دوفصل‌نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)
سال ۱۴۰۱، جلد ۲۰، شماره ۱ (۲۶-۳۶)
https://monadi.isc.org.ir

ارائه‌شده در هجدهمین کنفرانس بین‌المللی انجمن رمز ایران در دانشگاه اصفهان، ۱۰ و ۱۱ شهریور ۱۴۰۰

پروتکل توافق کلید احراز اصالت شده‌ی سبک و امن برای بستر شبکه‌ی هوشمند انرژی★

سید حمید باغستانی* و فرخ‌لقا معظمی

پژوهشکده فضای مجازی دانشگاه شهید بهشتی، تهران، ایران

اطلاعات مقاله

کلمات کلیدی:
احراز اصالت متقابل
توافق کلید
شبکه‌ی هوشمند انرژی
حمله‌ی منع سرویس
به‌روزرسانی

dor: 20.1001.1.24763047.1401.11.1.4.1

نوع مقاله: پژوهشی

چکیده

شبکه‌ی برق سنتی مبتنی بر مصرف سوخت فسیلی است و خسارات زیادی را برای محیط زیست به همراه دارد. شبکه‌ی هوشمند، بستری است که به کمک آن می‌توان منابع تجدیدپذیر را با سیستم توزیع ادغام نمود و همچنین امکان برقراری جریان دوطرفه از انرژی و داده بین مدیران شبکه و مشترکین را در جهت مدیریت بهینه‌ی مصرف انرژی فراهم کرد. با این حال، این جریان داده ممکن است توسط مهاجمین مورد استفاده قرار گیرد و موجب برهم زدن امنیت و عدم تعادل در شبکه شود. بنابراین، نیازمند به‌کارگیری پروتکل‌های امنیتی مختلف در این بستر خواهیم بود. پروتکل توافق کلید احراز اصالت شده، یکی از این پروتکل‌ها است که به کمک آن طرفین ارتباط یکدیگر را شناسایی کرده و یک کلید را برای رمز کردن داده‌ها به اشتراک می‌گذارند. اخیراً ژانگ و همکاران یک پروتکل توافق کلید احراز اصالت شده‌ی سبک مبتنی بر توابع چکیده‌ساز ارائه کردند که در این مقاله، ما پروتکل آن‌ها را مورد بررسی قرار می‌دهیم و نشان خواهیم داد که پروتکل آن‌ها در برابر حمله‌ی منع سرویس آسیب‌پذیر است و همچنین کارایی لازم برای پیاده‌سازی در بستر شبکه‌ی هوشمند را ندارد و در ادامه یک پروتکل سبک و امن، مبتنی بر توابع چکیده‌ساز ارائه می‌دهیم.

© ۱۴۰۱ انجمن رمز ایران

۱ مقدمه

اگر چه تقاضا برای مصرف برق طی صد سال گذشته به طرز چشمگیری افزایش یافته است، اما شبکه‌ی توزیع برق سنتی هیچ تغییر قابل توجهی نکرده است. به دلیل کمبود منابع انرژی سوخت‌های فسیلی و ناکارآمدی شبکه‌ی توزیع انرژی سنتی، مقرون به صرفه نمودن چنین تقاضایی تنها به کمک بهره‌گیری از منابع انرژی تجدیدپذیر و همچنین مدیریت تولید و مصرف انرژی فراهم می‌شود [۲]. این مشکلات باعث ظهور مفهوم شبکه‌ی هوشمند شد که با برقراری یک جریان دوطرفه از انرژی و اطلاعات، نیازمندی‌های مذکور را برآورده می‌کند [۳]. بهره‌گیری از فناوری اطلاعات این امکان را به شبکه اضافه می‌کند تا از منابع انرژی تجدیدپذیر مناسب با توجه به شرایط محیطی استفاده شود و همچنین اطلاعات مفیدی را در اختیار تولیدکنندگان انرژی از وضعیت توزیع بار موجود در شبکه برای مدیریت بهینه‌ی مصرف انرژی قرار داده و این امکان را به مصرف‌کنندگان انرژی می‌دهد تا برخلاف شبکه‌ی سنتی، به طور لحظه‌ای از میزان مصرف خود و هزینه‌های آن مطلع گردند. این امر موجب می‌شود تا مصرف‌کنندگان به دلیل بالا رفتن هزینه‌ها در ساعات اوج مصرف که ممکن است طی فصول و شرایط مختلف به صورت پویا تغییر کند، مصرف برق خود را کاهش دهند [۴].

علی‌رغم تمام فواید ذکر شده، عدم توجه به برقراری صحیح امنیت، می‌تواند خسارات جبران‌ناپذیری به شبکه و همچنین مشترکین وارد نماید که موجب عدم اقبال عمومی شهروندان به این شبکه‌ها خواهد شد. از

★از کمیته علمی هجدهمین کنفرانس بین‌المللی انجمن رمز ایران برای داوری این مقاله تشکر می‌شود.
*نویسنده مسئول
آدرس‌های رایانامه: seyedhamid.baghestani@gmail.com (سید حمید باغستانی)، f_moazemi@sbu.ac.ir (فرخ‌لقا معظمی)
© ۱۴۰۱ تمامی حقوق متعلق به انجمن رمز ایران است.

خطرات ناشی از عدم توجه به برقراری صحیح امنیت می‌توان به نشت حریم خصوصی مشترکین با دستیابی غیرمجاز به اطلاعات میزان مصرف انرژی، اعمال بار مضاعف به شبکه با دستکاری داده‌های مصرفی در ساعات اوج مصرف، ایجاد خاموشی‌های گسترده و ایجاد اختلال در مدیریت و کنترل انرژی و هدر رفتن انرژی اشاره کرد. بنابراین، ارائه‌ی یک پروتکل احراز اصالت مناسب و سپس توافق بر روی یک کلید مشترک برای رمزنگاری داده‌ها بین اجزای مختلف شبکه، از نیازمندی‌های اساسی شبکه‌ی هوشمند است [۵].

در بستر شبکه‌ی هوشمند، کنتور هوشمند، وظیفه‌ی اندازه‌گیری و ارسال اطلاعات مصرفی مشترک را بر عهده دارد که این داده‌ها از طریق زیرساخت اندازه‌گیری هوشمند (AMI [1]) به ارائه‌دهندگان خدمات جهت مدیریت بهینه‌ی شبکه ارسال می‌گردند [۶]. از مهم‌ترین چالش‌هایی که طراحان پروتکل‌های امنیتی در بستر شبکه‌ی هوشمند با آن مواجه هستند، محدود بودن منابع محاسباتی و حافظه به ویژه در سمت کنتور هوشمند است. از این رو طراحان باید در نظر داشته باشند پروتکلی که ارائه می‌دهند علاوه بر برآورده کردن نیازمندی‌های امنیتی تا جای ممکن سبک طراحی شود [۷].

۲ کارهای پیشین

با توجه به نیازهای مطرح شده، تسای و لو پروتکلی مبتنی بر جفت‌های دوسویی [2] ارائه دادند که گمنامی [3] کنتورهای هوشمند را برآورده می‌کند [۸]. اما به دلیل بالا بودن هزینه‌ی محاسباتی جفت‌های دوسویی، برای پیاده‌سازی بر روی بستر شبکه‌ی هوشمند انرژی با منابع محدود، مناسب نیست و از آنجایی که طرح در مدل مهاجم CK [4] [۹] امن نبود، اودلو و همکاران مقاله‌ای [۱۰] به کمک خواص جفت‌های دوسویی ارائه دادند که در آن ابتدا نشان داده شد، طرح مقاله‌ی [۸] در مدل مهاجم CK آسیب‌پذیر بوده و با نشت مقدار تصادفی، کلید نشست به راحتی قابل محاسبه است. به دلیل استفاده از توابع جفت‌های دوسویی، این طرح نیز برای پیاده‌سازی بر روی بستر شبکه‌ی هوشمند مناسب نبود.

با توجه به بار سنگین جفت‌های دوسویی خلید محمود و همکاران یك طرح توافق کلید به کمک خم‌های بیضوی ارائه دادند [۱۱]. در طرح ارائه شده گمنامی کنتورهای هوشمند در نظر گرفته نشده است و شناسه‌ی طرفین ارتباط به‌راحتی توسط مهاجم قابل دسترسی است. عباسی نژاد و نیکوقدم [۱۲] نشان دادند که طرح مقاله‌ی [۱۱] در مدل مهاجم CK امن نیست و با نشت مقدار تصادفی، کلید نشست آشکار می‌شود؛ اما در طرح آن‌ها [۱۲] نیز راهکاری برای گمنامی تجهیزات در نظر گرفته نشده است.

وزید و همکاران، یک پروتکل احراز اصالت کاربر سه عاملی را ارائه دادند [۱۳] که از استخراج فازی [5] و ویژگی‌های بیومتریک برای احراز اصالت بهره می‌گیرد. همچنین طرح آن‌ها از اضافه شدن پویا و گمنامی کنتورهای هوشمند پشتیبانی می‌کند. نراج کومار و همکاران یک پروتکل احراز اصالت و توافق کلید مبتنی بر خم بیضوی در بستر شبکه‌ی هوشمند بین کنتور هوشمند و ارائه دهنده‌ی خدمات طراحی کرده‌اند [۱۴]. ما در مقاله‌ی [۱]، نشان دادیم، در طرح آن‌ها [۱۴]، ارائه دهنده‌ی خدمات در گام دوم، هیچ‌گونه بررسی بر روی صحت داده‌های دریافتی انجام نمی‌دهد و این امر امکان اعمال بار محاسباتی سنگین از طرف مهاجم را در پی خواهد داشت.

پاردپ کومار و همکاران یک طرح احراز اصالت دوطرفه ارائه کردند [۱۵] که در این طرح، دروازه‌ی NAN [6] به‌عنوان یک نهاد قابل اعتماد، وظیفه‌ی ثبت کنتورها و اختصاص پارامترهای خصوصی آن‌ها را نیز بر عهده دارد. در این طرح که مبتنی بر خم بیضوی است از رمزنگاری متقارن AES و همچنین از MAC نیز استفاده شده است. این ناهمگون بودن توابع رمزنگاری باعث می‌شود که حجم حافظه‌ی زیادی برای پیاده‌سازی توابع اشغال شود. همچنین، ما در مقاله‌ی [۱] عنوان کردیم، برخلاف ادعای طراحان، طرح ارائه شده به‌خوبی گمنامی را برآورده نمی‌کند و با توجه به آشکار بودن شناسه‌ی NAN برای کنتورهای عضو در شبکه، یک کنتور خرابکار می‌تواند سایر کنتورهای هوشمند را ردگیری کرده و تشخیص دهد آیا دو جلسه متعلق به یک کنتور هوشمند است یا خیر.

اصفهانی و همکاران طرح احراز اصالت و توافق کلید به کمک توابع چکیده‌ساز برای محیط اینترنت اشیا ارائه دادند [۱۶]. در طرح آن‌ها، میان پیام‌هایی که رد و بدل می‌شود، پیامی وجود دارد که در هر نشست مربوط به یک حسگر هوشمند خاص، ثابت است. با توجه به این که این پیام داده‌ی منحصربه‌فردی است که در مرحله‌ی ثبت نام، TA [7] در اختیار حسگر می‌گذارد، امکان ردگیری [8] حسگر هوشمند را به دشمن می‌دهد. ژانگ و همکاران با الهام گرفتن از طرح [۱۶]، پروتکل احراز اصالت و توافق کلیدی مبتنی بر توابع چکیده‌ساز و رمزنگاری متقارن برای شبکه‌های هوشمند ارائه دادند [۱۷] که با به‌روز کردن داده‌های منحصربه‌فرد و ثابت در پایان نشست، مشکل ردگیری کنتورها را رفع کردند. با این حال، ما دریافتیم، پروتکل آن‌ها در برابر حمله‌ی منع سرویس [9] آسیب‌پذیر است و همچنین برای جلوگیری از حمله‌ی ناهمگام‌سازی [10]، نیازمند ذخیره‌ی اطلاعات قبلی به ازای هر کنتور است که این امر با توجه به گسترش شبکه و افزایش کنتورهای هوشمند، موجب ایجاد سربار داده و عدم مقیاس‌پذیری شبکه خواهد شد. همچنین این طرح به گونه‌ای است که هر دو طرف پروتکل نیاز به به‌روزرسانی و ذخیره‌ی داده‌های ثابت به صورت متقابل دارند که این امر راه را برای اعمال حمله‌ی ناهمگام‌سازی باز می‌گذارد.

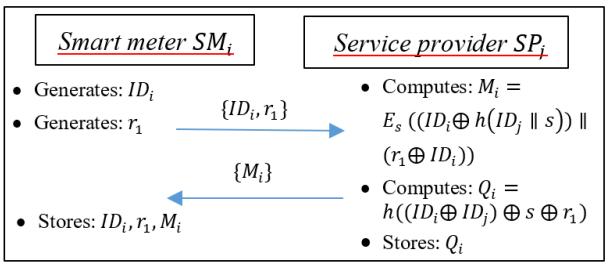
لی و همکاران طرحی برای بستر شبکه‌ی بی‌سیم ارائه دادند [۱۸] که در آن فقط طرف اول پروتکل نیاز به ذخیره‌ی مقادیر ثابت به‌روز شده دارد. در این روش به‌روزرسانی، مسئله‌ی ناهمگام‌سازی مطرح نخواهد بود.

[1] Advanced Metering Infrastructure [2] bilinear paring [3] anonymity
[4] CK-adversary [5] fuzzy extraction

[6] Neighbor Area Network [7] Trusted Authority [8] tracking [9] denial of service
[10] de-synchronization

جدول ۱. نمادها

نمادها	توضیحات
SP_j	jامین ارائه دهنده‌ی خدمات
SM_i	iامین کنتور هوشمند
ID_j	شناسه‌ی jامین ارائه دهنده‌ی خدمات
ID_i	شناسه‌ی i امین کنتور هوشمند
s	کلید اصلی ارائه دهنده‌ی خدمات
K	کلید رمزنگاری متقارن
$E_K[ms]$	عمل رمزگذاری با کلید K
$D_K[ms]$	عمل رمزگشایی با کلید K
$r_۱, r_۲, r_۳$	اعداد تصادفی
$H(\cdot), MAC$	تابع چکیده‌ساز یک‌طرفه و کد احراز اصالت پیام



شکل ۱. مرحله‌ی ثبت نام

۳ مروری بر طرح ژانگ و همکاران

طرح ژانگ و همکاران [۱۷] شامل دو مرحله است. ۱) مرحله‌ی ثبت نام که به کمک یک کانال امن انجام می‌شود. ۲) مرحله‌ی احراز اصالت و توافق کلید. نمادهای طرح در جدول ۱ نشان داده شده است.

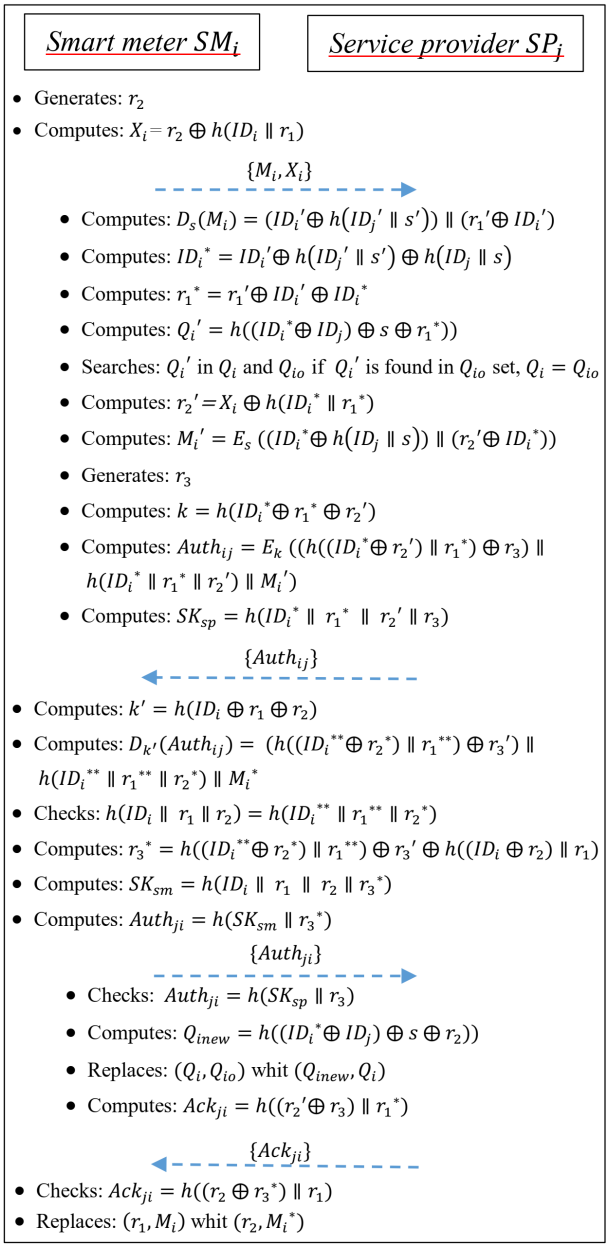
۱.۳ مرحله‌ی ثبت نام

روند مرحله‌ی ثبت نام در این طرح مطابق شکل ۱ است.

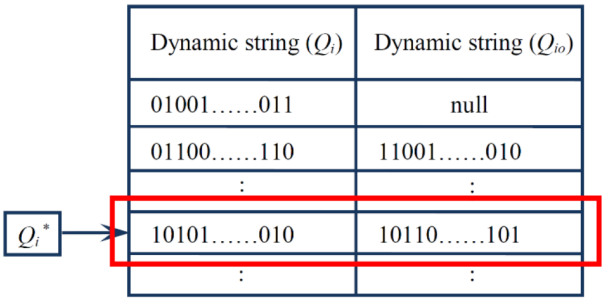
۲.۳ مرحله‌ی احراز اصالت و توافق کلید

روند مرحله‌ی احراز اصالت و توافق کلید در این طرح مطابق شکل ۲ است.

مطابق با شکل ۲، ارائه دهنده‌ی خدمات مقدار Q_i را محاسبه می‌کند و طبق شکل ۳ با مقادیر فعلی و قبلی که در پایگاه داده‌ی خود به ازای هر کنتور ذخیره دارد مقایسه می‌کند، اگر با هیچ یک تطابق نداشته باشد جلسه را خاتمه می‌دهد.



شکل ۲. مرحله‌ی احراز اصالت و توافق کلید



شکل ۳. تأیید پویا

۴ تحلیل طرح ژانگ و همکاران

۱.۴ حمله‌ی منع سرویس

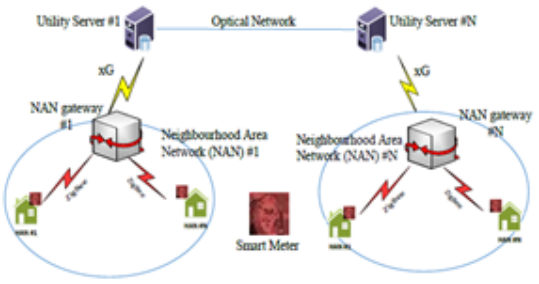
در این حمله، مهاجم پیام‌های معتبر M_i و X_i از یک کنتور مجاز را شنود کرده و به طور مکرر به طرف ارائه دهندگان خدمات ارسال می‌کند. ارائه دهندگان خدمات تمام پیام‌های دریافتی را به دلیل عدم بهره‌گیری و دخالت مهر زمانی در آن‌ها معتبر دانسته و به ازای هر جفت پیام M_i و X_i، محاسبات را تا محاسبه‌ی کلید جلسه SK_{sp} و پیام $Auth_{ji}$ ادامه می‌دهد و حتی پیام $Auth_{ji}$ را روی کانال ارسال می‌کند. بنابراین مهاجم یا مهاجمین قادر خواهند بود با ارسال مکرر پیام‌های معتبر از یک کنتور یا کنتورهای مختلف که شنود کرده‌اند، موجب به‌کارگیری منابع محاسباتی ارائه دهندگان خدمات و همچنین اشغال کانال ارتباطی گردند. به گونه‌ای که امکان ارائه‌ی صحیح خدمات به کنتورهای مجاز ممکن نباشد یا به کندی انجام شود. این در حالی است که بستر شبکه‌ی هوشمند به خودی خود نیازمند همزمان شدن طرفین ارتباط است، بنابراین قابلیت همگام شدن زمانی و بهره‌گیری از مهر زمانی را به خوبی دارا است و به راحتی می‌توان از بروز چنین حملات خسارت باری جلوگیری کرد.

۲.۴ ضعف به‌روزرسانی مقادیر ثابت

در این طرح، برای از بین بردن ارتباط بین نشست‌های مختلف، لازم است مقادیر ثابت M_i و Q_i پایان هر نشست به‌روز شوند. این به‌روزرسانی به گونه‌ای است که کنتور iام برای شرکت در نشست بعدی به مقدار به‌روز شده‌ی M_i احتیاج داشته و ارائه دهنده‌ی خدمات نیز به طور متقابل برای تائید اعتبار کنتور مورد نظر در نشست بعدی، نیاز به ذخیره‌ی مقدار به‌روز شده‌ی Q_i دارد. این نوع به‌روزرسانی دست مهاجم را برای اعمال حمله‌ی ناهمگام‌سازی به گونه‌ای که طرفین پروتکل دیگر قادر به برقراری ارتباط نباشند، باز می‌گذارد. در این طرح، برای جلوگیری از چنین حمله‌ای ارائه دهنده‌ی خدمات به ازای هر کنتور، مقدار قبلی Q_i و مقدار به‌روز شده‌ی آن را در پایان هر نشست مطابق با شکل ۳ ذخیره می‌کند تا بتواند در صورت بروز حمله‌ی ناهمگام‌سازی، از مقدار قبلی Q_i برای جلوگیری از قطع ارتباط استفاده کند. این روش کارایی طرح را از نظر مقیاس‌پذیری با توجه به افزایش روزافزون کنتورهای هوشمند در شبکه‌ی هوشمند انرژی پایین می‌آورد.

۵ طرح پیشنهادی

در این قسمت، ما یک پروتکل توافق کلید احراز اصالت شده‌ی سبک و امن مبتنی بر توابع چکیده‌ساز بین کنتور هوشمند و شبکه‌ی همسایگی NAN ارائه می‌دهیم، به گونه‌ای که مشکلات امنیتی و ضعف‌های ارائه شده در بخش قبل را نداشته باشد و از منظر کارایی نیز از طرح [۱۷] و مابقی طرح‌ها سبک‌تر باشد. طرح ارائه شده، شامل دو مرحله‌ی ثبت نام و مرحله‌ی احراز اصالت و توافق کلید است و نمادهای طرح مطابق با جدول ۱ تنظیم شده است.



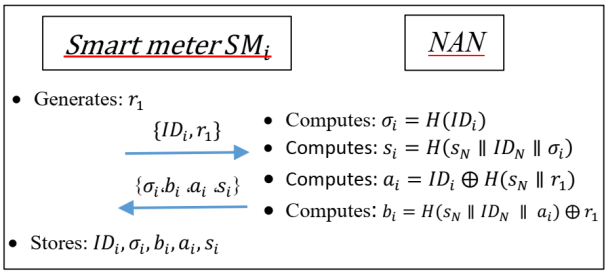
شکل ۴. زیرساخت اندازه‌گیری هوشمند [۱۴]

۱.۵ مدل شبکه

در زیرساخت اندازه‌گیری هوشمند (AMI) مطابق با شکل ۴ ارسال اطلاعات از کنتورهای هوشمند تا ارائه‌دهندگان خدمات دارای لایه‌های مختلفی است. در لایه‌ی میانی، شبکه‌ی همسایگی NAN قرار دارد که از تمامی شبکه‌های کوچک خانگی تشکیل شده و مانند یك تجمیع کننده‌ی شبکه، تمامی داده‌ها را به لایه‌ی بالاتر ارسال می‌کند. در بالاترین لایه نیز شبکه‌ی گسترده‌ی (WAN) قرارگرفته است که شبکه‌های NAN را به هم ارتباط می‌دهد. تمامی اطلاعات تجمیع شده توسط NAN از طریق لایه‌ی WAN به سطوح مدیریتی و ارائه دهندگان خدمات منتقل می‌شوند. بنابراین در این زیرساخت هر کنتور تنها با یک شبکه‌ی همسایه در ارتباط است و این فرض که شبکه‌ی همسایگی NAN نقش نهاد قابل اعتماد را نیز بازی کند و هر کنتور خود را در NAN مربوط به خود ثبت نام کند، فرضی عملی خواهد بود؛ اما در طرح ژانگ و همکاران [۱۷] این ارتباط مستقیم بین کنتور هوشمند و ارائه دهندگان خدمات در نظر گرفته شده و با این وجود، فرض شده است که ارائه دهندگان خدمات وظیفه‌ی یک نهاد قابل اعتماد را نیز بر عهده دارند. این فرض به این معنی است که هر کنتور برای ارتباط با هر یک از ارائه دهندگان خدمات، نیاز به ثبت نام در ارائه دهنده‌ی خدمات مربوطه را داشته که با توجه به نیاز مرحله‌ی ثبت نام به یک کانال ارتباطی امن، انتقال داده در چنین مدلی بسیار هزینه‌بردار است.

۲.۵ مدل حمله

در این طرح، مطابق طرح ژانگ فرض می‌کنیم که یک مهاجم مانند مدل Dolve-Yao [۱۹] می‌تواند کانال‌های بی‌سیم دوطرفه را استراق سمع و ردگیری کند. یک مهاجم می‌تواند سعی کند پیام‌های قدیمی را دوباره به SM یا دروازه‌ی NAN پخش کند. مهاجم می‌تواند برای تزریق پیام‌های جدید و جعل پیام برای اهداف خاص خود تلاش کند. همچنین مهاجم می‌تواند کلید یک نشست را در اختیار داشته باشد. به علاوه پروتکل به گونه‌ای طراحی شده است که با دستیابی مهاجم به اعداد تصادفی، هیچ یک از مقادیر حساس نشست و پارامترهای خصوصی موجود در حافظه‌ی طرفین برای مهاجم آشکار نمی‌شود و طرح در برابر نشت راز موقت مقاوم است.



شکل ۵. مرحله‌ی ثبت نام طرح پیشنهادی

۳.۵ مرحله‌ی ثبت نام

کنتورهای هوشمند باید ابتدا به کمک کانال امن، در دروازه‌ی NAN ثبت شوند. روند مرحله‌ی ثبت نام مطابق شکل ۵ به شرح زیر است:

هر کنتور هوشمند (به عنوان مثال i)، یک شناسه‌ی مخفی (ID_i) را انتخاب کرده و به همراه یک عدد تصادفی r_1 به سمت دروازه‌ی NAN مورد نظر ارسال می‌کند. NAN از شناسه‌ی مخفی ID_i برای محاسبه‌ی $\sigma_i = H(ID_i)$ استفاده می‌کند. سپس از کلید اصلی خود یعنی s_N برای محاسبه‌ی کلید خصوصی مربوط به کنتور هوشمند، یعنی $s_i = H(s_N \| ID_N \| \sigma_i)$ استفاده می‌کند و همچنین در گام آخر، مقادیر $a_i = ID_i \oplus H(s_N \| r_1)$ و $b_i = H(s_N \| ID_N \| a_i) \oplus r_1$ را محاسبه کرده و پارامترهای امنیتی $\{s_i, a_i, b_i, \sigma_i\}$ را از طریق کانال امن برای SM ارسال می‌کند تا در حافظه‌ی خود ذخیره کند. در این طرح، دروازه‌ی NAN به ازای هر کنتور، تنها شناسه‌ی آن کنتور (به عنوان مثال ID_i) را در حافظه‌ی خود ذخیره می‌کند.

۴.۵ مرحله‌ی احراز اصالت و توافق کلید

روند مرحله‌ی احراز اصالت و توافق کلید مطابق با شکل ۶ به شرح زیر است:

گام اول: کنتور هوشمند SM، عدد تصادفی r_2 را تولید کرده و $B_i = r_2 \oplus s_i$ را محاسبه می‌کند. سپس کلید $L = H(ID_i \| B_i \| T_1)$ را حساب کرده که T_1 مهر زمانی SM است و در ادامه، $c_i = \sigma_i \oplus r_2$ را محاسبه می‌کند و پیام شروع را به NAN ارسال می‌کند که شامل $\{a_i, b_i, c_i, L, T_1\}$ است.

گام دوم: دروازه‌ی NAN بعد از دریافت پیام شروع از جانب کنتور هوشمند، ابتدا صحت مهر زمانی را بررسی می‌کند و سپس عدد تصادفی $r_1^* = H(s_N \| ID_N \| a_i) \oplus b_i$ را حساب کرده و به کمک r_1^*، و کلید اصلی خود یعنی s_N، مقدار $ID_i^* = H(s_N \| r_1^*) \oplus a_i$ را به دست می‌آورد. سپس تساوی $ID_i^* = ID_i$ را با شناسه‌ای که از SM در مرحله‌ی ثبت، ذخیره کرده است، بررسی می‌کند. اگر برقرار بود، نشست را ادامه می‌دهد و مقدار $\sigma_i' = H(ID_i)$ را محاسبه کرده و مقدار r_2، که عدد تصادفی انتخابی توسط SM در گام اول است را به کمک رابطه‌ی $r_2 = c_i \oplus \sigma_i'$ به دست می‌آورد. سپس مقادیر $B_i' = H(s_N \| ID_N \| \sigma_i) \oplus r_2$ و $L' = H(ID_i \| B_i' \| T_1)$ را حساب می‌کند و صحت تساوی $L' = L$ را بررسی می‌کند، اگر تأیید نشود، درخواست را متوقف می‌کند. در غیر این صورت، مقدار تصادفی r_3 را تولید کرده و مقادیر $\theta = \sigma_i \oplus r_3$، $\omega = r_3 \oplus ID_i \oplus B_i$ و $\omega' = r_2 \oplus \sigma_i \oplus B_i$ را محاسبه می‌کند. سپس با جایگزین کردن r_2 با r_1 مقادیر a_i و b_i را مطابق با روابط $a_i^+ = ID_i \oplus H(s_N \| r_2)$ و $b_i^+ = H(s_N \| ID_N \| a_i^+) \oplus r_2$ به‌روز می‌کند و مقادیر $\eta = \omega \oplus a_i^+$ و $\mu = \omega' \oplus b_i^+$ را محاسبه می‌کند تا SM بتواند به کمک آن‌ها مقادیر به‌روزشده‌ی a_i^+ و b_i^+ را به دست آورد. لازم به ذکر است، دروازه‌ی NAN هیچ نیازی به ذخیره‌ی a_i^+ و b_i^+ ندارد. سرانجام کلید $SK = H(ID_i \| B_i \| r_2 \| r_3 \| \eta \| \mu)$ را حساب کرده و به کمک آن $Y = H(SK \| ID_i \| r_3)$ را حساب می‌کند و پیام پاسخ $\{\theta, \eta, \mu, Y\}$ را برای SM ارسال می‌کند.

گام سوم: SM، مقدار r_3، که عدد تصادفی انتخابی توسط NAN در گام دوم است را طبق تساوی $r_3^* = \sigma_j \oplus \theta$ به دست می‌آورد و به کمک آن کلید نشست $SK' = H(ID_i \| B_i \| r_2 \| r_3^* \| \eta \| \mu)$ و سپس مقدار $Y' = H(SK' \| ID_i \| r_3^*)$ را محاسبه کرده و $Y' = Y$ را بررسی می‌کند، اگر تساوی برقرار باشد، $\omega = r_3 \oplus ID_i \oplus B_i$ و $\omega' = r_2 \oplus \sigma_i \oplus B_i$ را محاسبه می‌کند و $a_i^+ = \omega \oplus \eta$ و $b_i^+ = \omega' \oplus \mu$ را به دست آورده و در انتها مقادیر (a_i, b_i) را با (a_i^+, b_i^+) جایگزین می‌کند.

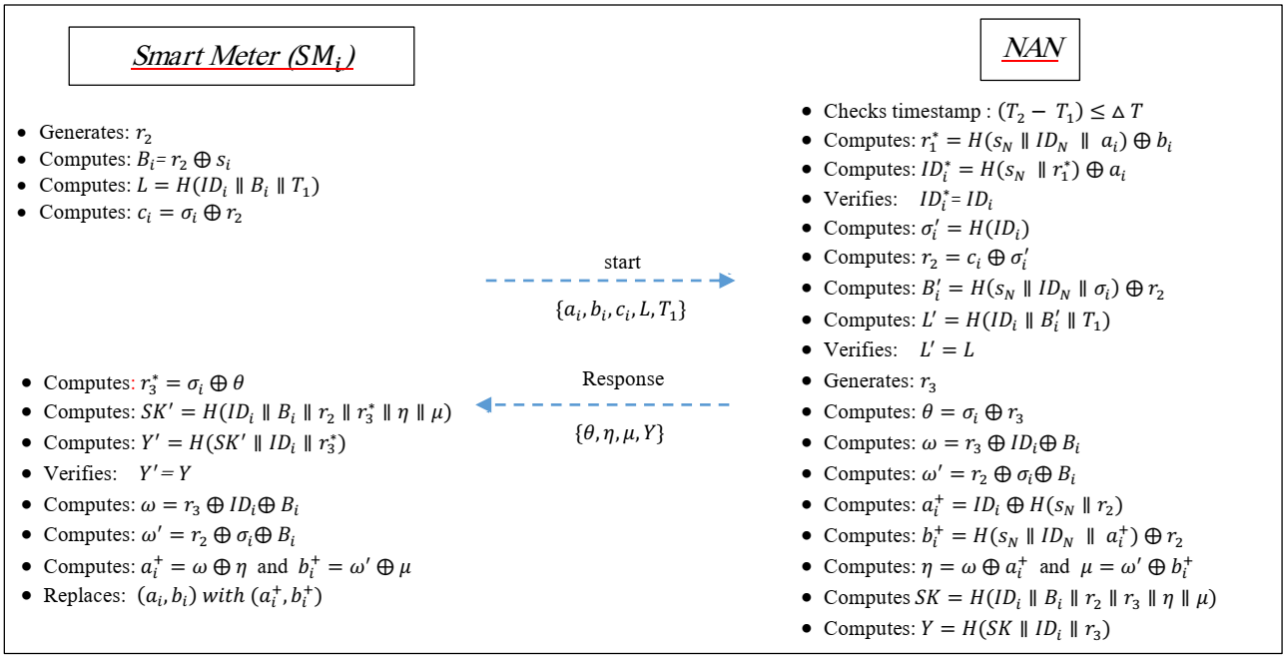
۶ تحلیل امنیتی غیررسمی

در این بخش، امنیت طرح پیشنهادی مورد بررسی قرار گرفته است و در جدول ۴، مقایسه‌ی طرح پیشنهادی از منظر برآورده شدن نیازمندی‌های امنیتی، با طرح‌های اخیراً ارائه شده در بستر شبکه‌ی هوشمند، نشان داده شده است.

حمله‌ی تکرار[1]: در طرح ارائه شده، تمام پیام‌های رد و بدل شده در هر نشست، به علت بهره‌گیری از مهر زمانی و مقادیر تصادفی با سایر نشست‌ها متفاوت هستند. با توجه به اینکه در طرح ارائه شده، علاوه بر استفاده از مهر زمانی، هر طرف پروتکل مقدار تصادفی به کار رفته توسط طرف مقابل را به دست می‌آورد و از آن استفاده می‌کند، در نتیجه، بازپخش پیام‌های قدیمی موجب عدم تصدیق طرف مقابل خواهد شد.

حمله‌ی فرد در میانه[2]: در این نوع حمله، مهاجم بر سر راه ارتباط طرفین پروتکل قرار گرفته و با تغییر و ارسال پیام‌ها، قصد خرابکاری و بر هم زدن روال عادی پروتکل را دارد. فرض کنید مهاجم در گام اول بخواهد پیام L را تغییر دهد. این کار برای مهاجم مفید نیست، زیرا L یک تابع چکیده‌ساز است که شامل B_i است و B_i به کمک کلید خصوصی کنتور، یعنی s_i محاسبه می‌شود که برای مهاجم شناخته نشده است. همچنین مهاجم قادر به ایجاد تغییر در هیچ کدام از پیام‌های $\{a_i, b_i\}$ نیست،

[1] replay attack [2] Man-in-the-middle attack (MITM)



شکل ۶. مرحله‌ی احراز اصالت و توافق کلید طرح پیشنهادی

زیرا طرف دوم پروتکل یعنی NAN به کمک این مقادیر و محاسبه‌ی عدد تصادفی r_1 که توسط کنتور در مرحله‌ی ثبت نام تولید شده است و کلید اصلی خود یعنی s_N، شناسه‌ی مخفی طرف اول را به دست می‌آورد و شناسه‌ی به دست آمده را با پایگاه داده‌ای که از شناسه‌های مجاز دارد، مقایسه می‌کند و در صورت عدم برقراری تساوی $ID_i^* = ID_i$ پروتکل را خاتمه می‌دهد. همچنین اگر مهاجم قصد تغییر در پیام c_i را داشته باشد، دروازه‌ی NAN عدد تصادفی r_2 را اشتباه محاسبه کرده و این باعث عدم برقراری تساوی $L' = L$ خواهد شد. همچنین اگر مهاجم قصد تغییر در مهر زمانی را داشته باشد، حتی اگر مهر زمانی جعلی در بازه‌ی مجاز قرارگرفته باشد و شرط $(T_2 - T_1) \leq \Delta T$ را احراز کند، با توجه به قرار داشتن مقدار مهر زمانی در تابع چکیده‌ساز L، تساوی $L' = L$ برقرار نخواهد شد. به طور مشابه، تغییر در هر یک از پیام‌های ارسالی از طرف دروازه‌ی NAN مانند θ، η، μ، Y نیز موجب عدم برقراری تساوی $Y' = Y$ خواهد شد.

حمله‌ی جعل هویت[1]: در این حمله، مهاجم تلاش می‌کند با جعل هویت یکی از طرفین به جای آن با طرف مقابل داده رد و بدل کند. در این طرح، مهاجم بدون در اختیار داشتن ID_i قادر به ارسال پیام Lای به طرف NAN نخواهد بود به گونه‌ای که $L' = L$ شود؛ زیرا پیام L با مقادیر ID_i و مهر زمانی T_1 درآمیخته شده است و تنها دروازه‌ی NAN قادر خواهد بود به کمک کلید اصلی خود یعنی s_N و مقادیر a_i و b_i که توسط کنتور iام ارسال می‌شود، شناسه‌ی کنتور ID_i را محاسبه کند و همچنین شناسه‌ی به دست آمده را با شناسه‌ی ذخیره شده در پایگاه داده‌ی خود تطابق دهد. به علاوه اگر فرض کنیم مهاجم به هر نحوی به شناسه‌ی مخفی کنتور هوشمند دسترسی داشته باشد، بدون در اختیار داشتن کلید خصوصی s_i و عدد تصادفی r_2، قادر به محاسبه‌ی B_i به گونه‌ای نیست که تساوی $L' = L$ برقرار شود. به طور مشابه، مهاجم قادر نخواهد بود به‌عنوان یک دروازه‌ی قانونی NAN بدون در اختیار داشتن کلید اصلی s_N و شناسه‌ی ID_N، پیام پاسخی را ارسال کند که تساوی $Y' = Y$ که نشان دهنده‌ی صحت شناسه‌ی ID_N است، برقرار شود.

حمله‌ی منع سرویس: در طرح ارائه شده دروازه‌ی NAN در همان ابتدای گام دوم، مهر زمانی و همچنین صحت داده‌های دریافتی از جانب کنتور هوشمند را بررسی می‌کند و در صورت عدم تأیید، جلسه خاتمه پیدا می‌کند. بنابراین مهاجم قادر نیست با ارسال داده‌های اشتباه منابع محاسباتی دروازه‌ی NAN را اشغال کند. یکی از روش‌های اعمال حمله‌ی منع سرویس از سوی مهاجم، بازپخش پیام‌های قدیمی است. با این حال، با توجه به مقاومت طرح پیشنهادی در برابر حمله‌ی تکرار، می‌تواند در برابر این نوع حمله‌ی منع سرویس نیز مقاومت کند.

گمنامی: هدف این سرویس این است که مهاجم با ردگیری پیام‌های رد و بدل شده در کانال ارتباطی ناامن نتواند شناسه‌ی واقعی طرفین ارتباط را به دست آورد. در این طرح، شناسه‌ی واقعی کنتورها و دروازه‌ی NAN در کانال ناامن بدون استفاده از تابع چکیده‌ساز یک‌طرفه ارسال نمی‌گردند و همچنین این شناسه‌ها با مقادیر تصادفی درآمیخته می‌شوند که باعث متفاوت شدن این مقادیر در هر نشست می‌شوند.

عدم برقراری ارتباط بین نشست‌ها: هدف این سرویس این است که علاوه بر برآورده شدن گمنامی، مهاجم حتی قادر به برقراری ارتباط بین یک نشست از یک کنتور خاص با نشست‌های دیگر همان کنتور نباشد. برای جلوگیری از ردگیری کنتورهای هوشمند توسط مهاجم ضروری است، تمام پیام‌های رد و بدل شده در هر نشست، متفاوت از سایر نشست‌ها

[1] impersonation attack

باشد، به علاوه مهاجم قادر نباشد با استفاده از داده‌های رد و بدل شده، به مقداری دست یابد که در هر نشست ثابت است. با در نظر گرفتن پیام‌های $\{a_i, b_i, c_i, L, T_1\}$ که در اولین ارتباط از طرف کنتور ارسال می‌شوند، درمی‌یابیم که پیام‌های L و c_i شامل عدد تصادفی r_2 هستند، بنابراین در هر نشست متفاوت خواهند بود. و همچنین مقادیر a_i و b_i نیز انتهای هر نشست به‌روز می‌شوند. به طور مشابه می‌توان دید تمام پیام‌های $\{\theta, \eta, \mu, Y\}$ که در دومین ارتباط از جانب NAN برای کنتور ارسال می‌شوند نیز دارای مقادیر تصادفی هستند و در هر نشست متفاوت از سایر نشست‌ها خواهند بود. در طرح ارائه شده، تمام مقادیر تنها به کمک عملیات XOR و تابع چکیده‌ساز محاسبه می‌شوند. بنابراین، طرح به گونه‌ای طراحی شده است که با XOR دو به دو یا هر تعداد از پیام‌های رد و بدل شده، به داده‌ی ثابتی نخواهیم رسید.

حمله‌ی ناهمگام‌سازی: یک پروتکل ممکن است در برابر حمله‌ی ناهمگام‌سازی آسیب‌پذیر باشد، اگر نیاز باشد تا طرفین برخی مقادیر خود را به طور همگام به‌روز کنند. در این حالت، پس از اینکه یک طرف مقادیر مورد نظر خود را به‌روز کرد، حمله‌کننده با روش‌های خلاقانه ارتباط را به گونه‌ای دستکاری می‌کند تا طرف مقابل نتواند مقادیر مورد نظر خود را به طور همگام به‌روز کند. در طرح پیشنهادی، مقادیر a_i و b_i در انتهای پروتکل به‌روز می‌شوند، اما فقط کنتور هوشمند این مقادیر را ذخیره کرده و طرف دوم پروتکل یعنی NAN، نیاز به به‌روزرسانی و ذخیره‌ی این مقادیر ندارد، زیرا که در ابتدای هر نشست این مقادیر توسط کنتور متقاضی ارتباط برای دروازه‌ی NAN ارسال می‌شوند. بنابراین، طرح پیشنهادی در برابر چنین حملاتی امن است.

امنیت رو به جلو: در این طرح، کلید نشست تلفیقی از مقادیر بلندمدت و مقادیر مختص به همان نشست مانند r_2، r_3، η، μ و B_i خواهد بود که این امر موجب می‌شود با نشت کلید یک نشست، امنیت کلید سایر نشست‌ها به خطر نیفتد.

امنیت کامل رو به جلو: یک پروتکل ویژگی امنیت کامل رو به جلو را دارد هر گاه با فرض لو رفتن کلیدهای خصوصی بلندمدت طرفین اجرایی پروتکل، کلید مشترک نشست‌های قبلی فاش نشود. برقراری این ویژگی با فرض لو رفتن تمام پارامترهای خصوصی در طرح‌های مبتنی بر توابع چکیده‌ساز و به طور کلی طرح‌هایی با ماهیت متقارن امکان‌پذیر نیست؛ اما اگر مطابق تعریف این ویژگی، فرض کنیم که کلیدهای خصوصی طرفین ارتباط لو برود و نه لزوماً تمام پارامترهای خصوصی [۱۰، ۱۱، ۱۷] در این صورت در طرح ارائه شده، مشابه طرح [۱۷] به علت عدم دسترسی مهاجم به شناسه‌ی مخفی دروازه‌ی NAN یعنی ID_N و به تبع آن عدم توانایی در محاسبه‌ی شناسه‌ی کنتور هوشمند (به عنوان مثال ID_i)، قادر به محاسبه‌ی کلید نشست نخواهد بود و لذا طرح ارائه شده ویژگی امنیت کامل رو به جلو را دارا است.

مقاومت در برابر نشت مقادیر موقت: در این طرح به کمک توابع چکیده‌ساز و یا XOR داده‌ها، از مقادیر حساسی که آشکار شدن آن‌ها موجب بر هم زدن امنیت طرح خواهد شد، به گونه‌ای محافظت می‌شود که حتی نشت تمام مقادیر موقت به طور هم‌زمان نیز موجب نشت این مقادیر حساس نشود.

جدول ۲. زمان اجرای عملیات مختلف

نمادها	توضیحات	(ms)
TH	زمان محاسبه‌ی تابع چکیده‌ساز	۰/۰۰۲۳
Tse	زمان محاسبه‌ی رمزگذاری و رمزگشایی متقارن	۰/۰۰۴۶
Tae	زمان محاسبه‌ی رمزگذاری و رمزگشایی نامتقارن	۳/۸۵
Te	زمان محاسبه‌ی عملیات توان‌رسانی	۳/۸
Tp	زمان محاسبه‌ی یک جفت دوسویی	۵/۸۱
Tmp	زمان محاسبه‌ی ضرب نقطه‌ای خم بیضوی	۲/۲۲۶
Tadd	زمان محاسبه‌ی جمع نقطه‌ای خم بیضوی	۰/۰۲۸۸
TMAC	زمان محاسبه‌ی عملیات MAC	۰/۰۰۴۶

۷ تحلیل عملکرد

از آنجایی که کنتورهای هوشمند ادواتی با منابع محدود هستند، برای پیاده‌سازی پروتکل‌های امنیتی در این گونه ادوات، پروتکل پیشنهادی باید در کنار برآورده کردن نیازمندی‌های امنیتی، ازنظر هزینه‌ی محاسباتی، سبک‌وزن و از نظر هزینه‌ی ارتباطی و سربار داده در وضعیت بهینه باشد.

۱.۷ هزینه‌ی محاسباتی

برای مقایسه‌ی هزینه‌ی محاسباتی طرح پیشنهادی، مطابق با مقالات [۲۰، ۲۱] جدول ۲ را تنظیم کردیم که زمان اجرای عملیات رمزنگاری مختلف را نشان می‌دهد. از جدول ۲ مشخص است که طرح‌های مبتنی بر خم بیضوی عموماً می‌توانند از طرح‌های مبتنی بر جفت‌های دوسویی یا رمزنگاری نامتقارن دارای هزینه‌ی محاسباتی کمتری باشند؛ اما با این حال، زمان عملیات ضرب نقطه‌ای خم بیضوی نیز نسبت به عملیاتی مانند تابع چکیده‌ساز بسیار بیشتر است. در جدول ۴ طرح خود را از منظر هزینه‌های محاسباتی با طرح‌های اخیراً ارائه شده در بستر شبکه‌ی هوشمند انرژی مقایسه می‌کنیم. همان طور که از جدول ۴ مشخص است، طرح پیشنهادی سبک‌ترین طرح ارائه شده تا کنون برای بستر شبکه‌ی هوشمند از منظر هزینه‌ی محاسباتی است که از دیگر طرح مبتنی بر توابع چکیده‌ساز ارائه شده برای بستر شبکه‌ی هوشمند یعنی طرح ژانگ و همکاران [۱۷] نیز علاوه بر رفع مشکلات امنیتی، چه از نظر هزینه‌ی محاسباتی و چه از نظر هزینه‌ی ارتباطی سبک‌تر است.

۲.۷ هزینه‌ی ارتباطی

یکی دیگر از معیارها برای سنجش سبک‌وزن بودن طرح‌ها هزینه‌های ارتباطی است. به این نحو که طرفین اجرایی پروتکل برای رسیدن به اهداف پروتکل که در اینجا توافق کلید و احراز اصالت است، در مجموع

جدول ۳. تعداد بیت عملیات مختلف

پارامترها	ارزش برحسب بیت
خروجی تابع چکیده‌ساز	۱۲۸
عدد تصادفی و شناسه	۱۲۸
MAC	۳۲
مهر زمانی	۳۲
پایه P	۳۲۰

چند بار با یکدیگر ارتباط برقرار کرده‌اند و در این ارتباطات چند بیت داده رد و بدل شده است. در طرح ارائه شده، طرفین برای توافق کلید و احراز اصالت در مجموع تنها نیاز به دو بار برقراری ارتباط و رد و بدل کردن داده دارند که کمترین تعداد ممکن است. برای محاسبه‌ی تعداد بیت پیام‌هایی که رد و بدل می‌شوند از مقادیر جدول ۳ استفاده می‌کنیم که این جدول مطابق مقاله‌ی [۱۵] تنظیم شده است. جدول ۴ مقایسه‌ی طرح ما با سایر طرح‌ها از منظر هزینه‌های ارتباطی را در کنار هزینه‌های محاسباتی و مقایسه‌ی امنیتی نشان می‌دهد.

۳.۷ سربار داده و مقیاس‌پذیری

در طرح پیشنهادی، دروازه‌ی NAN به ازای هر کنتور تنها باید شناسه‌ی آن یعنی (ID_i) را در حافظه‌ی خود ذخیره کند، که به دلیل افزایش تعداد کنتورهای هوشمند، از نظر مقیاس‌پذیری و سربار داده بسیار بهینه است.

۸ نتیجه‌گیری

در این مقاله پروتکل ارائه شده توسط ژانگ و همکاران مورد بررسی قرار گرفت و با تحلیل امنیتی پروتکل، نشان داده شد طرح آن‌ها در برابر حمله‌ی منع سرویس آسیب‌پذیر است و همچنین این طرح با توجه به افزایش کنتورهای هوشمند کارآمدی لازم را برای پیاده‌سازی در بستر شبکه‌ی هوشمند را ندارد. در ادامه، ما طرح جدیدی مبتنی بر توابع چکیده‌ساز ارائه دادیم و آن را از لحاظ برآورده کردن نیازمندی‌های امنیتی بررسی کردیم و همچنین نشان دادیم طرح ما از منظر هزینه‌های محاسباتی، حافظه و ارتباطی بسیار سبک و کاربردی بوده و مناسب برای پیاده‌سازی در بستر شبکه‌ی هوشمند انرژی است.

مراجع

[۱] باغستانی، سیدحمید و معظمی، فرخ لقا. تحلیل امنیتی دو پروتکل تبادل کلید احراز اصالت شده در بستر شبکه هوشمند انرژی. در بیست و هشتمین کنفرانس مهندسی برق ایران، صفحات ۲۳۱-۲۳۶، تبریز، ایران، مرداد ۱۳۹۹. دانشگاه تبریز.

[2] Okay, Feyza Yildirim and Ozdemir, Suat. A fog computing based smart grid model. in *2016 international symposium on networks, computers and communications (ISNCC)*, pp. 1–6. IEEE, 2016.

[3] Komninos, Nikos, Philippou, Eleni, and Pitsillides, Andreas. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4):1933–1954, 2014.

[4] Tuballa, Maria Lorena and Abundo, Michael Lochinvar. A review of the development of smart grid technologies. *Renewable and Sustainable Energy Reviews*, 59:710–725, 2016.

[5] Erol-Kantarci, Melike and Mouftah, Hussein T. Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues. *IEEE Communications Surveys & Tutorials*, 17(1):179–197, 2014.

[6] Kamilaris, Andreas, Pitsillides, Andreas, and Yiallouros, Michalis. Building energy-aware smart homes using web technologies. *Journal of Ambient Intelligence and Smart Environments*, 5(2):161–186, 2013.

[7] Metke, Anthony R and Ekl, Randy L. Security technology for smart grid networks. *IEEE Transactions on Smart Grid*, 1(1):99–107, 2010.

[8] Tsai, Jia-Lun and Lo, Nai-Wei. Secure anonymous key distribution scheme for smart grid. *IEEE transactions on smart grid*, 7(2):906–914, 2015.

[9] Canetti, Ran and Krawczyk, Hugo. Analysis of key-exchange protocols and their use for building secure channels. in *International conference on the theory and applications of cryptographic techniques*, pp. 453–474. Springer, 2001.

[10] Odelu, Vanga, Das, Ashok Kumar, Wazid, Mohammad, and Conti, Mauro. Provably secure authenticated key agreement scheme for smart grid. *IEEE Transactions on Smart Grid*, 9(3):1900–1910, 2016.

[11] Mahmood, Khalid, Chaudhry, Shehzad Ashraf, Naqvi, Husnain, Kumari, Saru, Li, Xiong, and Sangaiah, Arun Kumar. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication. *Future Generation Computer Systems*, 81:557–565, 2018.

[12] Abbasinezhad-Mood, Dariush and Nikooghadam, Morteza. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid com-

جدول ۴. مقایسه‌ی طرح پیشنهادی با طرح‌های اخیراً ارائه شده در بستر شبکه‌ی هوشمند انرژی

طرح‌ها	۱	۲	۳	۴	۵	۶	۷	۸	۹	کنتور هوشمند	زمان (میلی ثانیه)	ارائه دهنده‌ی خدمات یا دروازه‌ی NAN	زمان (میلی ثانیه)	تعداد ارتباط	تعداد بیت منتقل شده
[۸]	✔	✘	✘	✔	✔	✔	-	✔	✘	$۳Tmp + Te + ۵TH$	۱۳	$۳Tmp + Te + ۲Tb + ۵TH$	۲۲	۳	۳۴۲۴
[۱۰]	✔	✘	✘	✔	✔	✔	-	✔	✔	$۳Tmp + Te + ۶TH$	۱۱	$۲Tmp + Te + ۲Tb + ۶TH$	۲۰	۳	۳۷۴۴
[۱۱]	✔	✔	✔	✔	✔	✘	-	✔	✘	$۵Tmp + ۲Tadd + ۴TH$	۱۱٫۲	$۵Tmp + ۲Tadd + ۴TH$	۲۲٫۴	۲	۱۸۱۲
[۱۲]	✘	✔	✔	✘	✔	✘	-	✔	✔	$۴Tmp + ۲Tadd + ۴TH$	۹	$۴Tmp + ۲Tadd + ۴TH$	۹	۳	۱۸۱۲
[۱۳]	✔	✔	✔	✔	✔	✔	-	✔	✔	$۴Tmp + ۲Tadd + ۵TH$	۹	$۲Tmp + TF + ۸TH$	۶٫۷	۳	۱۶۰۰
[۱۴]	✔	✘	✔	✔	✘	✔	-	✔	✔	$۲Tmp + ۶H$	۴٫۴۷	$۲Tmp + ۶TH$	۴٫۴۷	۳	۱۲۴۸
[۱۵]	✔	✔	✔	✔	✔	✘	-	✔	✔	$۳Tmp + ۴TH + ۲TMAC + ۲Tse$	۶٫۷	$۳Tmp + ۵TH + ۲TMAC + ۲Tse$	۶٫۷	۲	۱۰۸۸
[۲۲]	✔	✔	✘	✔	✘	✔	-	✔	✔	$۲Tmp + Te + ۵TH$	۸٫۳۱	$۳Tmp + Te + Tb + ۵TH$	۱۶٫۳	۳	۲۷۵۲
[۲۳]	✔	✔	✔	✔	✔	✔	-	✔	✘	$۴Tmp + ۱Tadd + ۵TH$	۸٫۹۴	$۶Tmp + ۲Tadd + ۶TH$	۱۳٫۴۳	۳	۱۶۳۲
[۲۴]	✔	✔	✔	✔	✔	✘	-	✘	✘	$۱TH + ۱TMAC + ۲Tse + ۳Tae$	۱۲	$۱TH + ۱TMAC + ۲Tse + ۳Tae$	۱۲	۲	۶۴۰۰
[۲۵]	✔	✔	✔	✔	✘	✘	-	✔	✔	$۲Tmp + ۳TH$	۴٫۴۶	$۳Tmp + ۲Tadd + ۴TH$	۶٫۷۴	۳	۱۶۳۲
[۲۶]	✔	✔	✘	✔	✔	✔	-	✔	✔	$۳Te + ۳TH$	۱۱٫۶	$۴Te + ۳TH$	۱۵٫۴	۲	۲۶۵۶
ژانگ [۱۷]	✔	✔	✔	✔	✘	✔	✔	✔	✔	$۱Tse + ۷TH$	۰٫۰۲۰۷	$۳Tse + ۹TH$	۰٫۰۳۴۵	۴	۱۴۰۸
طرح پیشنهادی	✔	✔	✔	✔	✔	✔	✔	✔	✔	$۳TH$	۰٫۰۰۶۹	$۹TH$	۰٫۰۲	۲	۱۰۵۶

۱- احراز اصالت متقابل، ۲- مقاومت در برابر حمله‌ی جعل هویت، ۳- تغییر پیام و مقاومت در برابر حمله‌ی فرد در میانه، ۴- مقاومت در برابر حمله‌ی تکرار ۵- مقاومت در برابر حمله‌ی منع سرویس ۶- برقراری گمنامی و عدم ردگیری، ۷- مقاومت در برابر حمله‌ی ناهمگام‌سازی، ۸- برقراری امنیت کامل روبه‌جلو، ۹- مقاومت در برابر نشت راز موقت

[16] Esfahani, Alireza, Mantas, Georgios, Matischek, Rainer, Saghezchi, Firooz B, Rodriguez, Jonathan, Bicaku, Ani, Maksuti, Silia, Tauber, Markus G, Schmittner, Christoph, and Bastos, Joaquim. A lightweight authentication mechanism for m2m communications in industrial iot environment. *IEEE Internet of Things Journal*, 6(1):288–296, 2017.

[17] Zhang, Liping, Zhao, Lanchao, Yin, Shuijun, Chi, Chi-Hung, Liu, Ran, and Zhang, Yixin. A lightweight authentication scheme with privacy protection for smart grid communications. *Future generation computer systems*, 100:770–778, 2019.

[18] Li, Xiong, Ibrahim, Maged Hamada, Kumari, Saru, Sangaiah, Arun Kumar, Gupta, Vidushi, and Choo, Kim-Kwang Raymond. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Computer Networks*, 129:429–443, 2018.

[13] Wazid, Mohammad, Das, Ashok Kumar, Kumar, Neeraj, and Rodrigues, Joel JPC. Secure three-factor user authentication scheme for renewable-energy-based smart grid environment. *IEEE Transactions on Industrial Informatics*, 13(6):3144–3153, 2017.

[14] Kumar, Neeraj, Aujla, Gagangeet Singh, Das, Ashok Kumar, and Conti, Mauro. Eccauth: A secure authentication protocol for demand response management in a smart grid system. *IEEE Transactions on Industrial Informatics*, 15(12):6572–6582, 2019.

[15] Kumar, Pardeep, Gurtov, Andrei, Sain, Mangal, Martin, Andrew, and Ha, Phuong H. Lightweight authentication and key agreement for smart metering in smart energy networks. *IEEE Transactions on Smart Grid*, 10(4):4349–4359, 2018.

2017.

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

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

[21] Abbasinezhad-Mood, Dariush, Ostad-Sharif, Arezou, and Nikooghadam, Morteza. Novel anonymous key establishment protocol for isolated smart meters. *IEEE Transactions on Industrial Electronics*, 67(4):2844–2851, 2019.

[22] Chen, Yuwen, Martínez, José-Fernán, Castillejo, Pedro, and López, Lourdes. An anonymous authentication and key establish scheme for smart grid: Fauth. *Energies*, 10(9):1354, 2017.

[23] He, Debiao, Wang, Huaqun, Khan, Muhammad Khurram, and Wang, Lina. Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography. *IET Communications*, 10(14):1795–1802, 2016.

[24] Mahmood, Khalid, Chaudhry, Shehzad Ashraf, Naqvi, Husnain, Shon, Taeshik, and Ahmad, Hafiz Farooq. A lightweight message authentication scheme for smart grid communications in power sector. *Computers & Electrical Engineering*, 52:114–124, 2016.

[25] Mohammadali, Amin, Haghighi, Mohammad Sayad, Tadayon, Mohammad Hesam, and Mohammadi-Nodooshan, Alireza. A novel identity-based key establishment method for advanced metering infrastructure in smart grid. *IEEE Transactions on Smart Grid*, 9(4):2834–2842, 2016.

[26] Li, Xiong, Wu, Fan, Kumari, Saru, Xu, Lili, Sangaiah, Arun Kumar, and Choo, Kim-Kwang Raymond. A provably secure and anonymous message authentication scheme for smart grids. *Journal of Parallel and Distributed Computing*, 132:242–249, 2019.

MonadiAfta-Bianual Scientific Journal for Cyberspace Security
2022, Volume 20, Number 1 (pp. 26–36)
https://monadi.isc.org.ir

Presented at the ISCISC 2021 in University of Isfahan, Isfahan, Iran

Lightweight and Secure Authentication Key Agreement Protocol for Smart Grid★

Seyed Hamid Baghestani * and Farokhlagha Moazami

Cyberspace Research Institute, University of Shahid Beheshti (SBU), Tehran, Iran

ARTICLE INFO.

Keywords:
mutual authentication
key agreement
smart grid
denial of service attack
update

dor: 20.1001.1.24763047.1401.11.1.4.1

Type: research paper

ABSTRACT

The conventional electricity infrastructure relies on the usage of fossil fuels, which harms the environment greatly. A smart grid is an infrastructure that enables the integration of renewable resources with the distribution system, as well as the potential of establishing a two-way flow of energy and data between network management and subscribers in order to optimize energy use. However, this data flow may be misused by attackers to disrupt security and causes power network imbalances.Therefore, it is necessary to exploit different security protocols to exchange data in this platform. One of these security protocols is the authenticated key agreement protocol, which allows the parties to authenticate each other and share a key to encrypt data. Recently Zhang et al. proposed a lightweight key authentication protocol based on hash functions. In this paper, we examine their protocol and show that vulnerable to denial of service (DOS) attack and also is not optimized to implement on smart grid. Then we present a lightweight and secure authentication protocol based on hash functions.

© 2022 ISC

★ The ISCISC 2021 Program Committee effort is highly acknowledged for reviewing this paper.
* Corresponding author
Email addresses: seyedhamid.baghestani@gmail.com (Seyed Hamid Baghestani), f_moazemi@sbu.ac.ir (Farokhlagha Moazami)
© 2022 ISC. All rights reserved.