مجله کنترل
ISSN (print) 2008-8345
ISSN (online) 2538-3752
مقاله پژوهشی
جلد۱۷، شماره ۴، زمستان ۱۴۰۲، صفحه ۷۳-۶۵

احراز هویت و اعتبارسنجی تلفیقی در شبکه کنتورهای هوشمند

فاطمه رضائی[۱]، پریا رشیدی[۲]

[۱] استادیار، دانشکدهٔ مهندسی کامپیوتر، گروه شبکه‌های کامپیوتری، دانشگاه صنعتی خواجه نصیرالدین طوسی،تهران، ایران frezaei@kntu.ac.ir

[۲] فارغ‌التحصیل کارشناسی ارشد مهندسی کامپیوتر، گروه شبکه‌های کامپیوتری، دانشگاه صنعتی خواجه نصیرالدین طوسی،تهران، ایران rashidyparya@gmail.com

دریافت: ۱۴۰۲/۰۷/۲۲ ویرایش: ۱۴۰۲/۱۰/۰۷ پذیرش: ۱۴۰۲/۱۱/۲۰

چکیده: با وجود گسترش شبکه هوشمند (Smart Grid)، امنیت اطلاعات در این شبکه با چالش‌های زیادی روبرو بوده و نیازمند چارچوب امنیتی قوی برای آن هستیم. در این مقاله، روشی تلفیقی و کارا برای اعتبارسنجی در شبکه کنتورهای هوشمند ارائه می‌شود. در مدل پیشنهادی، ابتدا احراز هویت وسایل مصرفی و حسگری در کنتور هوشمند انجام می‌شود و سپس مقدار زنجیره چکیده تجمعی داده‌های جمع‌آوری شده در کنتور هوشمند محاسبه و به جمع‌کننده ارسال می‌شود. در بخش اول روش پیشنهادی، وسایل مصرفی با استفاده از برچسب‌های شناسایی فرکانس رادیویی (RFID) به کنتور هوشمند متصل می‌شوند تا احرازهویت انجام شود. برای احراز هویت وسایل مصرفی در کنتور هوشمند، از روش خم بیضوی (Elliptic Curve) استفاده می‌کنیم که قابلیت تامین سطح یکسانی از امنیت در مقایسه با سایر روش‌های رمزنگاری کلید همگانی مانند RSA را در ازای طول کلید کوتاه‌تر و هزینه‌های محاسباتی کمتر فراهم می‌کند. در بخش دوم روش پیشنهادی، با محاسبه زنجیره چکیده تجمعی و مقایسه با مقدار دریافتی، اعتبارسنجی پیام‌های دریافتی در جمع‌کننده انجام می‌شود. بنابراین از ارسال داده‌های اضافی به جمع‌کننده، اشغال پهنای باند و امکان نفوذ وسایل مخرب نیز جلوگیری می‌شود. روش پیشنهادی در این مقاله علاوه بر انطباق با ساختار شبکه هوشمند، هزینه محاسباتی و ارتباطی کمتری نیز نسبت به روش‌های موجود فراهم می‌کند.

کلمات کلیدی: احراز هویت، امنیت شبکه، شبکه هوشمند انرژی، کنتورهوشمند، درهم سازی.

Compound authentication in the network of smart meters

Fatemeh Rezaei, Parya Rashidy

Abstract: Despite the expansion of the smart grid, information security in this network has faced many challenges, and we need a strong security framework for it. In this article, a compound and efficient method for authentication in the network of smart meters is presented. In the proposed model, first, the authentication of devices and sensor data is done in the smart meter, and then the value of the cumulative hash chain of the authorized devices' data is calculated in the smart meter and along with the cumulative data is sent to the collector. In the first step of the proposed method, devices are connected to the smart meter using RFID tags, and the device ID is processed in the smart meter. We use the Elliptic Curve method for authentication. In the second step, by calculating the value of the cumulative hash chain and comparing it with the received value, the validation of the received messages is done on the collector. Therefore, sending additional data to the collector, occupying the bandwidth, and the possibility of intrusion of malicious devices are prevented. The proposed method, in addition to adapting to the structure of the smart grid, also provides a lower computational and communication cost than the existing methods.

Keywords: Authentication, network security, smart grid, smart meter, hashing.

[DOI: 10.61186/joc.17.4.65]

۱- مقدمه

پیاده‌سازی شبکه هوشمند راه حلی برای کاهش تقاضای برق، مدیریت کارآمد و بهینه‌سازی استفاده از منابع مدیریتی است. کنتورهای هوشمند دستگاه‌هایی هستند که قادر به نظارت بر مصرف انرژی مصرف-کنندگان برق در زمان واقعی هستند. استفاده از کنتورهای هوشمند می‌تواند عملیات سیستم توزیع برق را تسهیل و خدمات با ارزش افزوده متنوعی را ایجاد کند. از طرفی، داده‌های مصرف انرژی که کنتورها جمع‌آوری می‌کنند، اطلاعات حساس مصرف کننده هستند. بنابراین، حفظ حریم خصوصی و امنیت اطلاعات یک نگرانی کلیدی و بازدارنده اصلی جمع‌آوری داده‌های بلادرنگ در عمل است. برای حفظ حریم خصوصی در شبکه کنتورهای هوشمند باید از روش‌هایی برای ارتقای امنیت شبکه استفاده کنیم. رایانش ابری، اینترنت اشیا و ارتباطات بی‌سیم فناوری‌های بسیار امیدوارکننده‌ای برای پیاده‌سازی شبکه هوشمند هستند، اما خطرات و چالش‌های امنیتی آن‌ها باید به خوبی مورد توجه قرار گیرد و راه حلی برای آن‌ها ارائه شود [۳]-[۱]. از تهدیدات رایج در شبکه هوشمند می‌توان به نفوذ، منع خدمت، بدافزارها، تزریق داده‌های نادرست یا مسمومیت داده اشاره کرد. بنابراین نیازمند چارچوب امنیتی قوی در شبکه هوشمند انرژی هستیم که نه تنها از نفوذ جلوگیری کند، بلکه حریم خصوصی و صحت داده‌های مصرف‌کننده را تضمین کند.

کنتورهای هوشمند با بهره‌گیری از هوش محاسباتی، مصرف توان وسایل را ثبت و به واحد جمع کننده ارسال می‌کنند. با افزایش تعداد کنتورهای هوشمند در شبکه، خواندن موردی این کنتورها دشوار می‌شود. بنابراین از روش تجمیع توزیع‌شده داده‌ها در شبکه هوشمند استفاده می-شود. به این ترتیب که کنتورهای هوشمند داده‌ها را از فرزندان خود جمع-آوری می‌کنند و به گره والد خود در درخت تجمیع ارسال می‌کنند تا در نهایت به واحد جمع‌کننده می‌رسد [۴]. به دلیل این مدل و فرآیند تجمیع و ارسال داده و اهمیت حیاتی اطلاعات در این حوزه، ارائه سازوکارهای امنیت و حفظ حریم خصوصی مختص شبکه کنتورهای هوشمند با در نظر گرفتن این ساختار سلسله مراتبی ضروری است. در این مقاله روشی تلفیقی و کارا برای اعتبارسنجی در شبکه کنتورهای هوشمند ارائه می‌کنیم.

در ادامه این مقاله در بخش دوم پیشینه پژوهش بررسی شده و الگوریتم‌های احرازهویت و درهم‌سازی معرفی می‌شوند. در بخش سوم مدل پیشنهادی احراز هویت و اعتبارسنجی در شبکه کنتورهای هوشمند ارائه می‌شود. بخش چهارم به نتایج شبیه سازی روش پیشنهادی می‌پردازد. در بخش آخر نیز جمع بندی و پیشنهادات آتی ارائه خواهد شد.

۲- پیشینه پژوهش

کنتور هوشمند دستگاهی است که اطلاعات را از وسایل مصرف‌کننده به دست آورده و مصرف انرژی را اندازه‌گیری می‌کند. سپس اطلاعات جمع‌آوری شده را برای نظارت و حسابرسی در اختیار شرکت برق یا اپراتور سیستم قرار می‌دهد. کنتور هوشمند از ارتباطات دو طرفه بین کنتور و سیستم مرکزی پشتیبانی می‌کند و می‌تواند برای نظارت و کنترل وسایل و مدیریت تقاضا و بار در ساختمان‌های هوشمند مورد استفاده قرار گیرد. سیستم‌های کنتور هوشمند از نظر فناوری و طراحی متفاوت هستند اما کارکرد مشابهی دارند. کنتورهای هوشمند داده‌ها را از مصرف‌کنندگان نهایی جمع‌آوری می‌کنند و این داده‌ها را از طریق شبکه محلی به جمع‌کننده داده منتقل می‌کنند. این فرآیند انتقال را می‌توان هر ۱۵ دقیقه یا به ندرت یک‌بار در روز بر حسب نیاز اجرا کرد [۵].

شبکه هوشمند عملکرد شبکه برق را قابل اطمینان‌تر، قابل کنترل و مقرون به صرفه‌تر می‌کند. این شبکه از دستگاه‌های ناهمگنی تشکیل شده‌است که از طریق شبکه‌های عمومی در حال ارتباط هستند و این ارتباطات در معرض حملات سایبری و نقض حریم خصوصی هستند. به عنوان مثال یک مهاجم می‌تواند با تزریق کدهای مخرب، کنتورهای هوشمند را به خطر بیندازد و با تغییر در محتوای حافظه کنتورهای هوشمند، از مزایای مالی بهره‌مند شود. با وجود مزایای شناخته‌شده فناوری شبکه هوشمند و کنتورهای هوشمند، هنوز کاملاً مشخص نیست که تا چه میزان، حملات سایبری می‌تواند عملکرد کنتورهای هوشمند و جمع‌آوری داده-های مصرف برق از مشتری را مختل کند [۶].

۱-۲ احرازهویت در اینترنت اشیا

احرازهویت و اعتبارسنجی، کنترل دسترسی، محرمانه بودن داده‌ها، یکپارچگی داده، عدم انکار و دردسترس بودن از خدمات امنیتی در شبکه هستند. احراز هویت به گیرنده اطمینان می‌دهد که پیام از منبعی دریافت شده است که ادعا می‌کند و تضمین می‌کند که شخص ثالث نتواند به عنوان یکی از دو طرف قانونی به منظور ارسال یا دریافت غیرمجاز خود را معرفی کند. در ادامه به بررسی روش‌های ارائه شده در مقالات برای احراز هویت در اینترنت اشیا [۷] می‌پردازیم.

- احرازهویت به کمک فناوری شناسایی فرکانس رادیویی RFID

فناوری RFID عمدتاً برای شناسایی و ردیابی برچسب‌های متصل به اشیاء استفاده می‌شود و به عنوان یکی از فناوری‌های کلیدی بازار پرسرعت اینترنت اشیا در نظر گرفته می‌شود و انتظار می‌رود ارزش بازار آن از ۱۲,۰۸ میلیارد دلار در سال ۲۰۲۰ به ۱۶,۲۳ میلیارد دلار تا سال ۲۰۲۹ افزایش یابد [۸]. در سال‌های اخیر، فناوری RFID معمولاً در زمینه مراقبت‌های بهداشتی برای کاربردهایی مانند حفاظت از کودک [۹]، نظارت بر موقعیت دارایی‌های پزشکی [۱۰]، نظارت و اعتبارسنجی وضعیت پزشکی [۱۱]، ردیابی بیمار و مدیریت دارو [۱۲]، انتقال خون [۱۳] و مدیریت ایمنی خانه سالمندان [۱۴] استفاده شده است. از آنجایی که داده‌های سلامت جنبه جدایی‌ناپذیر حریم خصوصی شخصی [۱۵] است، حفظ امنیت داده‌های پزشکی خصوصی و تضمین ناشناس بودن و محافظت از ردیابی از دسترسی در طول فرآیند احرازهویت RFID حیاتی است. همچنین در حال حاضر در

[DOI: 10.61186/joc.17.4.65]

بسیاری از برنامه‌های کاربردی دیگر مانند مدیریت هوشمند [۱۶]، کنترل دسترسی ایمن [۱۷]، پرداخت خودکار عوارض [۱۸]، نظارت کارکنان و پیشگیری از سرقت [۱۹] گسترش یافته است.

یک شبکه RFID از یک دستگاه که شامل یک برچسب، یک خواننده و یک پردازشگر پشتیبان است تشکیل شده است که در آن خواننده دارای یک شناسایی خاص است و می‌تواند برای عملیات خواندن یا نوشتن به منطقه کاری برچسب دسترسی داشته باشد. برچسب پس از مقداردهی اولیه با عناصر امنیتی مورد نیاز از سرور داخلی، جزئیات هویت را رمزگذاری کرده و به خواننده منتقل می‌کند. سپس خواننده می‌تواند داده‌های به‌دست‌آمده و شناسه برچسب را با تکیه بر اطلاعات موجود در سرور پشتیبان، چه به صورت آنلاین یا آفلاین، احرازهویت کند. دستگاه RFID بر اساس اینکه آیا دستگاه از برچسب‌هایی با منبع انرژی داخلی استفاده می‌کند یا توسط انرژی توزیع شده توسط خوانندگان RFID به صورت پیوسته کنترل می‌شود، به عنوان غیرفعال یا فعال طبقه بندی می‌شود. زمانی که برچسب RFID در فاصله‌ی نزدیک کنتور هوشمند باشد می‌تواند احرازهویت بین برچسب و کنتور هوشمند انجام شود تا در صورت تأیید، داده‌ها رد و بدل شوند.

روش‌های متداول رمزگذاری سنتی، هزینه دستگاه‌های RFID را به دلیل مصرف انرژی بالا افزایش می‌دهند. از آنجایی که در طراحی سیستم‌های RFID محافظت‌شده کم‌هزینه کاهش اندازه و قابلیت پردازش دارای اهمیت است، به کارگیری روش احرازهویت قابل اعتماد و مقرون‌به‌صرفه برای اطمینان از امنیت اطلاعات کاربر حیاتی است. درگذشته، پروتکل‌های احراز هویتی RFID مبتنی بر توابع درهم‌ساز و رمزنگاری متقارن بودند. در سال‌های اخیر، روش رمزنگاری خم بیضوی به دلیل قابلیت تامین سطح یکسانی از امنیت با سایر روش‌های رمزنگاری کلید همگانی مانند RSA در ازای طول کلید کوتاه‌تر و هزینه‌های محاسباتی کمتر، محبوبیت فزاینده‌ای برای استفاده در شبکه‌های حسگری و اینترنت اشیا یافته است. یک پروتکل احراز هویت مبتنی بر خم بیضوی برای یک شبکه حسگری مجهز به RFID در [۲۰] ارائه شده است که نویسندگان اثبات کرده‌اند که پروتکل پیشنهادی‌شان در مقایسه با کارهای مرتبط از امنیت بیشتری برخوردار است. در بخش ۴، به مقایسه عملکرد روش پیشنهادی خود با این مقاله خواهیم پرداخت.

- احراز هویت با زنجیره چکیده تجمعی

یکی دیگر از روش‌های ارائه شده در مقالات برای احراز هویت در اینترنت اشیا، استفاده از زنجیره چکیده تجمعی است [۲۱]. در این روش، اطلاعات هویتی در گره حسگر به کنترل‌کننده ارسال می‌شود و کنترل-کننده، گره‌های حسگری را احراز هویت می‌کند. در روش ارائه شده در مقاله [۲۱] مطابق شکل ۱، گره حسگر N ابتدا اطلاعاتی را که می‌خواهد به کنترل‌کننده (CRN) ارسال کند، درهم‌سازی می‌کند و یک مقدار چکیده تولید می‌کند مثلاً H_1. سپس H_1 را با دو مقدار دیگر، یعنی کلید مخفی مشترک (TK_N) بین خودش و کنترل‌کننده و مقدار چکیده تجمعی CH_F^x، که x نشان دهنده شماره دنباله یا ترتیب مقادیر است، درهم‌سازی کرده و زنجیره می‌کند. در ادامه، مقدار حاصل را به اطلاعات ضمیمه می‌کند. فرض کنید H_F مرحله قبل در پیامی که به کنترل‌کننده ارسال می‌شود برابر با $H_F = h(H_1, TK_N, {}^x CH_F)$ باشد، در نهایت، مقدار حاصل H_F را دوباره با کلید مخفی مشترک TK_N درهم می‌کند و آن را در پایگاه داده به عنوان یک مقدار جدید به شکل CH_F ذخیره می‌کند. کنترل‌کننده نیز همان روش را برای اطمینان از صحت مقدار چکیده دریافتی پس از دریافت داده اعمال می‌کند. ابتدا، تمام اطلاعاتی که از گره حسگر دریافت شده را درهم‌سازی می‌کند، سپس مقدار چکیده را با دو مقدار دیگر یعنی کلید مخفی مشترک و مقدار چکیده تجمعی قبلی، درهم‌سازی و زنجیره می‌کند.

شایان ذکر است که این روش مقادیر چکیده جلسه را با درهم‌ساز کردن مقدار چکیده جلسه جدید با دو مقدار، یعنی کلید رمزنگاری موقت و مقدار چکیده تجمعی قبلی، به هم زنجیر می‌کند. بنابراین، این روش در ابتدا مانند یک فناوری بلاک‌چین به نظر می‌رسد، اما در واقع به خودی خود از بلاک‌چین استفاده نمی‌کند. می‌توان استدلال کرد که یک مهاجم می‌تواند ورودی‌های زنجیره‌ای اولین مورد را به خطر بیاندازد یا کشف کند، سپس او فقط باید کلید مخفی را برای شکستن این مرحله از پروتکل بداند. با این حال، یافتن کلید مخفی آسان نیست زیرا در هر جلسه تغییر می‌کند. حتی اگر مهاجم کلید مخفی یا اولین درهم‌ساز را بداند، برای او بی فایده است زیرا از یک کلید نشست زودگذر استفاده می‌شود.

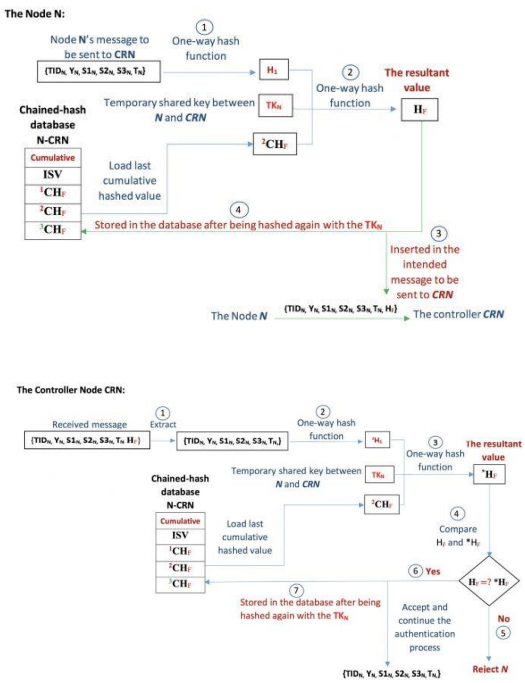
۲-۲ احرازهویت در شبکه هوشمند

همان طور که پیش‌تر گفته شد، کنتورهای هوشمند مصرف توان دستگاه‌های مصرفی را ثبت و به واحد جمع‌کننده ارسال می‌کنند. با افزایش تعداد کنتورهای هوشمند در شبکه، خواندن موردی این کنتورها دشوار می‌شود. بنابراین از روش تجمیع توزیع‌شده داده‌ها در شبکه هوشمند استفاده می‌شود. به این ترتیب که کنتورهای هوشمند داده‌ها را از فرزندان خود جمع آوری می‌کنند و به گره والد خود در درخت تجمیع ارسال می-کنند تا در نهایت به واحد جمع‌کننده می‌رسد. به دلیل این مدل و فرآیند تجمیع و ارسال داده و اهمیت حیاتی اطلاعات این حوزه، سازوکارهای امنیت و حفظ حریم خصوصی مختص شبکه کنتورهای هوشمند با در نظر گرفتن این ساختار سلسله مراتبی ضروری است. با وجود راه‌حل‌های مختلفی که برای امنیت داده در شبکه هوشمند انرژی ارائه شده است، اغلب این روش‌ها بر مبنای سیستم رمزنگاری Paillier [۲۲] هستند که پیچیدگی محاسباتی بالای عملیات آن مناسب کنتورهای هوشمند با منابع محدود نیست [۲۳] و [۲۴]. روش رمزنگاری خم بیضوی به دلیل قابلیت تامین سطح یکسانی از امنیت با سایر روش‌های رمزنگاری کلید همگانی در ازای طول کلید کوتاه‌تر و هزینه محاسباتی کمتر، گزینه مناسبی برای استفاده در شبکه هوشمند است. در [۴]، به کارگیری رمزنگاری خم بیضوی برای تامین محرمانگی اطلاعات در شبکه هوشمند بررسی شده است. در روش ارائه

[DOI: 10.61186/joc.17.4.65]

شده در این مقاله، واحد جمع‌کننده مسئول تولید کلید عمومی و خصوصی است. کلید عمومی تولید شده توسط جمع کننده بین کنتورهای هوشمند در شبکه توزیع می‌شود و کنتورهای هوشمند از این کلید عمومی برای رمزگذاری داده‌های خوانش شده خود استفاده می‌کنند و داده‌های رمزشده را برای واحد جمع‌کننده ارسال می‌کنند. واحد جمع‌کننده هم برای رمزگشایی داده‌های جمع‌آوری شده از کلید خصوصی خود استفاده می‌کند. لازم به تاکید است که مقاله [۴] تنها به محرمانگی داده‌ها از طریق رمزنگاری خم بیضوی در شبکه هوشمند پرداخته و به احراز هویت و اعتبار سنجی پیام های ارسالی نپرداخته است.

در مقاله حاضر، به بحث احراز هویت و اعتبارسنجی در شبکه کنتورهای هوشمند می‌پردازیم. احراز هویت متقابل در کنتور هوشمند به عنوان اولین خط دفاع در برابر حملات، می‌تواند هویت بین کنتورهوشمند و شبکه هوشمند را قبل از انتقال داده تأیید کند و یک رویکرد کارآمد و ایمن برای محافظت از داده‌های کنتور با اجازه دسترسی صرفاً به وسایل احرازهویت شده را فراهم کند.



شکل ۱: ایجاد زنجیره چکیده تجمعی در گره حسگر و کنترل کننده [۲۱]

۳- روش پیشنهادی اعتبارسنجی در شبکه کنتورهای هوشمند

همانطور که ذکر شد، حفظ امنیت و حریم خصوصی چالشی بسیار حیاتی در به‌کارگیری کنتورهای هوشمند است. کنتورهوشمند و ارائه دهنده برق باید قبل از اشتراک‌گذاری اطلاعات مانند مصرف برق، صورتحساب، شارژ خودکار و غیره، به طور متقابل تأیید و احرازهویت شوند، زیرا این اطلاعات برای کاربر محرمانه است. در این بخش روشی تلفیقی و کارا برای اعتبارسنجی در شبکه کنتورهای هوشمند ارائه می‌شود.

۳-۱ مدل پیشنهادی

ارتباط بین کنتورهای هوشمند و جمع‌کننده یک شرط اساسی برای مدیریت مصرف انرژی در بخش مصرف‌کننده است. ارتباط دو طرفه بین کنتور هوشمند و جمع‌کننده از طریق کانال عمومی نا امن، در برابر جعل هویت، قابلیت ردیابی کنتور هوشمند و حملات ضبط فیزیکی کنتور هوشمند آسیب پذیر است. بسیاری از روش‌های موجود نیاز به یک طرح احرازهویت کارآمد و ایمن برای زیرساخت‌های شبکه هوشمند دارند. در مدل پیشنهادی ارائه شده در شکل ۲، ابتدا وسایل مصرفی و حسگری در کنتور هوشمند احرازهویت شده و پس از تأیید، یک روش درهم سازی زنجیره‌ای بر روی داده‌های مصرف‌کننده اعمال شده و سپس به سمت جمع‌کننده ارسال می‌شود. به این ترتیب در مدل پیشنهادی در دو مرحله، ابتدا احراز هویت وسایل مصرفی و حسگری در کنتور هوشمند انجام می‌شود و سپس مقدار زنجیره چکیده تجمعی داده‌های وسایل مجاز در کنتور هوشمند محاسبه می‌شود و به همراه داده‌های دریافتی به سمت جمع‌کننده ارسال می‌شود. در جمع کننده با محاسبه زنجیره چکیده تجمعی و مقایسه با مقدار دریافتی، اعتبارسنجی پیام‌های دریافتی انجام می‌شود و به این صورت صحت و اعتبار داده‌های شبکه هوشمند تأیید می‌شود. در شکل ۲ مراحل روش پیشنهادی نشان داده شده که به شرح زیر است:

۱. احرازهویت وسایل مصرفی مجهز به برچسب RFID با کمک خم بیضوی در کنتور هوشمند: در مرحله نخست، وسایل مصرفی و حسگری با استفاده از برچسب‌های RFID به کنتور هوشمند متصل می‌شوند و اطلاعات را به کنتورهای هوشمند ارسال می‌کنند. در این مرحله شناسه‌ی برچسب وسایل دریافتی در کنتور هوشمند پردازش و احرازهویت انجام می‌شود. در گذشته احراز هویت RFID با توابع درهم ساز و رمزنگاری متقارن انجام می‌شد، اما به دلیل بهبود عملکرد و کاهش طول کلید، استفاده از رمزنگاری خم بیضوی در این مرحله پیشنهاد می‌شود. رمزنگاری خم بیضوی یک طرح سبک وزن برای احرازهویت و حفظ حریم خصوصی در شبکه است که در این مقاله مورد استفاده قرار می‌گیرد.

۲. اعتبارسنجی داده‌ها بین کنتور هوشمند و جمع‌کننده با استفاده از زنجیره چکیده تجمعی: یکی از بخش‌های دیگر روش پیشنهادی برای تضمین اعتبار داده‌های دریافتی استفاده از زنجیره چکیده تجمعی است. همانطور که در شکل ۳ مشاهده می‌شود، در مرحله نخست، وسایل مصرفی در کنتور هوشمند احرازهویت شده و داده‌های وسایل مجاز تجمیع شده و به همراه زنجیره چکیده تجمعی به جمع‌کننده ارسال می‌شوند و جمع‌کننده پس از تأیید اعتبار، داده‌های دریافتی معتبر را ذخیره می‌کند.

به این ترتیب، در روش پیشنهادی یک ساختار سلسله مراتبی و تلفیقی برای احراز هویت و اعتبارسنجی با در نظر گرفتن ویژگی‌ها و الزامات

[DOI: 10.61186/joc.17.4.65]

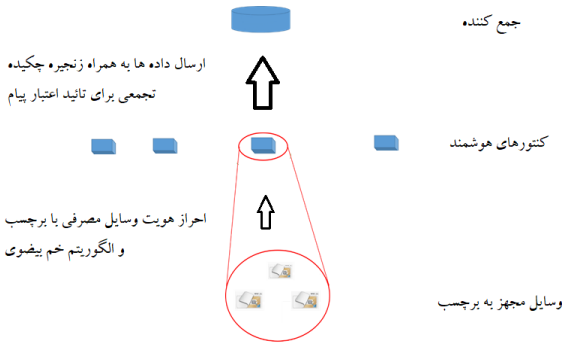
خاص شبکه هوشمند ارائه می‌دهیم. لازم به ذکر است که روش‌های موجود برای احراز هویت در اینترنت اشیا که در بخش قبل مرور شد، همگی از یک ساختار یک سطحی برخوردارند که مناسب معماری شبکه هوشمند انرژی نیستند. به علاوه، روش‌های احرازهویت مبتنی بر برچسب RFID در اینترنت اشیا که در مقالات ارائه شده اند، نیازمند این است که برچسب و خواننده فاصله زیادی با یکدیگر نداشته باشند، بنابراین پیاده سازی عملی این روش‌ها بین وسایل مصرفی و جمع‌کننده مرکزی که فاصله زیادی با هم دارند امکان‌پذیر نیست. اما در روش پیشنهادی، ابتدا وسایل مصرفی با کمک برچسب و الگوریتم خم بیضوی در کنتور هوشمند احرازهویت شده و سپس داده‌های مجاز به صورت تجمعی از کنتور هوشمند به جمع‌کننده ارسال می‌شوند. به این ترتیب، بار کاری جمع‌کننده مرکزی کاهش یابد. بنابراین اگر داده‌ها مربوط به یک وسیله غیرمجاز باشد در همان ابتدا احرازهویت آن در کنتور هوشمند تائید نمی‌شود و دیگر نیازی به ارسال داده به جمع‌کننده نیست. با این کار از ارسال داده‌های اضافی به جمع‌کننده، اشغال پهنای باند و امکان نفوذ وسایل مخرب نیز جلوگیری می‌شود. روش پیشنهادی این مقاله علاوه بر انطباق با ساختار شبکه هوشمند، پیچیدگی کمتری از منظر هزینه محاسباتی و ارتباطی نیز فراهم می کند که در بخش بعد به آن می‌پردازیم. در ادامه این بخش، جزئیات روش پیشنهادی توضیح داده می‌شود.

۲-۳ احرازهویت وسایل مصرفی مجهز به برچسب RFID با کمک خم بیضوی در کنتور هوشمند

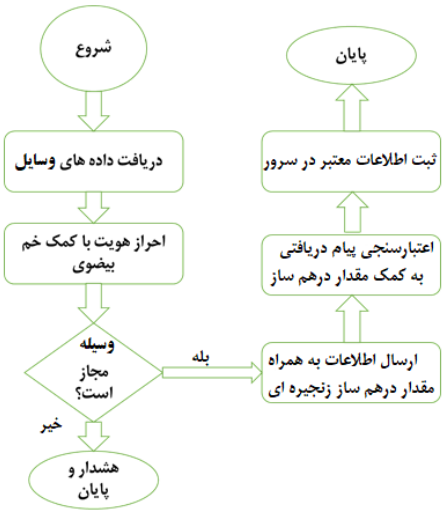
حلقه ابتدایی در بحث احراز هویت در شبکه هوشمند، احرازهویت وسایلی است که به کنتور هوشمند متصل می‌شوند. وسایل مصرفی و حسگری با استفاده از برچسب‌های RFID به کنتور هوشمند متصل می‌شوند و شناسه‌ی کاربران در کنتورهوشمند پردازش می‌شود تا احرازهویت انجام شود. از آنجایی که ارتباط بین برچسب و برچسب خوان در یک محیط باز از طریق سیگنال‌های رادیویی اتفاق می‌افتد، مکانیزمی برای احراز هویت اعتبارسنجی و شناسایی پیام‌ها در هر دو طرف نیاز است. به منظور کاهش هزینه‌ها نباید محاسبات پیچیده‌ای در وسایل انجام شود، از این رو از روش خم بیضوی برای احراز هویت در این مرحله استفاده می کنیم.

زمانی که با برچسب‌های RFID قصد اتصال به کنتور هوشمند و ارسال و دریافت داده را داریم، اطلاعات در فاز اول در زمانی که برای اولین بار از برچسب استفاده می‌شود، با کمک خم بیضوی ثبت می‌شوند و در دفعات بعدی در زمان ارسال اطلاعات ورود از سمت برچسب‌های RFID مجدد با کمک خم بیضوی احرازهویت انجام شده و در صورتی که اطلاعات تایید شود، دریافت و ارسال داده‌ها انجام می‌شود.

امنیت رمزنگاری خم بیضوی به مسئله لگاریتم گسسته خم بیضوی و مسئله دیفی هلمن خم بیضوی متکی است که هر دو در دسته مسائل NP-hard هستند. نمادهای به کار رفته در روش پیشنهادی در جدول ۱ آمده است.



شکل ۲: مدل احراز هویت و اعتبارسنجی پیشنهادی



شکل ۳: مراحل روش پیشنهادی احراز هویت و اعتبارسنجی

یک مجموعه به نام Z_p تشکیل می‌دهیم که عناصر این مجموعه بین 1 تا p-1 است، که این گروه تحت mod p شکل می‌گیرد. خم بیضوی E در Z_p به صورت زیر تعریف می‌شود:

$$y^2 = x^3 + ax + b\,, \qquad (۱)$$

که a , b عضو Z_p هستند و داریم:

$$4a^3 + 27b^2 \neq 0 \mod p. \qquad (۲)$$

$E(Z_p)$ شامل تمام نقاط (x,y) است که x,y عضو Z_p هستند و توسط معادلات بالا به دست می‌آیند.

روش پیشنهادی از دو فاز مقدار دهی اولیه و احراز هویت تشکیل شده‌است. در فاز مقدار دهی اولیه، خم بیضوی E را در Z_p انتخاب می کنیم. یک نقطه P را که عضو $E(Z_p)$ است و از مرتبه‌ی n است پیدا می‌کنیم. ابتدا، خواننده عدد تصادفی s را ایجاد می کند و Y=s.P محاسبه می‌شود،

[DOI: 10.61186/joc.17.4.65]

سپس مقدار s را به عنوان کلید خصوصی خود و Y را به عنوان کلید عمومی خود قرار می‌دهد. سپس کنتور عدد تصادفی d_i را تولید کرده و به عنوان کلید خصوصی برچسب iام تخصیص می‌دهد و به ازای هر برچسب مقدار $ID_i=d_i.P$ را محاسبه می‌کند و بعد مقادیر (P,Y,t_i ,ID_i) را از طریق یک کانال امن بین برچسب‌ها توزیع می‌کند. سپس یک عدد صحیح d را در بازه‌ی [1, n-1] انتخاب کرده و Q= d.P را محاسبه می‌کنیم. کلید خصوصی d و کلید عمومی (E, P, n, Q) است. یک عدد k تصادفی در بازه [1, n-1] تولید می‌کنیم و k.P را محاسبه کرده که یک نقطه به مختصات (x_1,y_1) ایجاد می‌شود.

$$r = x_1 \bmod n. \quad (۳)$$

اگر r صفر بود به مرحله‌ی اول می‌رویم و $۱/k \bmod n$ را حساب می‌کنیم، پس از آن $s = ۱/k\left(H(M)+d.r\right)\bmod n$ را حساب می‌کنیم که h(.) یک تابع درهم ساز است. اگر s=0 بود آنگاه به مرحله اول می‌رویم.

امضای پیام M عبارت است از یک جفت عدد صحیح (r, s). با استفاده از کلید عمومی (E, P, n, Q) می توانیم صحت امضا را تأیید کنیم. می‌دانیم که (r, s) اعداد صحیحی در بازه [1, n-1] هستند. پس از آن روابط زیر را محاسبه می‌کنیم:

$$w = 1/s \bmod n, \quad (۴)$$

$$u_1 = h(M).w \mod n, \quad (۵)$$

$$u_2 = r.w \mod n, \quad (۶)$$

$$u_1.P + u_2.Q = (x_0, y_0), \quad (۷)$$

$$v = x_0 \mod n. \quad (۸)$$

پس از آنکه روابط بالا را به دست آوردیم اگر و فقط اگر v=r بود احرازهویت قابل تایید است. بنابراین اگر داده‌ها مربوط به یک وسیله غیرمجاز باشد در همان ابتدا و زمانی که احرازهویت آن منفی می‌شود، دیگر نیازی به ارسال داده به جمع کننده نیست. با این کار از ارسال داده‌های اضافی به سمت سرور و اشغال پهنای باند جلوگیری می‌شود.

جدول ۱: لیست نمادها

نمادها	توضیحات
P	یک نقطه عضو خم بیضوی $E(Z_p)$
ID_i	شناسه برچسب iام
s	کلیدخصوصی سرویس دهنده
d_i	کلید خصوصی برچسب iام
Y	کلید عمومی سرویس دهنده
h	تابع درهم‌ساز
t_i	مهر زمانی

۳-۳ اعتبارسنجی داده‌ها بین کنتور هوشمند و جمع‌کننده به کمک زنجیره چکیده تجمعی

در این بخش روش پیشنهادی اعتبارسنجی داده‌ها بر اساس زنجیره چکیده تجمعی بین کنتور هوشمند و جمع‌کننده ارائه می‌شود. برای داشتن یک احرازهویت کامل متقابل، یک مکانیسم احرازهویت پاسخ به چالش باید در نظر گرفته شود. در این مقاله، از روش زنجیره چکیده تجمعی [۲۱] که یک روش احرازهویت یک طرفه چالش-پاسخ است استفاده می‌شود. در روش زنجیره چکیده تجمعی، الگوریتم درهم‌سازی مورد استفاده از اهمیت ویژه‌ای برخوردار است. الگوریتم‌های درهم‌سازی ایمن SHA از نوع ۰، ۱و۲ هستند، که الگوریتم SHA-1 دارای سطح ایمنی بالاتری نسبت به SHA-0 است. در مقاله [۲۱] از الگوریتم درهم‌ساز SHA1 برای محاسبه چکیده پیام در زنجیره چکیده تجمعی در خانه هوشمند، استفاده شده که چکیده ۱۶۰ بیتی به عنوان خروجی تولید می‌کند. اما در روش پیشنهادی، بر خلاف مقاله [۲۱]، از الگوریتم درهم ساز SHAKE-128 استفاده می‌کنیم تا روش‌های قبلی را که از SHA-1 و یا SHA-0 استفاده کرده‌اند بهبود دهیم. لازم به ذکر است که الگوریتم SHAKE-128، دارای سرعت ۴۴۵ مبی‌بایت در ثانیه (MiB/s) است که نسبت به SHA-256 سرعت بالاتری دارد و ثابت شده است که SHAKE-128، در برابر حملات تصادم و پیش تصویر اول و دوم مقاومت بیشتری نسبت به الگوریتم‌های مذکور دارد.

٤- ارزیابی عملکرد

در این بخش به ارزیابی عملکرد و هزینه محاسباتی و هزینه ارتباطی طرح پیشنهادی و مقایسه با روش‌های موجود می‌پردازیم. به علت اینکه طرح پیشنهادی از دو بخش در شبکه هوشمند تشکیل شده، هزینه محاسباتی و ارتباطی در هر دو بخش ارائه می‌شود. لازم به ذکر است که در روش پیشنهادی، مشابه مقاله [۲۰] سطح امنیتی ۱۲۸ بیت را در نظر گرفته‌ایم، به این معنی که برای اجتناب از انواع حملات تصادم و پیش-تصویر، طول نقاط خم بیضوی و چکیده پیام را حداقل ۲۵۶ بیت در نظر می‌گیریم.

۴-۱ هزینه محاسباتی

- احرازهویت وسایل مجهز به برچسب RFID با کمک خم بیضوی در کنتور هوشمند

همان طور که پیش‌تر گفته شد، ابتدا وسایل مصرفی و حسگری با استفاده از برچسب‌های RFID به کنتور هوشمند متصل می‌شوند و اطلاعات را به کنتورهای هوشمند ارسال می‌کنند. در این مرحله شناسه‌ی برچسب وسایل دریافتی در کنتور هوشمند پردازش و احرازهویت به کمک خم بیضوی انجام می‌شود. محاسبات در این بخش از شبکه، شامل مجموعه‌ای از عملیات xor، محاسبه چکیده و عملیات خم بیضوی است که از بین آنها، ضرب خم بیضوی بیشترین حجم محاسبات را دارد و در هزینه محاسباتی

[DOI: 10.61186/joc.17.4.65]

کل غالب است. بنابراین تحلیل هزینه محاسباتی در این بخش شبکه را متمرکز به مقدار محاسبات عملیات ضرب خم بیضوی مورد نیاز در وسایل برچسب‌دار و خواننده در کنتور هوشمند می‌کنیم و این مقدار را با T_M نمایش می‌دهیم. طبق نتایجی بررسی شده در [۲۰]، کمترین هزینه محاسباتی در بین روش‌های موجود در این بخش در وسیله مجهز به برچسب، CC_{tag} و خواننده، CC_{reader} برابر $2T_M$ است:

$$CC_{tag} = 2T_M, \quad (۹)$$

$$CC_{reader} = 2T_M. \quad (۱۰)$$

- اعتبارسنجی داده‌ها بین کنتور هوشمند و جمع‌کننده با استفاده از زنجیره چکیده تجمعی

در بخشی از شبکه که از کنتور هوشمند تا جمع‌کننده است، روش زنجیره چکیده تجمعی را به کار برده‌ایم، که از دو نوع عملیات xor و تابع درهم‌ساز یکطرفه تشکیل شده‌است. زمان محاسبه یک عملیات xor را با T_{xor} و زمان محاسبه چکیده را با T_h نمایش می‌دهیم. در روش زنجیره چکیده تجمعی مورد بررسی در کنتور هوشمند، ۵ بار عملیات xor و ۸ بار تابع درهم ساز یکطرفه فراخوانی می‌شود و بنابراین کل هزینه محاسباتی این روش در کنتور هوشمند را اگر با CC_{SM} نمایش دهیم، برابر با مقدار زیر است:

$$CC_{SM} = 8T_h + 5T_{xor}. \quad (۱۱)$$

جمع کننده نیز در روش زنجیره چکیده تجمعی، ۷ بار عملیات xor و ۹ بار تابع درهم ساز یکطرفه را فراخوانی می‌کند و اگر کل هزینه محاسباتی در جمع کننده را با CC_{CLC} نمایش دهیم، برابر با مقدار زیر است:

$$CC_{CLC} = 9T_h + 7T_{xor}. \quad (۱۲)$$

از آنجایی که زمان عملیات xor بسیار ناچیز است، می‌توانیم از آن صرف نظر کنیم و هزینه محاسباتی روش زنجیره چکیده تجمعی را در کنتور هوشمند و جمع کننده به صورت زیر در نظر بگیریم:

$$CC_{SM} \approx 8T_h, \quad (۱۳)$$

$$CC_{CLC} \approx 9T_h. \quad (۱۴)$$

در جدول ۲ به مقایسه هزینه محاسباتی روش پیشنهادی با روش‌های موجود در مقالات می‌پردازیم. تعداد گره‌های حسگری در شبکه تحت پوشش یک کنتور هوشمند را با n_1 و تعداد کنتورهای هوشمند را با n_2 نمایش می‌دهیم، بنابراین تعداد کل گره‌های حسگری در شبکه $n_1.n_2$ خواهد بود. لازم به ذکر است که همان طور که در بخش‌های قبل توضیح داده شد، روش‌های مرتبط احراز هویت در مقالات برای اینترنت اشیا طراحی شده اند و یک سطحی هستند و بنابراین از دو بخش حسگر و جمع‌کننده تشکیل شده‌اند. برای مقایسه پیچیدگی محاسباتی کل این روش‌ها، اگر n_2= n_1= n در نظر بگیریم، همان طور که مشاهده می‌شود پیچیدگی محاسباتی روش‌های موجود از مرتبه $O(n^2)$ است، در حالی که پیچیدگی محاسباتی روش پیشنهادی از مرتبه $O(n)$ خواهد بود.

جدول ۲: مقایسه هزینه محاسباتی روش پیشنهادی با مقالات

روش	هزینه محاسباتی در حسگر	هزینه محاسباتی در کنتور هوشمند	هزینه محاسباتی در جمع کننده
[20]	$2T_M$	NA	$(2T_M)\ n_1.n_2$
[21]	$8T_h$	NA	$(9T_h)\ n_1.n_2$
روش پیشنهادی	$2T_M$	$(2T_M)n_1+8T_h$	$(9T_h)\ n_2$

۲-۴ هزینه ارتباطی

یکی دیگر از معیارهای ارزیابی عملکرد، هزینه ارتباطی است که بیانگر تعداد بیت‌های ارسالی بین گره‌ها برای انجام روش مورد نظر است. در ادامه به مقایسه هزینه ارتباطی روش پیشنهادی و روش‌های موجود در دو بخش شبکه می‌پردازیم.

- از وسایل مجهز به برچسب RFID تا کنتور هوشمند

در این بخش شبکه، دو سمت ارتباط دستگاه برچسب‌دار و خواننده هستند. تعداد بیت‌های ارسالی از وسیله برچسب‌دار به خواننده را با $N_{tag\rightarrow reader}$ و تعداد بیت‌های ارسالی از خواننده به وسیله برچسب‌دار را با $N_{reader\rightarrow tag}$ نمایش می‌دهیم.

برای محاسبه تعداد بیت‌های ارسالی، سطح امنیتی ۱۲۸ بیت در نظر گرفته شده است، به این معنی که برای اجتناب از انواع حملات تصادم و پیش‌تصویر، طول نقاط خم بیضوی و چکیده پیام را حداقل ۲۵۶ بیت قرار داده ایم. به علاوه برای جلوگیری از حملات جستجوی جامع، طول شناسه-ها هم ۱۲۸ بیت در نظر گرفته می‌شود. طبق نتایج بررسی شده در [۲۰]، در بخش وسیله برچسب‌دار تا خواننده، کمترین هزینه ارتباطی با استفاده از روش خم بیضوی به این صورت به دست می‌آید:

$$N_{tag\rightarrow reader} = 768 \text{ bits}, \quad (۱۵)$$

$$N_{reader\rightarrow tag} = 512 \text{ bits}. \quad (۱۶)$$

- از کنتور هوشمند تا جمع کننده

در این بخش شبکه، دو سمت ارتباط کنتور هوشمند و جمع کننده هستند. تعداد بیت‌های ارسالی از کنتور هوشمند به جمع‌کننده را با $N_{SM\rightarrow CLC}$ و تعداد بیت‌های ارسالی از جمع‌کننده به کنتور هوشمند را با $N_{CLC\rightarrow SM}$ نمایش می‌دهیم. در روش زنجیره چکیده تجمعی پیام ارسالی فراسو شامل ۶ مقدار چکیده به طول N_h بیت، یک برچسب زمانی به طول N_T و یک شناسه به طول N_{ID} بیت است. پیام ارسالی فروسو نیز شامل ۲

[DOI: 10.61186/joc.17.4.65]

مقدار چکیده به طول N_h بیت، یک برچسب زمانی به طول N_T و یک شناسه به طول N_{ID} بیت است. همان طو که پیش‌تر گفته شد، در روش پیشنهادی ما برخلاف [۲۱]، برای امنیت بیشتر از الگوریتم درهم ساز SHAKE-128 استفاده شده است که طول چکیده آن N_h=256 بیت است و مقادیر برچسب زمانی N_T=32 بیت و شناسه N_{ID}=16 بیت هستند. بنابراین هزینه ارتباطی روش پیشنهادی ما در این بخش شبکه به این صورت به دست می‌آید:

$$N_{SM\to CLC} = 6N_h + N_T + N_{ID} = 6\times 256 + 32 + 16 = 1584 \text{ bits,} \quad (۱۷)$$

$$N_{CLC\to SM} = 2N_h + N_T + N_{ID} = 2\times 256 + 32 + 16 = 560 \text{ bits.} \quad (۱۸)$$

همان طور که مشاهده می‌شود، مرتبه هزینه ارتباطی روش پیشنهادی نیز در مجموع، کمتر از سایر روش‌های موجود است.

جدو ل ۳: مقایسه هزینه ارتباطی روش پیشنهادی با مقالات

روش‌ها	هزینه ارتباطی در حسگر(بیت)	هزینه ارتباطی در کنتور هوشمند (بیت)	هزینه ارتباطی در جمع کننده (بیت)
[20]	768	NA	512 n_1n_2
[21]	1008	NA	368 n_1n_2
روش پیشنهادی	768	768n_1+ 1584	560 n_2

۵- نتیجه‌گیری

در این مقاله، یک روش احراز هویت و اعتبارسنجی دو سطحی با استفاده از برچسب‌های RFID و الگوریتم خم بیضوی و زنجیره چکیده تجمعی در شبکه کنتورهای هوشمند ارائه شد. در روش پیشنهادی یک طرح جدید احرازهویت و اعتبارسنجی در شبکه کنتورهای هوشمند برای مقابله با حملات امنیتی جعل هویت و دستکاری پیام ارائه کردیم. به این ترتیب کنتور هوشمند، وسایل مصرفی را احرازهویت کرده و داده‌های وسایل مجاز به همراه مقدار زنجیره چکیده تجمعی را برای جمع‌کننده ارسال می‌کند و اعتبارسنجی نهایی پیام‌های دریافتی در جمع‌کننده مرکزی انجام می‌شود. بنابراین از ارسال داده‌های اضافی به جمع‌کننده، اشغال پهنای باند و امکان نفوذ وسایل مخرب نیز جلوگیری می‌شود. روش پیشنهادی در این مقاله علاوه بر انطباق با ساختار شبکه هوشمند، هزینه محاسباتی و ارتباطی کمتری نیز نسبت به روش‌های موجود فراهم می‌کند. به عنوان پیشنهاد برای کارهای آتی می‌توان برای بهبود عملکرد انتقال داده‌های کنتور هوشمند از شبکه‌های نسل پنجم 5G استفاده کرد و برای استفاده از شبکه 5G باید پروتکل‌های امنیتی مورد نیاز را تدوین و ارائه کرد.

مراجع

[1] M. R. Asghar, G. Dan, D. Miorandi, and I. Chlamtac, "Smart Meter Data Privacy: A Survey," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2820-2835, 2017.

[2] G. R. Barai, S. Krishnan, and B. Venkatesh, "Smart metering and functionalities of smart meters in smart grid-a review," IEEE Electrical Power and Energy Conference (EPEC), 2015.

[3] S. Nimbargi, S. Mhaisne, S. Nangare, and M. Sinha, "Review on AMI technology for Smart Meter," 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), 2016.

[4] K. Deepak and K. Chandrasekaran, "Investigating Elliptic Curve Cryptography for Securing Smart Grid Environments", Third ISEA Conference on Security and Privacy (ISEA-ISAP), 2020.

[5] J. Zheng, D. W. Gao, and L. Lin, "Smart Meters in Smart Grid: An Overview," IEEE Green Technologies Conference (GreenTech), 2013.

[6] S. Kumar, H. Kumar, and G. R. Gunnam, "Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack," 2019 2nd International Conference on Data Intelligence and Security (ICDIS), 2019.

[7] A. Albalawi, A. Almrshed, A. Badhib, and S. Alshehri, "A Survey on Authentication Techniques for the Internet of Things", International Conference on Computer and Information Sciences (ICCIS), 2019.

[8] RFID Forecasts, Players and Opportunities, IDTechEx, 2020.

[9] X. Lin, R. Lu, D. Kwan, and X. S. Shen, "REACT: an RFIDbased privacy-preserving children tracking scheme for large amusement parks," Computer Networks, vol. 54, no. 15, pp. 2744-2755, 2010.

[10] D. C. Wyld, "Preventing the "worst case scenario:" combating the lost laptop epidemic with RFID technology," Novel Algorithms and Techniques in Telecommunications and Networking, pp. 29–33, Springer, 2010.

[11] S. W. Wang, W. H. Chen, C. S. Ong, L. Liu, and Y. W. Chuang, "RFID application in hospitals: a case study on a demonstration RFID project in a Taiwan hospital," in Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), 2006.

[12] M. M. Perez, M. Cabrero-Canosa, J. V. Hermida et al., "Application of RFID technology in patient tracking and medication traceability in emergency care," Journal of Medical Systems, vol. 36, no. 6, pp. 3983-3993, 2012.

[13] J. E. Katz and R. E. Rice, "Public views of mobile medical devices and services: a US national survey of consumer sentiments towards RFID healthcare technology," International Journal of Medical Informatics, vol. 78, no. 2, pp. 104-114, 2009.

[14] A. Ohsaga and K. Kondoh, "Bedside medication safety management system using a PDA and RFID tags," in 2013 7th International Symposium on Medical Information and Communication Technology (ISMICT), pp. 85-89, Tokyo, Japan, 2013.

[15] Y. T. Liao, T. L. Chen, T. S. Chen, Z. H. Zhong, and J. H. Hwang, "The application of RFID to healthcare management of nursing house," Wireless Personal Communications, vol. 91, no. 3, pp. 1237–1257, 2016.

[16] K. Fan, W. Jiang, H. Li, and Y. Yang, "Lightweight RFID protocol for medical privacy protection in IoT," IEEE Transactions on Industrial Informatics, vol. 14, pp. 1656-1665, 2018.

[17] S. Anandhi, R. Anitha, and V. Sureshkumar, "IoT enabled RFID authentication and secure object tracking system for smart logistics," Wireless Personal Communications, vol. 104, no. 2, pp. 543–560, 2019.

[18] Y. K. Lee, L. Batina, and I. Verbauwhede, "EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol," in 2008 IEEE international conference on RFID, pp. 97-104, Las Vegas, NV, USA, 2008.

[19] R. Want, "An introduction to RFID technology," IEEE Pervasive Computing, vol. 5, no. 1, pp. 25-33, 2006.

[20] H. Lamrani Alaoui, A. El Ghazi, M. Zbakh, A. Touhafi, and A. Braeken, "A Highly Efficient ECC-Based Authentication Protocol for RFID," Journal of Sensors, 2021.

[21] M. Alshahrani and I. Traore, "Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain," Journal of Information Security and Applications, no. 45, pp.156-175, 2019.

[22] F. Li, B. Luo, and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, pp. 327-332, 2010.

[23] P. Bhanse, B. Mishra, and D. Jena, "A Novel Smart Meter Authentication Scheme for Secure Smart Grid Communication," 2019 IEEE Region 10 Conference (TENCON), 2019.

[24] A. Madhu and P. Prajeesha, "Prevention of FDI Attacks in Smart Meter by providing Multi-Layer Authentication using ElGamal and SHA," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 2021.

[DOI: 10.61186/joc.17.4.65]