–۱۶]، پروتکل‌های احراز هویت سه عاملی را مطرح کردند؛ چرا که داده‌های ذخیره شده در توکن توسط مهاجم در معرض خطر قرار می‌گیرد و نمی‌تواند ارتباط امن را تضمین کند. برای غلبه بر این ضعف‌ها، آنها افزودن عامل دیگری مانند اثر بیومتریک [1] را به این روش‌ها پیشنهاد دادند که دارای چندین ویژگی مهم از جمله مقاومت در برابر جعل است. ژو و همکاران [۱۷] یک طرح احرازهویت سبُک‌وزن در محیط رایانش ابری ارائه کردند که پلاز و همکاران [۱۸] نشان دادند طرح آنها نمی‌تواند در برابر حمله‌های جعل، عامل درونی، شخص میانی، حدس رمز عبور و تسخیر کلید نشست مقاومت کند. یو و همکاران [۱۹] نشان دادند که طرح پلاز و همکاران ضمن فقدان امنیت در برابر حمله‌های جعل، تکرار و تسخیر کلید نشست، به احرازهویت متقابل و قابلیت گمنامی دست پیدا نمی‌کند. با این وجود، طرح آنها نیز دارای نقاط ضعفی مانند عدم پایداری در حمله‌های جعل، تکرار، تسخیر کلید نشست، نشت پارامتر مخفی، عدم محرمانگی و مقیاس‌پذیری بوده و از فقدان قابلیت گمنامی رنج می‌برد. ضیا و همکاران [۸] چگونگی برقراری کلید نشست در یک شبکه حسگر بدن بین دستگاه‌ها، دروازه و گره کنترل (سرور) را مدل کرده‌اند.

به دلیل مشکلات زیادی از جمله آسیب‌پذیری در برابر حمله‌های امنیتی مختلف، عدم سازگاری با استاندارد شبکه، فقدان احرازهویت متقابل و مانند آن، بسیاری از پروتکل‌های موجود در LoRaWAN را نمی‌توان برای ارائه خدمات امنیتی مورد نیاز استفاده کرد. برخلاف کارهایی که مورد بحث قرار گرفتند، در پژوهش فعلی، طراحی زیرساختی را گزارش می‌کنیم که یک طرح جدید احراز هویت و توافق کلید امن برای شبکه LoRaWAN است. طرح پیشنهادی احراز هویت متقابل و ایجاد کلیدهای نشست را در بین موجودیت‌ها فراهم می‌کند که با استاندارد شبکه سازگار است و از همان رمزنگاری‌های اولیه استاندارد LoRaWAN استفاده می‌کند. برای

[1] Biometrics

جدول ۱. نمادهای استفاده شده در این پژوهش

ID_i, GID_j, ID_{NS}: شناسه‌های طرفین	CID_x: شناسه مخفی شده x
PW_i, BIO_i: رمزعبور و بیومتریک	$T_1, T_2, \ldots$: مُهرزمانی
SK: کلید نشست کاربر، دروازه و سرور SK_{is}: کلید نشست انتهایی کاربر و سرور	
$\|\|$: عملگر الحاق	$\mathcal{A}$: مهاجم
$h(\cdot)$: تابع چکیده‌ساز	$\oplus$: عملیات XOR

سادگی مفاهیم، نمادهای استفاده شده در این پژوهش و توضیحات آنها در جدول ۱ آمده است.

۳ آسیب‌پذیری‌های طرح ضیا و همکاران

ضیا و همکاران مدعی شدند که طرح ابداعی آنها در مقایسه با سایر روش‌ها مقیاس‌پذیر، امن و سُبک‌وزن است؛ در برابر حمله‌های مختلف مقاوم بوده و از نظر سربار ارتباطی و محاسباتی کارآمدتر است. در اینجا، با هدف تمرکز بر روی روش پیشنهادی مقاله (بخش ۴)، از توضیح طرح ضیا و همکاران صرف نظر کرده‌ایم؛ اما پیشنهاد می‌شود برای مشاهده جزئیات طرح آنها به [۸] مراجعه شود. در ادامه با تجزیه و تحلیل عملکرد پروتکل آنها، حمله‌هایی که مطابق مدل‌های شناخته‌شده Dole-Yao [۲۰] و CK [۲۱] می‌تواند در این طرح رخ دهد را به صورت گام به گام شرح داده‌ایم.

حمله جعل ناشی از تسخیر کلید سرور: با افشای کلید خصوصی سرور (K_{cn})، مهاجم (A) این حمله را پیاده‌سازی می‌کند.

(۱) $\mathcal{A}$ با دریافت پیام اول و دوم، به شناسه گره دروازه (id_mn) و شناسه گره سنجش (tid_w) و مقدار y_m دست پیدا می‌کند؛ به کمک این دو کلید، مقادیر

$$(id_w \| r_{sa}) \leftarrow D_{cn},$$
$$X_{in} \leftarrow h(id_{mn} \| K_{cn}),$$
$$x_m = h(id_w \| K_c n),$$
$$r_m = x_m \oplus r_m,$$
$$c_m \leftarrow h(K_{cn} \| id_w)$$

را محاسبه می‌کند.

(۲) عدد تصادفی $f_m^{\mathcal{A}}$ را انتخاب و

$$\alpha_c^{\mathcal{A}} \leftarrow h(K_{cn} \| id_w) \oplus f_m^{\mathcal{A}}$$
$$tid_w^{\mathcal{A}^{new}} \leftarrow \mathcal{E}_{K_{cn}}(id_w \| f_m^{\mathcal{A}})$$
$$\eta_c^{\mathcal{A}} \leftarrow h(h(_{cn} \| id_w) \| f_m^{\mathcal{A}}) \oplus tid_w^{\mathcal{A}^{new}}$$
$$\beta_c^{\mathcal{A}} \leftarrow h(x_m \| r_m \| f_m^{\mathcal{A}} \| \eta_c^{\mathcal{A}})$$

و در نهایت کلید نشست جعلی $S_K^{\mathcal{A}} \leftarrow h(id_w \| r_m \| f_m^{\mathcal{A}} \| K_m)$ و مقدار $V_c^{\mathcal{A}} \leftarrow h(id_{mn} \| X_{in} \| T_3)$ را محاسبه و پیام جعل شده $\{\alpha_c^{\mathcal{A}}, \beta_c^{\mathcal{A}}, \eta_c^{\mathcal{A}}, V_c^{\mathcal{A}}, T_3\}$ را برای گره دروازه ارسال می‌کند.

(۳) گره دروازه و گره سنجش قادر به تشخیص پیام اصلی و جعلی نخواهند بود، مهاجم این حمله را با موفقیت پیاده‌سازی می‌کند.

حمله متن آشکار معلوم. دستگاه حسگر ضمن دانستن شناسه خود، id_w، مقدار مخفی f_m را از سرور دریافت می‌کند؛ پس هم متن رمزشده $(tid_w^{new} = Enc_{K_{cn}}(id_w \| f_m))$ و هم متن آشکار $(id_w$ و $f_m)$ را در اختیار دارد؛ یعنی تلاش خود برای دستیابی به کلید سرور یعنی cn را انجام می‌دهد. در نتیجه، طرح پیشنهادی در مقابل این حمله ناامن است.

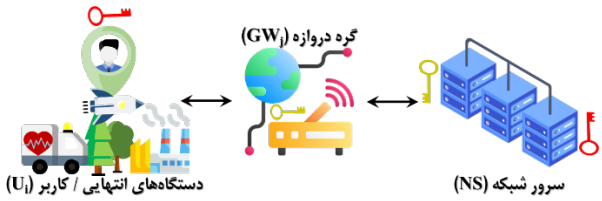
حمله شخص میانی. در فرایند احراز هویتی که توسط دروازه انجام می‌شود هیچ مشخصاتی از گره حسگر $V_c \leftarrow h(id_{mn} \| X_{in} \| T_۳)$ تأیید و بررسی نمی‌شود؛ پس عامل درونی متخاصم به راحتی می‌تواند پیام سرور را دریافت، و با جعل خود به عنوان یک دروازه تأیید شده، در اختیار گره حسگر قرار دهد و حمله سیبل را پیاده‌سازی کند. همچنین در پیام دوم، فرایند احراز هویت گره حسگر و دروازه کاملا مجزا از یکدیگر هستند و سرور به هیچ عنوان قادر به تشخیص تناظر بین پیام‌های گره حسگر و دروازه با یکدیگر نخواهد بود؛ چرا که تنها قادر به تشخیص تازگی پیام است.

حمله افشای پارامتر مخفی. با افشای f_m، مهاجم به $c_m = \alpha_c \oplus f_m$ و $tid_w^{new} = h(c_m \| f_m) \oplus \eta_c$ دسترسی پیدا می‌کند. α_c و η_c در کانال عمومی منتشر شده و tid_w^{new} در دور بعد به عنوان شناسه موقت در کانال ارسال می‌شود، به این ترتیب پیام‌های گره حسگر قابل رهگیری هستند. همچنین با داشتن c_m، مهاجم می‌تواند همه‌ی f_mهای دورهای بعد را به‌صورت $f_m = c_m \oplus \alpha_m$ که یک پارامتر موقت مهم برای ساخت کلید نشست است، بدست آورد. مهاجم برای دسترسی به کلیه اطلاعات گره حسگر، از جمله کلید نشست، تنها به یک شناسه id_w احتیاج دارد که با افشای آن مهاجم می‌تواند شانس خود را حتی برای دستیابی به کلید سرور از طریق حمله دانستن متن رمزشده و متن آشکار امتحان کند.

در بخش بعدی در راستای حل مشکلات این پروتکل و دیگر طرح‌های پیشین، روش پیشنهادی و جزئیات مربوط به آن را ارائه داده‌ایم.

۴ روش پیشنهادی

معماری شبکه LoRaWAN از دستگاه‌های انتهایی مبتنی بر LoRa (حسگرها و عملگرها)، دروازه‌ها، سرور شبکه و در آخر سرور نرم‌افزار کاربری تشکیل شده است. همانطورکه در شکل ۱ نشان داده شده است، مدل شبکه برای روش پیشنهادی نیز مبتنی بر همین ساختار است. شبکه‌های LoRaWAN در یک توپولوژی ستاره‌ای قرار گرفته‌اند که در آن دروازه‌ها بسته‌های بین دستگاه‌ها و سرور شبکه را کنترل می‌کنند. سرور شبکه، به نوبه خود، بسته‌های دریافت شده توسط دروازه را به یک سرور برنامه مرتبط هدایت می‌کند. ارتباط عموما دو طرفه است، اگرچه انتظار می‌رود که ارتباط uplink از یک دستگاه به شبکه و سرورهای



شکل ۱. معماری شبکه LoRaWAN برای طرح پیشنهادی

برنامه ترافیک غالب باشد. علاوه بر این، لینک‌ها می‌توانند توسط چندین دروازه دریافت شوند. این لینک ارتباطی می‌تواند توسط شبکه 3G، LTE، Ethernet و یا شبکه‌های داخلی طراحی شود و در آخر اطلاعات توسط سرور شبکه در اختیار نرم‌افزار کاربران قرار می‌گیرد.

طرح احرازهویت و توافق کلید پیشنهادی خاص شبکه LoRaWAN طراحی شده است. مراحل روش پیشنهادی به شرح زیر است.

۱.۴ مرحله آغازین و ثبت‌نام اولیه

در ابتدا سرور شبکه NS، کلید خصوصی s را ایجاد و نزد خود نگه می‌دارد. از طرف دیگر، مجموعه شناسه‌های معتبری را تولید می‌کند تا به کاربران و گره‌های دروازه اختصاص دهد. لازم به ذکر است که برای سادگی محاسبات و امکان مقایسه با طرح‌های ارائه‌شده در دیگر محیط‌های IoT، سرور شبکه و سرور کاربرد را به عنوان یک موجودیت در نظر گرفته‌ایم.

۲.۴ مرحله ثبت‌نام

در ابتدا گره دروازه در NS ثبت‌نام می‌شود تا بتواند به کاربران خدماتی را ارائه دهد و سپس کاربر/گره انتهایی به NS دسترسی پیدا می‌کند تا بتواند در آن ثبت‌نام انجام دهد. جزئیات هر بخش در زیر به تفصیل بیان شده است.

۱.۲.۴ ثبت‌نام گره دروازه در سرور شبکه

جزئیات ثبت‌نام GW_j در NS شامل مراحل زیر است:

۱) GW_j شناسه (GID_j) را انتخاب و عدد تصادفی (β_j) را تولید کرده و از طریق یک کانال خصوصی برای NS ارسال می‌کند.

۲) NS صحت شناسه دریافتی را بررسی و با تولید پارامتر مخفی r_j، $CID_j = h(GID_j \| \beta_j)$ و $GI_j = h(CID_j \| h(s \| r_j))$ را محاسبه می‌کند. NS پس از ارسال $\langle CID_j, GI_j \rangle$ برای GW_j از طریق کانال خصوصی، CID_j و r_j را در حافظه ذخیره می‌کند.

۲.۲.۴ ثبت‌نام کاربر در سرور شبکه

جزئیات ثبت‌نام U_i در NS شامل مراحل زیر است:

۱) در برخی موارد، به دلیل عدم وجود عامل انسانی در دستگاه‌های انتهایی، اثر بیومتریک پشتیبانی نمی‌شود؛ در نتیجه، بهره‌گیری از این

فاکتور می‌تواند یک امر اختیاری باشد. پس، دو سناریو خواهیم داشت:

- سناریو ۱ / طرح پیشنهادی سه فاکتوره: U_i شناسه (ID_i)، رمز عبور (PW_i) را انتخاب و اثر بیومتریک (BIO_i) را وارد می‌کند. سپس تابع $\langle R_i, P_i\rangle = Gen(BIO_i)$ را اعمال کرده و مقادیر P_i (مقدار آستانه خطای قابل تحمل در استخراج ویژگی‌های بیومتریک) و R_i (داده منحصر به فرد بیومتریک) را استخراج می‌نماید. همچنین، تابع $Rep(*)$ به جهت استخراج اطلاعات بیومتریک از عامل بیومتریک وارد شده استفاده می‌شود.
- سناریو ۲ / طرح پیشنهادی دو فاکتوره: U_i شناسه (ID_i) و رمز عبور (PW_i) را انتخاب می‌کند. پس از تولید عدد تصادفی (α_i)، شناسه و مقادیر مخفی شده‌ای را که از مقادیر اصلی تولید شده‌اند $CID_i = h(ID_i\|\alpha_i)$ و $CPW_i = h(ID_i\|PW_i\|\alpha_i)$ را محاسبه می‌کند و $\langle CID_i, CPW_i, \alpha_i\rangle$ را برای NS در کانال خصوصی ارسال می‌کند.

۲) NS، $X_i = UI_i \oplus h(CPW_i)$، $UI_i = h(CID_i\|\alpha_i\|s)$، $Y_i = h(UI_i\|X_i)$ و $Z_i = h(UI_i\|s)$ را محاسبه و $\{X_i, Y_i, Z_i, h(*)\}$ را در کارت هوشمند (SC_i) ذخیره می‌کند؛ سپس مقدار UI_i و CID_i را درون حافظه خود نگهداری می‌کند.

۳) با توجه به وجود / فقدان اثر بیومتریک خواهیم داشت:

- سناریو ۱: U_i مقدار $L_i = h(R_i\|PW_i) \oplus \alpha_i$ را محاسبه و L_i و P_i را به SC_i اضافه می‌کند.
- سناریو ۲: U_i مقدار $L_i = h(ID_i\|PW_i) \oplus \alpha_i$ را محاسبه و L_i را به SC_i اضافه می‌کند.

۳.۴ مرحله ورود، احرازهویت متقابل و توافق کلید

اگر U_i درخواست استفاده از سرویس‌ها و خدمات GW_j را داشته باشد، باید به شبکه ورود کرده و پس از احراز هویت متقابل بر کلید مشترک در یک کانال ارتباطی عمومی توافق کنند. دو سناریو داریم:

- سناریو ۱: U_i پس از ورود SC_i (ID_i، PW_i، BIO_i)، $R_i = Rep(BIO_i, P_i)$، $\alpha_i = L_i \oplus h(R_i\|PW_i)$ را محاسبه می‌کند.
- سناریو ۲: U_i پس از ورود SC_i (ID_i، PW_i)، رابطه $L_i \oplus h(R_i\|PW_i)$ $= \alpha_i$ را محاسبه می‌کند.

سپس $CID_i = h(ID_i\|\alpha_i)$، $CPW_i = h(ID_i\|PW_i\|\alpha_i)$، $UI_i = X_i \oplus h(CPW_i)$ و $Y_i^* = h(UI_i\|X_i)$ را محاسبه می‌کند. پس از آن، SC_i شرط $Y_i^* =? Y_i$ را بررسی می‌کند که در صورت عدم برقراری شرط مذکور یک ورود غیرمجاز تشخیص داده شده و پس از سه تکرار اشتباه، کارت هوشمند غیرفعال خواهد شد. ادامه جزئیات این فاز به طور مفصل در جدول ۲ شرح داده شده است.

در آخر، U_i، GW_j و NS کلید $SK = h(n_i\|h(n_j\|n_s))$ را با یکدیگر به اشتراک می‌گذارند. همچنین U_i کلید $K_{is} = h(Z_i\|ID_i\|UI_i^{new}\|T_1)$ بین خود و سرور شبکه را محاسبه می‌کند.

۴.۴ مرحله بروزرسانی رمز عبور و اطاعات بیومتریک

کاربر U_i بدون نیاز به دخالت گره دروازه یا سرور شبکه، بروزرسانی رمز عبور و یا عامل بیومتریک خود را مطابق مراحل زیر انجام می‌دهد.

۱) U_i، کارت هوشمند خود (ID_i، PW_i، BIO_i) را وارد می‌کند.

۲) SC_i، $R_i = Rep(BIO_i, P_i)$ را به کمک آستانه خطای P_i به دست می‌آورد و $\alpha_i = L_i \oplus h(R_i\|PW_i)$ را بازیابی می‌کند؛ همچنین مقادیر $CID_i = h(ID_i\|\alpha_i)$، $CPW_i = h(ID_i\|PW_i\|\alpha_i)$، $UI_i = A_i \oplus h(CPW_i)$ و $Y_i^* = h(UI_i\|X_i)$ را محاسبه می‌کند. با برقراری شرط $Y_i^* =? Y_i$، عملیات ورود با موفقیت انجام شده پس کارت هوشمند درخواست رمز عبور و عامل بیومتریک جدید را برای U_i ارسال می‌کند.

۳) U_i، مقادیر جدید (PW_i^{new} و BIO_i^{new}) را وارد می‌کند.

۴) بعد از دریافت رمز عبور و اثر بیومتریک جدید از طرف U_i توسط SC_i، کارت هوشمند مقادیر $R_i^{new} = Rep(BIO_i^{new}, P_i)$، $L_i^{new} = \alpha_i \oplus h(R_i^{new}\|PW_i^{new})$، $CPW_i^{new} = h(ID_i\|PW_i^{new}\|\alpha_i)$ و $X_i^{new} = UI_i \oplus h(CPW_i^{new})$ و $Y_i^{new} = h(UI_i\|X_i^{new})$ را محاسبه می‌کند. در نهایت کارت هوشمند اطلاعات قدیمی $\{X_i, Y_i, L_i\}$ را با اطلاعات جدید $\{X_i^{new}, Y_i^{new}, L_i^{new}\}$ جایگزین می‌کند.

۵ ارزیابی روش پیشنهادی

در اینجا، پروتکل پیشنهادی به صورت غیررسمی با استفاده از دانش فردی و بصورت رسمی با AVISPA و منطق BAN تحلیل گردیده است؛ نتایج بدست آمده نشان می‌دهد که طرح ما در مقابل انواع حمله‌های رایج (مبنای مدل Dole-Yao [۲۰] و CK [۲۱]) امن بوده و پس از بررسی عملکرد شبکه، در مقایسه با طرح‌های پیشین از کارآمدی لازم برخوردار است.

۱.۵ تحلیل غیررسمی روش پیشنهادی

مقاومت پروتکل پیشنهادی در مقابل حمله‌های مختلف از جمله جعل، سرقت کارت هوشمند، شخص میانی و مانند آن به صورت غیررسمی در ادامه تحلیل شده است. طرح مذکور ضمن برخورداری از احراز هویت متقابل، قابلیت گمنامی و عدم ردیابی، در برابر انواع حمله‌های شناخته شده موجود در زمینه پروتکل‌های احرازهویت و توافق کلید مقاوم است.

مقاومت در برابر حمله جعل کاربر. اگر مهاجم (U_A) قصد جعل U_i را داشته باشد، می‌بایست پیامی مشابه $\langle CID_i, MAC_i, D_i, T_1\rangle$ و $\langle H_i, MAC_{2j}\rangle$ را تولید کند. به دلیل عدم دسترسی به α_i نمی‌تواند

جدول ۲. مرحله ورود، احراز هویت متقابل و توافق کلید در طرح پیشنهادی

کاربر (U_i)	گره دروازه (GW_j)	سرور شبکه (NS)
سناریو ۱: ورود ID_i، PW_i، BIO_i و محاسبه $R_i = Rep(BIO_i, P_i)$ $\alpha_i = L_i \oplus h(R_i \| PW_i)$ سناریو ۲: انتخاب ID_i، PW_i و محاسبه $\alpha_i = L_i \oplus h(ID_i \| PW_i)$ $CID_i = h(ID_i \| _i)$ $CPW_i = h(ID_i \| PW_i \| \alpha_i)$ $UI_i = X_i \oplus h(CPW_i)$ $Y_i^* = h(UI_i \| X_i)$ بررسی شرط $Y_i^* =? Y_i$، تولید n_i و محاسبه $D_i = h(UI_i \| T_1) \oplus n_i$ $MAC_i = h(Z_i \| n_i \| D_i \| GID_j \| T_1)$ ارسال پیام $\leftarrow \langle CID_i, MAC_i, D_i, T_1 \rangle$		
	بررسی مُهر زمانی $\|T_2 - T_1\| \leq \Delta T$ تولید n_j و محاسبه $D_j = h(T_2 \| GI_j) \oplus n_j$ $MAC_j, h(GID_j \| MAC_i \| GI_j \| n_j \| T_2)$ ارسال پیام $\leftarrow \langle CID_i, MAC_i, D_i, T_1, CID_j, D_j, MAC_j, T_2 \rangle$	
		بررسی مُهرزمانی $\|T_4 - T_2\| \leq \Delta T$ محاسبه $GI_j = h(CID_j \| h(s \| r_j))$ $n_j = D_j \oplus h(T_2 \| GI_j)$ $MAC_j^* = h(GID_j \| MAC_i \| GI_j \| n_j \| T_2)$ بررسی شرط $MAC_j^* =? MAC_j$، بازسازی UI_i از CID_i محاسبه $Z_i = h(UI_i \| s)$ $n_i = D_i \oplus h(UI_i \| T_1)$ $MAC_i^* = h(Z_i \| n_i \| D_i \| GID_j \| T_1)$ بررسی شرط $MAC_i^* ? = MAC_i$ تولید n_s و محاسبه $E_i = h(GI_j \| T_2) \oplus n_s$ $F_i = h(GI_j \| T_2 \| GID_j \| n_j) \oplus n_i$ $MAC_{SG} = h(E_i \| GI_j \| T_2 \| CID_i \| n_s)$ $MAC_SU = h(Z_i \| UI_i \| T_1 \| CID_j \| n_i)$ $SK = h(n_i \| h(n_j \| n_s))$ $CID_i^{new} = h(CID_i \| h(n_j \| n_s) \| Z_i)$ $UI_i^{new} = h(CID_i^{new} \| n_i \| UI_i)$ $SK_{is} = h(Z_i \| ID_i \| UI_i^{new} \| T_1)$ ارسال پیام $\leftarrow \langle MAC_{SG}, MAC_SU, E_i, F_i \rangle$
	محاسبه $n_s = E_i \oplus h(GI_j \| T_2)$ $MAC_{SG}^* = h(E_i \| GI_j \| T_2 \| CID_i \| n_s)$ بررسی شرط $M_{SG}^* =? M_{SG}$ و محاسبه $n_i = F_i \oplus h(GI_j \| T_2 \| GID_j \| n_j)$ $SK = h(n_i \| h(n_j \| n_s))$ $G_i = h(GID_j \| n_i)$ $H_i = G_i \oplus h(n_j \| n_s)$ $MAC2_j = h(MAC_{SU} \| SK \| G_i)$ ارسال پیام $\leftarrow \langle H_i, MAC2_j \rangle$	
محاسبه $MAC_SU^* = h(Z_i \| UI_i \| T_1 \| CID_j \| n_i)$ $G_i^* = h(GID_j \| n_i)$ $h(n_j \| n_s) = H_i \oplus G_i^*$ $SK = h(n_i \| h(n_j \| n_s))$ بررسی شرط $MAC2_j^* =? MAC2_j$ و محاسبه $CID_i^{new} = h(CID_i \| h(n_j \| n_s) \| Z_i)$ $UI_i^{new} = h(CID_i^{new} \| n_i \| UI_i)$ $X_i^{new} = UI_i^{new} \oplus h(CPW)$ $Y_i^{new} = h(UI_i^{new} \| X_i^{new})$ $Z_i^{new} = h(UI_i^{new} \| UI_i)$ $SK_{is} = h(Z_i \| ID_i \| UI_i^{new} \| T_1)$		

CID_i و همچنین به دلیل ناتوانی U_A در استخراج n_i، نمی‌تواند D_i و MAC_i را محاسبه نماید؛ پس طرح پیشنهادی در مقابل این حمله امن است.

مقاومت در برابر حمله جعل سرور شبکه. U_A به دلیل عدم آگاهی از n_i، n_j و n_s قادر به تولید $\langle H_i, MAC_{۲j}\rangle$ نخواهد بود. اگر مهاجم تلاش کند تا GW_j را با GID_j جعل نماید، NS مقدار دریافتی را با مقدار ذخیره شده در حافظه تطابق داده و در صورت اختلاف، پیام دریافت شده توسط NS رد می‌شود.

مقاومت در برابر حمله سرقت کارت هوشمند. با فرض دسترسی مهاجم به اطلاعات SC_i، مهاجم بدون داشتن ID_i، PW_i و BIO_i نمی‌تواند اطلاعات مفیدی را از مقادیر استخراج نمایند؛ چرا که این مقادیر توسط توابع چکیده‌ساز و یا عملیات XOR محافظت می‌شود.

مقاومت در برابر حمله شخص میانی و حمله تکرار. اگر U_A با شنود کانال عمومی قادر به تغییر و دستکاری پیام‌ها باشد؛ حتی با دسترسی به اطلاعات ذخیره شده در SC_i با هدف ایجاد یک کلید نشست معتبر، نمی‌تواند پیام درخواست ورود معتبری را ایجاد نماید؛ و یا از طریق ارسال مجدد پیام‌ها در کانال یک کاربر قانونی را جعل کند. چرا که هر پیام شامل مُهرهای زمانی و نانس‌های تصادفی و یک‌بار مصرف بوده که سبب می‌شود پیام فقط در زمان کوتاهی اعتبار داشته باشد و در هر دور احراز هویت تعویض می‌شوند. پس، پروتکل پیشنهادی در برابر حمله شخص میانی و حمله تکرار مقاوم خواهد بود.

مقاومت در برابر حمله حدس رمز عبور. به دلیل عدم دسترسی U_A به ID_i و BIO_i (استفاده از توابع چکیده‌ساز پی در پی)، کوچکترین تغییر در ورودی، نتایج خروجی این توابع را به طور کامل تغییر خواهد داد. از این رو مهاجم نمی‌تواند به طور صحیح حدس صحیح بزند.

مقاومت در برابر حمله ناهمگام‌سازی. برای این حمله، U_A بایستی کانال ارتباطی را به کمک راهکارهایی نظیر پخش نویز تخریب کند تا پیام احراز هویت به دست کاربر قانونی نرسد. با این حال، NS از CID_i برای بازیابی UI_i استفاده می‌کند؛ پس از تایید درخواست ورود، CID_i^{new} محاسبه و با CID_i جایگزین می‌شود. مهاجم، با فرض تخریب کانال، باز هم نمی‌تواند حمله را پیاده‌سازی کند چرا که کاربر می‌تواند مقدار CID_i^{new} را به صورت محلی بازیابی کند. بنابراین، طرح پیشنهادی در مقابل این حمله کارآمد است.

مقاومت در برابر حمله نشت پارامتر مخفی. U_A با دستیابی به یکی از نانس‌های کلید نشست (n_i، n_j و n_s) قادر به استخراج دیگر نانس‌ها نیست؛ به دلیل استفاده از توابع چکیده‌ساز به همراه مُهر زمانی که برگشت‌پذیر نبوده و مکانیزم ارسال و دریافت و بازیابی این نانس‌ها مستقل از یکدیگر است.

مقاومت در برابر حمله عامل درونی. در مرحله ثبت‌نام، UI_i هر کاربر مقدار منحصر به فردی است که عامل درونی دیگری به α_i و CID_i آن دسترسی ندارد. همچنین CID_i در هر دور با CID_i^{new} تعویض و مقدار Z_i ذخیره شده در SC_i برای هر کاربر جداگانه محاسبه شده و یکتا است. هر GW_j نیز شامل پارامترهای مخفی GI_j و CID_j بوده که بین گره دروازه و سرور شبکه نگهداری می‌شود. پس، پروتکل پیشنهادی نسبت به این حمله امن است.

گمنام و غیرقابل ردیابی بودن. در پروتکل پیشنهادی، کاربر در هر احراز هویت یک شناسه موقت (CID_i) را ایجاد و بجای شناسه اصلی در کانال ارسال می‌کند و شناسه خود را تغییر می‌دهد و یک شناسه جدید (CID_i^{new}) ارسال می‌کند که باعث می‌شود تا پیام‌های ارسالی از سمت کاربر توسط مهاجم غیرقابل ردیابی باشند. گره دروازه از CID_j که درخواست ثبت‌نام به آن تعلق یافته است بجای شناسه GID_j استفاده می‌کند. از این رو، طرح پیشنهادی قابلیت گمنامی را برای کاربران و گره‌های دروازه به ارمغان می‌آورد.

حفظ امنیت پیشرو. کلید نشست از $SK = h(n_i \| h(n_j \| n_s))$ مشتق شده که n_i، n_j و n_s نانس‌های تصادفی هستند که توسط U_i و GW_j و NS استفاده شده‌اند و در هر نشست متفاوت هستند. این مقادیر همراه با توابع چکیده‌ساز و پارامترهای مخفی در کانال ارسال و دریافت می‌شوند. از آنجایی که کلید خصوصی NS هیچ سهمی در تولید کلید نشست ندارد حتی در صورت دستیابی مهاجم، U_A قادر نخواهد بود کلید جلسات قبلی را بدست آورد؛ پس، امنیت پیشرو در طرح حفظ شده است.

مقایسه ویژگی‌های امنیتی پروتکل پیشنهادی با سایر طرح‌های مرتبط در این زمینه در جدول ۳ نشان داده شده است؛ در این جدول مقدار ✔ به معنی این است که پروتکل پیشنهادی ویژگی امنیتی مورد نظر را برآورده کرده و در مقابل حمله امن و مقاوم می‌باشد و مقدار ✘ عکس این موضوع را نشان میدهد. مطابق جدول مذکور، پروتکل پیشنهادی ویژگی‌های امنیتی بیشتری را در مقایسه با سایر طرح‌های موجود ارائه می‌دهد.

۲.۵ تحلیل رسمی روش پیشنهادی

در ادامه با تحلیل رسمی به کمک ابزار AVISPA و منطق BAN، دستیابی پروتکل به امنیت و احراز هویت متقابل نشان داده شده است.

۱.۲.۵ اثبات امنیت با استفاده از ابزار AVISPA

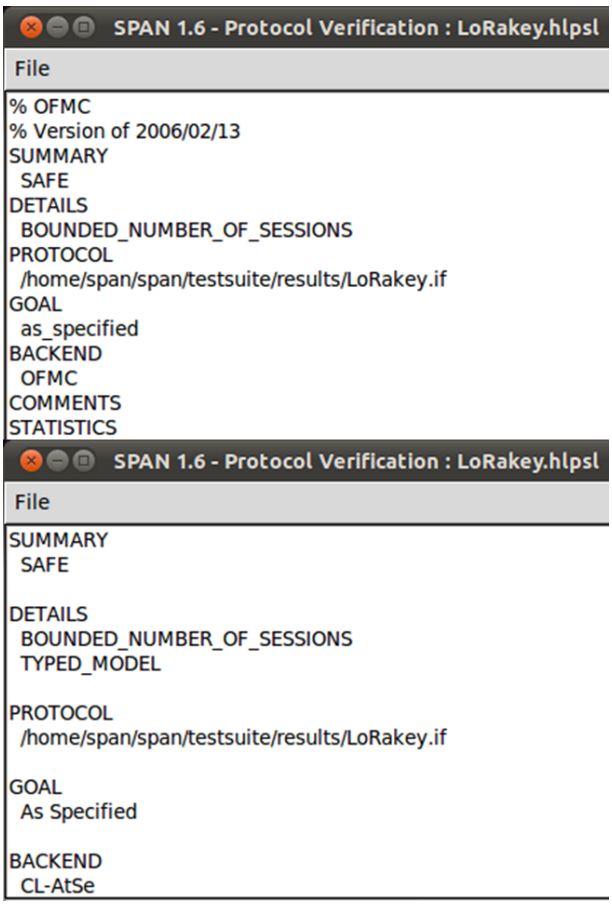
ابزار رسمی AVISPA از طریق HLPSL [1] پیاده‌سازی می‌شوند که مترجم HLPSL2IF مشخصات را به فرمت IF [2] تبدیل می‌کند. در نهایت، این فرمت می‌تواند ورودی برای Backendها در AVISPA باشد که برای تولید نتایج تایید پروتکل‌های احراز هویت شامل ATSE [3]، OFMC، SATMC و TA4SP است. خروجی AVISPA برای طرح احرازهویت

[1] High Level Protocol Specification Language (HLPSL) [2] Intermediate Format (IF) [3] ATtack SEarcher (ATSE)

جدول ۳. مقایسه امنیتی طرح پیشنهادی با سایر طرح‌ها

طرح	ویژگی‌های امنیتی											سربار محاسباتی	سربار ارتباطی
	الف	ب	ج	د	ه	و	ز	ح	ط	ی	ک		
[۱۷]	✘	✔	✘	✔	✔	✘	✔	✘	✘	✘	✔	$۳۶T_h$	$۲۴\|H\|$
[۱۸]	✘	✘	✔	✔	✔	✘	✔	✔	✘	✘	✔	$۴۰T_h + ۶T_{se}$	$۲۳\|H\|+۳\|TS\|+۱\|ID\|$
[۲۲]	✔	✔	✔	✔	✔	✔	✘	✔	✘	✔	✔	$۱۷T_h + ۱۵T_{ec}$	$۹\|H\|+۵\|TS\|+۱۰\|ECC\|$
[۸]	✔	✔	✘	✔	✔	✔	✘	✔	✘	✔	✔	$۱۶T_h + ۲T_{se}$	$۱۵\|H\|+۳\|TS\|+۳\|ID\|$
ours	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	$۳۵T_h$	$۱۵\|H\|+۳\|TS\|$

الف: مقاومت در برابر حمله جعل، ب: مقاومت در برابر حمله سرقت کارت هوشمند، ج: مقاومت در برابر حمله شخص میانی، د: مقاومت در برابر حمله حدس رمز عبور، ه: مقاومت در برابر حمله ناهمگام‌سازی، و: مقاومت در برابر مقاومت حمله تکرار، ز: مقاومت در برابر حمله نشت پارامتر مخفی، ح: مقاومت در برابر حمله عامل درونی، ط: مقاومت در برابر حمله تسخیر کلید، ی: قابلیت گمنامی و عدم ردیابی، ک: حفظ امنیت پیشرو.



شکل ۲. نتیجه OFMC و ATSE برای طرح پیشنهادی

پیشنهادی تحت OFMC و ATSE در شکل ۲ نشان داده شده است که از طریق SPAN [1] شبیه‌سازی می‌شود و نمودار توالی پیام را بر اساس نقش‌های مشخص شده تولید می‌کند. نتایج بدست آمده به وضوح نشان می‌دهد که پروتکل در اثر حمله‌های مختلف بی‌خطر و SAFE خواهد بود.

[1] Security Protocol Animator (SPAN)

۲.۲.۵ اثبات احراز هویت متقابل با استفاده از منطق BAN

ضمن شناخت نمادهای منطق BAN [۲۳]، با کمک قوانین منطقی آن و فرضیه‌های موجود در طرح باید به اهداف تعیین شده دست یابیم و نشان دهیم که احراز هویت متقابل بین شرکت‌کنندگان پروتکل حفظ می‌شود. مرحله ثبت‌نام و بروزرسانی پروتکل در یک کانال خصوصی انجام می‌شود؛ پس، فقط امنیت مرحله ورود و احراز هویت متقابل و توافق کلید نیاز به بررسی دارد. اثبات احراز هویت دو طرفه بین کاربر U_i، گره دروازه GW_j و سرور شبکه NS با استفاده از BAN به این صورت شکل می‌گیرد که در ابتدا پیام‌های ارسال شده در کانال عمومی به زبان این منطق ایده‌آل سازی می‌شوند

IDM1: $U_i \rightarrow GW_j : (CID_i, n_i, s, GID_j)_{UI_i}$
IDM2: $GW_j \rightarrow NS : (CID_i, n_i, s, GID_j, n_j)_{GI_j}$
IDM3: $NS \rightarrow GW_j : (n_s, n_i, UI_i, s)_{GI_j}$
IDM4: $GW_j \rightarrow U_i : (n_s, n_j, UI_i, GID_j, s)_{n_i}$

با دستیابی به اهداف زیر، احرازهویت متقابل و امنیت طرح محقق می‌گردد

G1: $GW_j \mid\mid\equiv NS \mid\equiv (n_s, n_i)$
G2: $GW_j \mid\equiv (n_s, n_i)$
G3: $NS \mid\equiv GW_j \mid\equiv (n_i, n_j)$
G4: $NS \mid\equiv (n_i, n_j)$
G5: $U_i \mid\equiv GW_j \mid\equiv (n_s, n_i)$
G6: $GW_j \mid\equiv (n_j, n_s)$

فرضیه‌ها و حالت‌های اولیه‌ای نیز در نظر گرفته می‌شود که با استفاده از ادوات، قوانین و فرضیه‌های منطق BAN ثابت می‌کنیم ارتباط امنی بین U_i، GW_j و NS وجود دارد. با توجه به IDM1 و IDM2 به استنتاج‌های زیر می‌رسیم:

- $GW_j \mid\equiv U_i \mid (CID_i, n_i, s, GID_j)_{UI_i}$
- $GW_j \mid\equiv U_i \# (CID_i, n_i, s, GID_j)_{UI_i}$
- $GW_j \mid\equiv U_i \mid\equiv (CID_i, n_i, s, GID_j)_{UI_i}$

- $GW_j|\equiv U_i|\equiv (n_i)_{UI_i}$
- $NS|\equiv GW_j|\ (CID_i, n_i, s, GID_j, n_j)_{GI_j}$
- $NS|\equiv GW_j|\equiv (CID_i, n_i, s, GID_j, n_j)_{GI_j} \rightarrow$ G3

از IDM3 و قانون معنای پیام، G1 از IDM4 و قانون معنای پیام G5 داریم

- $GW_j|\equiv NS|\ (n_s, n_i, UI_i, s)_{GI_j} \rightarrow$ G1
- $U_i|\equiv GW_j|\ (n_s, n_j, UI_i, GID_j, s)_{n_i}$
- $U_i|\equiv GW_j|\equiv (n_s, n_j, UI_i, GID_j, s)_{n_i} \rightarrow$ G5

با استفاده از هدف سوم و قانون اختیار به ترتیب بقیه اهداف G4، G2 و G6 نیز محقق می‌شود. طرفین به نانس‌های تصادفی به اشتراک گذاشته شده باور پیدا می‌کنند و یک احراز هویت متقابل سه‌بخشی ایجاد می‌شود.

۳.۵ تحلیل عملکرد روش پیشنهادی

با ارزیابی مقایسه‌ای، نشان می‌دهیم که طرح ما هنوز هم عملکرد بهتری در مقایسه با سایر طرح‌های [۸، ۱۷، ۱۸، ۲۲] از منظر هزینه محاسباتی و ارتباطی دارد. در ادامه، نمودارهای مقایسه سربار محاسباتی و ارتباطی در شکل ۳ نشان داده شده‌اند. از منظر هزینه ارتباطی، مرجع [۲۴] برای ارزیابی زمان انجام عناصر رمزنگاری از یک میکروکنترلر ARM ساخت شرکت NXP به نام LPC1788 استفاده شده است که بر روی این تراشه با استفاده از کتابخانه رمزنگاری ArduinoLibs بدست آمده است. بر این اساس، بین پروتکل پیشنهادی و سایر طرح‌ها، تابع چکیده‌ساز، محاسبات ضرب ECC، اعداد تصادفی، شناسه‌ها، و مهر زمانی به ترتیب ۲۵۶، ۳۲۰، ۱۲۸، ۱۲۸ و ۳۲ بیت در نظر گرفته شده است. جدول ۳ هزینه ارتباط طرح‌ها در مراحل ورود و تائید اعتبار را نشان می‌دهد. طرح پیشنهادی در مجموع با داشتن تنها $|TS|+۳|H|$، ۱۵، ۳۹۳۶ بیت سربار، کمترین میزان هزینه ارتباطی را نسبت به سایر طرح‌ها ارائه می‌کند و باعث بهبود عملکرد شبکه می‌گردد. زمان لازم برای اجرای عملیات‌های رمزنگاری نشان داده شده در جدول ۳، مطابق مرجع [۲۴] در نظر گرفته شده است که براساس گزارش کیلینک و یانیک [۲۵] بر روی یک رایانه شخصی با پردازنده Intel Pentium Dual CPU E2200 2.20GHz، رم 2048 MB و سیستم عامل Ubuntu 12.04.1 LTS 32bit بدست آمده است. شایان ذکر است که با توجه به منابع اشاره شده، $T_h \approx 0.0023$ ms زمان لازم برای عملیات تابع چکیده‌ساز، $T_{se} \approx 0.0046$ ms زمان لازم برای رمزگذاری/رمزگشایی متقارن و $T_{ec} \approx 2.226$ ms زمان لازم برای عملیات ضرب ECC در نظر گرفته شده است.

نتایج حاصل شده نشان می‌دهد که در مقایسه با طرح‌های مذکور، پروتکل پیشنهادی ما ویژگی‌های امنیتی بسیار بیشتری را پوشش می‌دهد و پس کارایی بهتری را ارائه می‌کند. به منظور بررسی دقیق‌تر، طرح ما به دلایلی همچون استفاده از مُهر زمانی، بررسی شرطهای برابری، توابع چکیده‌ساز پی در پی و مانند آن می‌تواند مقاومت در برابر حمله تسخیر کلید را ارائه دهد و در مقایسه با طرح‌های امن، کارایی محاسباتی معقول و تعداد پیام‌های کمتری دارد. در نتیجه، طرح ما با توجه به معیارهای کارایی و امنیت بهتر است.

۶ نتیجه‌گیری و پیشنهادات آتی

حفظ امنیت و حریم خصوصی LoRaWAN به عنوان یکی از حیاتی‌ترین موضوعات در اتخاذ و بکارگیری این شبکه است. در این مقاله، یک پروتکل ایجاد کلید امن برای فعال‌سازی احراز هویت متقابل در بین اعضای شبکه LoRaWAN پیشنهاد کردیم که می‌تواند بروزرسانی رمز عبور و اطلاعات بیومتریک را صرفاً از طریق کارت هوشمند پشتیبانی کند. رمزنگاری طرح پیشنهادی با کمک توابع چکیده‌ساز، در برابر حمله‌های فیزیکی محافظت می‌شود. ارزیابی غیررسمی و اثبات رسمی طرح با استفاده از منطق BAN و ابزار AVISPA، امن بودن آن را تایید کرده و در برابر حمله‌های مخرب مختلف مقاوم می‌کند. علاوه بر این، تجزیه و تحلیل عملکرد تصدیق کرد که طرح پیشنهادی کارآمد است. به عنوان کار پیشنهادی آینده، می‌توان یک پروتکل توافق کلید و احراز هویت با قابلیت تصحیح خطا ارائه نمود. همچنین یک پروتکل چهار عاملی ارائه نمود که در آن سرورهای کاربرد و شبکه به‌عنوان دو موجودیت مجزا در نظر گرفته شده باشند.

مراجع

[1] Rosendo, Miguel and Granjal, Jorge. Energy-aware security adaptation for low-power iot applications. *Network*, 2(1):36–52, 2022.

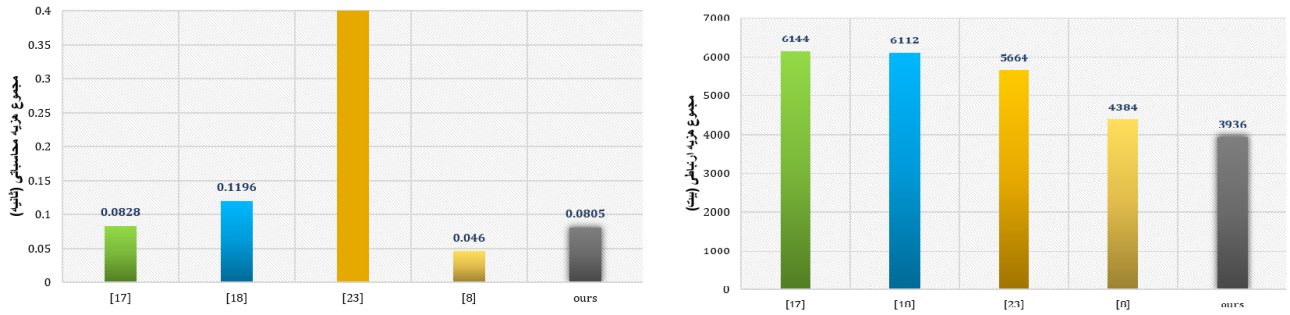
[2] Rizzardi, Alessandra, Sicari, Sabrina, and Coen-Porisini, Alberto. Analysis on functionalities and security features of internet of things related protocols. *Wireless Networks*, 28(7):2857–2887, 2022.

[3] Raza, Usman, Kulkarni, Parag, and Sooriyabandara, Mahesh. Low power wide area networks: A survey. *IEEE Commun. Surv. Tutorials*, 19(2), 2017.

[4] Mehic, Miralem, Duliman, Mugdim, Selimovic, Nejra, and Voznak, Miroslav. Lorawan end nodes: Security and energy efficiency analysis. *Alexandria Engineering Journal*, 61(11):8997–9009, 2022.

[5] Hessel, Frank, Almon, Lars, and Hollick, Matthias. Lorawan security: An evolvable survey on vulnerabilities, attacks and their systematic mitigation. *ACM Transactions on Sensor Networks*, 18(4):1–55, 2023.

[6] Noura, Hassan, Hatoum, Tarif, Salman, Ola, Yaacoub, Jean-Paul, and Chehab, Ali. Lorawan security survey: Issues, threats and possible mitigation techniques. *Internet*



شکل ۳. مقایسه هزینه محاسباتی و ارتباطی طرح پیشنهادی با سایر طرح‌ها

lightweight three-factor-based user authentication protocol for wireless sensor networks. in *Advances in Intelligent Systems and Computing: Proceedings of the 7th Euro-China Conference on Intelligent Data Analysis and Applications, May 29–31, 2021, Hangzhou, China*, pp. 319–326. Springer, 2022.

[15] Xu, Tao, Xu, Cheng, and Xu, Zisang. An efficient three-factor privacy-preserving authentication and key agreement protocol for vehicular ad-hoc network. *China Communications*, 18(12):315–331, 2021.

[16] Ryu, Jihyeon, Lee, Hakjun, Lee, Youngsook, and Won, Dongho. Smasg: secure mobile authentication scheme for global mobility network. *IEEE Access*, 10:26907–26919, 2022.

[17] Zhou, Lu, Li, Xiong, Yeh, Kuo-Hui, Su, Chunhua, and Chiu, Wayne. Lightweight iot-based authentication scheme in cloud computing circumstance. *Future generation computer systems*, 91:244–251, 2019.

[18] Martínez-Peláez, Rafael, Toral-Cruz, Homero, Parra-Michel, Jorge R, García, Vicente, Mena, Luis J, Félix, Vanessa G, and Ochoa-Brust, Alberto. An enhanced lightweight iot-based authentication scheme in cloud computing circumstances. *Sensors*, 19(9):2098, 2019.

[19] Yu, SungJin, Park, KiSung, and Park, YoungHo. A secure lightweight three-factor authentication scheme for iot in cloud computing environment. *Sensors*, 19(16):3598, 2019.

[20] Dolev, Danny and Yao, Andrew. On the security of public key protocols. *IEEE Transactions on information theory*, 29(2):198–208, 1983.

[21] Canetti, Ran and Krawczyk, Hugo. Analysis of key-exchange protocols and their use for building secure channels. in *International conference on the theory and of Things*, 12:100303, 2020.

[7] Fan, Chun-I, Zhuang, Er-Shuo, Karati, Arijit, and Su, Chun-Hui. A multiple end-devices authentication scheme for lorawan. *Electronics*, 11(5):797, 2022.

[8] Zia, Maryam, Obaidat, Mohammad S, Mahmood, Khalid, Shamshad, Salman, Saleem, Muhammad Asad, and Chaudhry, Shehzad Ashraf. A provably secure lightweight key agreement protocol for wireless body area networks in healthcare system. *IEEE Transactions on Industrial Informatics*, 19(2):1683–1690, 2022.

[9] Hakeem, Shimaa A Abdel, El-Kader, Sherine M Abd, and Kim, HyungWon. A key management protocol based on the hash chain key generation for securing lorawan networks. *Sensors*, 21(17):5838, 2021.

[10] Ribeiro, Victor, Holanda, Raimir, Ramos, Alex, and Rodrigues, Joel JPC. Enhancing key management in lorawan with permissioned blockchain. *Sensors*, 20(11):3068, 2020.

[11] Tsai, Kun-Lin, Leu, Fang-Yie, Hung, Li-Ling, and Ko, Chia-Yin. Secure session key generation method for lorawan servers. *IEEE Access*, 8:54631–54640, 2020.

[12] Thomas, John, Cherian, Season, Chandran, Saranya, and Pavithran, Vipin. Man in the middle attack mitigation in lorawan. in *2020 International Conference on Inventive Computation Technologies (ICICT)*, pp. 353–358. IEEE, 2020.

[13] Jabbari, Abdollah and Mohasefi, Jamshid Bagherzadeh. A secure and lorawan compatible user authentication protocol for critical applications in the iot environment. *IEEE Transactions on Industrial Informatics*, 18(1):56–65, 2021.

[14] Liu, Shuangshuang, Lee, Zhiyuan, Chen, Lili, Wu, Tsu-Yang, and Chen, Chien-Ming. On the security of a

applications of cryptographic techniques, pp. 453–474. Springer, 2001.

[22] Ma, Mimi, He, Debiao, Wang, Huaqun, Kumar, Neeraj, and Choo, Kim-Kwang Raymond. An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks. *IEEE Internet of Things Journal*, 6(5):8065–8075, 2019.

[23] Burrows, Michael, Abadi, Martin, and Needham, Roger. A logic of authentication. *ACM Transactions on Computer Systems (TOCS)*, 8(1):18–36, 1990.

[24] Abbasinezhad-Mood, Dariush, Ostad-Sharif, Arezou, Mazinani, Sayyed Majid, and Nikooghadam, Morteza. Provably secure escrow-less chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection. *IEEE Transactions on Industrial Informatics*, 16(12):7287–7294, 2020.

[25] Kilinc, H Hakan and Yanik, Tugrul. A survey of sip authentication and key agreement schemes. *IEEE communications surveys & tutorials*, 16(2):1005–1023, 2013.

پیوست‌ها (کد AVISPA)

```
%%% NO1 %%%  Basic Role : MobileUser(MU) %%% NO.1 %%%
role user(MU,GW,NS:agent,SKus:symmetric_key,H,Gen,Rep:hash_func,SND,RCV:channel(dy))
played_by MU
def=
    local
        State:nat,
        IDi,PWi,BIOi,Ai,Ri,PBi,CIDi,CPWi,Xi,Yi,Zi,Li,Ni,T1,Di,UIi,MACi,GIDj,CIDj,Hi,MAC2j,MACsu,Hnjns,Gi,SK,
            SKis,CIDinew,UIinew,Xinew,Yinew,Zinew:text
        const
        sec1,sec2,sec3,mu_gw_ni,mu_ns_ui,gw_mu_nj,ns_mu_maci:protocol_id
    init
        State:=0
    transition
% MU's REGISTRATION PHASE:
1.  State=0
                /\RCV(start)=|>State':=1
                /\IDi':=new()  /\PWi':=new()  /\BIOi':=new()  /\Ri':=Gen(BIOi')  /\PBi':=Gen(BIOi')  /\Ai':=new()
                    /\CIDi':=H(IDi'.Ai')
                    /\CPWi':=H(IDi'.PWi'.Ai')/\SND({CIDi'.CPWi'.Ai'}_SKus)
2. State=1
                /\RCV({Xi'.Yi'.Zi'}_SKus)=|>State':=2/\Ri':=Rep(BIOi.PBi)/\Li':=xor(H(Ri'.PWi),Ai)/\secret({
                    IDi,PWi},sec1,{MU})
% MU's LOGIN & MUTUAL AUTHENTICATION & KEY AGREEMENT PHASE :
                /\Ni':=new()  /\T1':=new()  /\CIDi':=h(IDi.Ai)  /\CPWi':=H(IDi.PWi.Ai)  /\UIi':=xor(Xi',H(CPWi
                    '))
                /\Di':=xor(H(UIi'.T1'),Ni')/\MACi':=H(Zi.Ni'.Di'.GIDj.T1')  /\SND(CIDi'.MACi'.Di'.T1')/\
                    witness(MU,GW,mu_gw_ni,Ni')
               /\ witness(MU,NS,mu_ns_ui,UIi')
3. State=2
                /\RCV(Hi'.MAC2j')=|>State':=3  /\MACsu':=H(Zi.UIi.T1.CIDj.Ni)/\Gi':=H(GIDj.Ni)/\Hnjns':=xor(Hi
                    ',Gi')
                /\SK':=H(Ni.Hnjns')/\secret({SK'},sec2,{MU,GW,NS})/\CIDinew':=H(CIDi.Hnjns'.Zi)/\UIinew':=H(
                    CIDinew'.Ni.UIi)
                /\Xinew':=xor(UIinew',H(CPWi))/\Yinew':=H(UIinew'.Xinew')/\Zinew':=H(UIinew'.UIi)/\SKis':=H(Zi
                    .IDi.UIinew'.T1)
                        \/ request(NS,MU,ns_mu_maci,MACsu')/\ request(GW,MU,gw_mu_nj,Hnjns')/\ secret({SKis
                            },sec3,{MU,NS})
end role
```

```
%%% NO.2 %%%  Basic Role : GateWay(GW) %%% NO.2 %%%
role gateway(MU,GW,NS:agent,SKgs:symmetric_key,H:hash_func,SND,RCV:channel(dy))
played_by GW
def=
    local
        State:nat,
            GIDj,Bj,CIDj,GIj,CIDi,MACi,Di,T1,Nj,Dj,MACj,MACsg,MACsu,Ei,Fi,Np,Ni,SK,Gi,Hi,MAC2j:text
        const
        sec4,sec5,mu_gw_ni,gw_mu_nj,gw_ns_nj,ns_gw_nj,ns_gw_macj:protocol_id
    init
        State:=0
    transition
% GW's REGISTRATION PHASE :
```

```
                1. State=0
                 /\RCV( start )=|> State ':=1/\ GIDj ':=new()    /\ Bj ':=new() /\SND({ GIDj '. Bj '}_SKgs)
               2. State=1
                 /\RCV({ CIDj '. GIj '}_SKgs)=|> State ':=2
% GW's AUTHENTICATION & KEY AGREEMENT PHASE :
                3. State=2
                 /\RCV( CIDi '. MACi '. Di '. T1 ')=|> State ':=3/\ Nj ':=new() /\ Dj ':= xor(H(T1 '. GIj ), Nj ') /\MACj ':=H( GIDj .
                     MACi '. GIj . Nj '. T1 ')
                 /\SND( CIDi '. MACi '. Di '. T1 '. CIDj . Dj ') /\ witness (GW,NS, gw_ns_nj , Nj ')
                4. State=3
                 /\RCV(MACsg '. MACsu '. Ei '. Fi ')=|> State ':=4/\ Np ':= xor( Ei ,H( GIj . T1 ))  /\ Ni ':= xor( Fi ',H( GIj . T1 . GIDj .
                     Nj ))
                 /\ SK ':=H( Ni '. H( Nj . Np ')) /\ secret ({ SK '}, sec5 ,{MU,GW,NS}) /\ Gi ':=H( GIDj . Nj ) /\ Hi ':= xor( Gi ',H( Nj . Np
                     '))
                 /\MAC2j ':=H(MACsu '. SK '. Gi ') /\SND( Hi '. MAC2j ') /\ witness (GW,MU, gw_mu_nj , Hi ')
                 /\ request (MU,GW, mu_gw_ni , Ni ') /\ request (NS,GW, ns_gw_nj ,MACsg ')
end role
```

```
%%% NO.3 %%%  Basic Role : NetworkServer (NS) %%% NO.3 %%%
role networkserver (MU,GW,NS: agent , SKus , SKgs : symmetric_key , H: hash_func , SND,RCV: channel (dy))
played_by NS
def=
    local
        State : nat ,
        IDi , CIDi , CPWi , Ai , UIi , Xi , Yi , Zi , GIDj , Bj , Rj , CIDj , GIj , MACi , Di , T1 , Dj , MACj , SK , SKis , SKns , Nj , Ni , Np , Ei , Fi , MACsg ,
            MACsu , CIDinew , UIinew : text
        const
          sec6 , mu_ns_ui , gw_ns_nj , ns_gw_nj , ns_gw_macj , ns_mu_maci : protocol_id
    init
        State :=0
    transition
% NS REGISTRATION PHASE for MU :
                1. State=0
                 /\RCV({ CIDi '. CPWi '. Ai '}_SKus)=|> State ':=1  /\ SKns ':=new()  /\ UIi ':=H( CIDi '. Ai '. SKns ')
                /\ Xi ':= xor( UIi ',H( CPWi ')) /\ Yi ':=H( UIi '. Xi ') /\ Zi ':=H( UIi '. SKns ') /\SND({ Xi '. Yi '. Zi '}_SKus)

                1. State=0
                 /\RCV({ GIDj '. Bj '}_SKgs)=|> State ':=1
                 /\ Rj ':=new()  /\ CIDj ':=H( GIDj . Bj ) /\ GIj ':=H( CIDj '. H( SKns . Rj ') /\ SND({ CIDj '. GIj '}_SKgs) /\ secret
                     ({ SKns }, sec6 ,{ NS })
% NS's LOGIN & MUTUAL AUTHENTICATION & KEY AGREEMENT PHASE :
                2. State=1
                 /\RCV( CIDi . MACi '. Di '. T1 '. CIDj . Dj '. MACj ')=|> State ':=2
                 /\ Zi ':=h( UIi . SKns ) /\ Ni ':= xor( Di ',H( UIi . T1 '))  /\MACi ':=H( Zi '. Ni '. Di '. GIDj . T1 ) /\ GIj ':=H( CIDj . H(
                     SKns . Rj )) /\ Nj ':= xor( Dj ',H( T1 '. GIj '))
                /\MACj ':=H( GIDj . MACi '. GIj . Nj '. T1 ')  /\ Np ':=new() /\ Ei ':= xor(H( GIj '. T1 '), Np ')  /\ Fi ':= xor(H( GIj '. T1
                    '. GIDj . Nj '), Ni ')
                 /\MACsg ':=H( Ei '. GIj '. T1 '. CIDi . Np ') /\MACsu ':=H( Zi '. UIi . T1 '. CIDi . Ni ')  /\ SK ':=H( Ni '. H( Nj '. Np '))
                     /\ CIDinew ':=H( CIDi . H( Nj '. Np '). Zi ')
                 /\ UIinew ':=H( CIDinew '. Ni '. UIi ) /\ SKis ':=H( Zi '. CIDinew '. UIinew '. T1 ')  /\SND(MACsg '. MACsu '. Ei '. Fi
                     ')
                                /\ witness (NS,GW, ns_gw_nj ,MACsu ') /\ request (GW,NS, gw_ns_nj , Nj ') /\ witness (NS,MU,
                                    ns_mu_maci , UIinew ')
                /\ request (MU,NS, mu_ns_ui , UIi )
end role
```

```
%%%      %%%  Session Role  %%%      %%%
role session(MU,GW,NS:agent,SKus,SKgs:symmetric_key,H,Gen,Rep:hash_func)
def=
    local
                S1,S2,S3,R1,R2,R3:channel(dy)
        composition
                user(MU,GW,NS,SKus,H,Gen,Rep,S1,R1)
                /\gateway(MU,GW,NS,SKgs,H,S2,R2)
                /\networkserver(MU,GW,NS,SKus,SKgs,H,S3,R3)
end role
```

```
role environment()
def=
    const
                mu,gw,ns:agent,
                skus,skgs:symmetric_key,
                h,gen,rep:hash_func,
                idi,pwi,bioi,ai,ri,rj,pbi,cidi,cpwi,xi,yi,zi,li,ni,t1,di,uii,maci,gidj,hi,mac2j,hnjns,gi,sk,
                     skis,skns:text,
                cidinew,uiinew,xinew,yinew,zinew,bj,cidj,gij,nj,dj,macj,macsg,macsu,ei,fi,np:text,
                sec1,sec2,sec3,sec4,sec5,sec6,mu_gw_ni,mu_ns_ui,gw_mu_nj,ns_mu_maci,gw_ns_nj,ns_gw_macj:
                     protocol_id
                intruder_knowledge={mu,gw,ns,h,gen,rep}
        composition
               session(mu,gw,ns,skus,skgs,h,gen,rep)
                /\ session(i,gw,ns,skus,skgs,h,gen,rep)
                /\ session(mu,i,ns,skus,skgs,h,gen,rep)
                /\ session(mu,gw,i,skus,skgs,h,gen,rep)
end role
```

```
%%%      %%%  Goal Section  %%%      %%%
goal
secrecy_of sec1
secrecy_of sec2
secrecy_of sec3
secrecy_of sec4
secrecy_of sec5
secrecy_of sec6
authentication_on mu_gw_ni
authentication_on gw_mu_nj
authentication_on mu_ns_ui
authentication_on ns_mu_maci
authentication_on gw_ns_nj
authentication_on ns_gw_nj
authentication_on ns_gw_macj
end goal
environment()
```

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2023, Volume 21, Number 2 (pp. 1–15)
https://monadi.isc.org.ir

Presented at the ISCISC 2023 in Iranian Research Organization for Science & Technology, Tehran, Iran

A Secure Authentication and Key Agreement Scheme for LoRaWAN★

Zahra Jafari [1], Sahar Palimi [2], Mohammad amin Sabaei [1], Rahman Hajian [1] and Hossein Erfani [*,3]

[1] *Department of IT Engineering, South Tehran Banch, Islamic Azad University, Tehran, Iran*
[2] *Department of Computer Engineering, Yadegar Emam Branch, Islamic Azad University, Tehran, Iran*
[3] *Department of Computer Engineering, South Tehran Banch, Islamic Azad University, Tehran, Iran*

ARTICLE INFO.

Keywords:
LoRaWAN
Security
Mutual Authentication
Key Agreement
AVISPA
BAN

dor: 20.1001.1.24763047.1402.12.2.1.7

Type: Research paper

ABSTRACT

In the Internet of Things (IoT) environment, security and privacy are paramount concerns for critical applications. The LoRa protocol efficiently enables long-range communication for resource-constrained end devices in LoRaWAN networks. To foster technology adoption and user trust, safeguarding the data collected by end devices is essential. Authentication and key agreement protocols play a pivotal role in achieving this goal. Here, we introduce a novel scheme for authentication and key exchange in LoRaWAN, enabling mutual authentication among participants. This scheme empowers users/end devices and network servers to establish secure end-to-end session keys without unconditional trust. We assess the scheme's security informally and provide formal verification using AVISPA tools and the BAN logic. Furthermore, we compare it to existing authentication schemes, demonstrating its efficiency in terms of computational and communication overhead.

★ The ISCISC 2023 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author

Email addresses: ms.zahraajafarii@gamil.com (Zahra Jafari), Sahar.palimii@gmail.com (Sahar Palimi), mohamad.amin.s.sut@gmail.com (Mohammad amin Sabaei), hajian.rh@gmail.com (Rahman Hajian), h_erfani@azad.ac.ir (Hossein Erfani)