تحلیل امنیتی دو پروتکل تبادل کلید احراز اصالت شده در شبکه هوشمند انرژی

سید حمید باغستانی[۱]، فرخ لقا معظمی گودرزی[۲]
[۱]دانشجوی کارشناسی ارشد پژوهشکده فضای مجازی دانشگاه شهید بهشتی، seyedhamid.baghestani@gmail.com
[۲]استادیار پژوهشکده فضای مجازی دانشگاه شهید بهشتی، f_moazemi@sbu.ac.ir

چکیده - امروزه با مصرف بیش‌ازحد انرژی، علم مهندسی، همواره به دنبال دست‌یابی به روش‌هایی برای مدیریت بهینه مصرف انرژی و جلوگیری از هدر رفت آن است. یکی از راهکارهای مفید در امر مدیریت مصرف انرژی ادغام شبکه انرژی با فناوری *IT* است، برای اینکه بین تولیدکنندگان و مصرف‌کنندگان انرژی داده ردوبدل گردد. به چنین شبکه‌ای شبکه هوشمند انرژی گفته می‌شود. این انتقال داده باید در بستری امن صورت پذیرد و آسیب‌پذیری این بستر می‌تواند حریم خصوصی شهروندانی که از شبکه هوشمند استفاده می‌کنند را به خطر اندازد و یا خسارات سنگینی به شبکه وارد نماید. تاکنون پروتکل‌های زیادی برای ایجاد بستری مناسب برای انتقال امن اطلاعات در محیط شبکه هوشمند طراحی‌شده است که هرکدام از آن‌ها دارای مشکلاتی هستند که هنوز مسئله را برای کار در این بستر باز نگه‌داشته‌اند. اخیراً پاردپ کومار و همکارانش و همچنین نراج کومار و همکارانش دو پروتکل تبادل کلید احراز اصالت شده را پیشنهاد کردند و نشان دادند که پروتکل‌های پیشنهادی آن‌ها در برابر حملات امنیتی مختلف امن است. بااین‌حال، در این مقاله ما نشان می‌دهیم که پروتکل پاردپ کومار، خاصیت گمنام بودن افزاره‌های هوشمند را به‌خوبی حفظ نمی‌کند و در برابر حمله ردگیری افزاره‌ها آسیب‌پذیر است و پروتکل نراج کومار، در برابر حمله منع سرویس آسیب‌پذیر است.

کلید واژه- احراز اصالت متقابل، تبادل کلید، شبکه هوشمند انرژی، گمنامی، حمله منع سرویس

۱- مقدمه

شبکه هوشمند در حال تبدیل شدن به شبکه برق نسل بعدی است و توزیع برق قابل اعتماد برای میلیون‌ها مشتری را به‌صورت خودکار امکان‌پذیر می‌کند [1]. برخلاف شبکه سنتی، شبکه هوشمند اجازه می‌دهد تا یک جریان دوطرفه از انرژی و اطلاعات برای کنترل بهینه تولید و مصرف انرژی ایجاد گردد و همچنین به مصرف‌کنندگان این امکان را می‌دهد تا به‌صورت لحظه‌ای از میزان انرژی مصرفی خود و هزینه آن مطلع گردند [2]. همچنین این امکان را به تولیدکنندگان انرژی می‌دهد تا به نسبت بار موجود در شبکه تعرفه‌های مصرفی را به‌صورت پویا تغییر دهند. در شبکه هوشمند، افزاره‌های اندازه‌گیری هوشمند، وظیفه اندازه‌گیری دقیق میزان مصرف مشترکین را بر عهده‌دارند. زیرساخت اندازه‌گیری هوشمند (AMI) یکی از زمینه‌های کاربردی مهم این شبکه‌ها است که به ارزیابی وضعیت شبکه برق برای مدیریت بهینه منابع توزیع‌شده کمک می‌کند [3,4].

با توجه به تمام فواید ذکرشده، بااین‌حال، داده‌های منتقل‌شده در ارتباطات شبکه هوشمند به سطح ترابایت رسیده و سوءاستفاده از قرائت افزاره‌های اندازه‌گیری هوشمند ممکن است منجر به نشت حریم خصوصی مشتریان شود [5]. بنابراین برقراری امنیت از فاکتورهای اساسی در طراحی شبکه هوشمند است. یکی از نیازمندی‌های اصلی برای دست‌یابی به بستر امن در محیط شبکه هوشمند، ارسال داده‌ها به‌صورت رمز شده است که برای دست‌یابی به آن نیازمند احراز اصالت متقابل و توزیع یک کلید نشست هستیم.

از مهم‌ترین چالش‌های اساسی که طراحان پروتکل‌های امنیتی در بستر شبکه هوشمند با آن مواجه هستند محدود بودن منابع محاسباتی و حافظه به‌ویژه در سمت افزاره‌های اندازه‌گیری هوشمند است. ازاین‌رو طراحان باید در نظر داشته باشند پروتکلی که ارائه می‌دهند علاوه بر برآورده کردن نیازهای امنیتی تا جای ممکن سبک طراحی گردند [6]. ارائه یک پروتکل احراز اصالت و تبادل کلید به‌صورت توأم نسبت به دو پروتکل احراز اصالت و تبادل کلید جدا، هم سبک‌تر بوده و هم نشت اطلاعات کمتری دارد [7]. بنابراین طراحی پروتکل‌های توزیع کلید احراز اصالت شده توجه محققان زیادی را به خود جلب کرده است.

درطرح‌های ارائه‌شده معمولاً پروتکل تبادل کلید احراز اصالت شده متقابل دارای سه فاز راه‌اندازی، ثبت و فاز احراز اصالت و تبادل کلید است که در فاز راه‌اندازی مقادیر و توابع مورداستفاده مانند تابع‌های چکیده ساز، گروه، میدان، مولدها مشخص و به‌صورت عمومی

اعلام می‌شوند. در فاز ثبت طرفین اجرایی پروتکل باید خود را در شبکه ثبت کنند. این فاز معمولاً به کمک یک کانال امن صورت می‌گیرد و پارامترهای خصوصی طرفین تولید و در اختیارشان قرار داده می‌شود. فاز احراز هویت و توزیع کلید نیز فازی است که طرفین پروتکل به کمک اطلاعاتی که از دو فاز قبل در اختیاردارند قادر خواهند بود خود را برای طرف مقابل احراز اصالت کرده و یک کلید نشست به اشتراک بگذارند [8].

در این مقاله ابتدا در بخش ۲ برخی از کارهای انجام‌شده در این زمینه را بررسی می‌کنیم. در بخش ۳ به معرفی پروتکل پاردپ کومار [۱] خواهیم پرداخت و در بخش ۴ حمله اعمال‌شده را شرح می‌دهیم. در بخش ۵ به معرفی پروتکل نراج کومار [۲] خواهیم پرداخت و حمله اعمال‌شده به این طرح را نیز در بخش ۶ شرح می‌دهیم. و در آخر در بخش ۷ یک جمع‌بندی از مقاله ارائه می‌دهیم.

۲- کارهای پیشین

با توجه به تمام نیازهای مطرح‌شده تسای [۳] و همکارش طرحی به کمک خواص جفت‌های دوسویی [۴] ارائه دادند که از مزایای آن گمنامی شناسه افزاره هوشمند است [9]. اما به دلیل بالا بودن هزینه محاسباتی جفت‌های دوسویی، روش ارائه‌شده برای اجرا بر روی بستر شبکه هوشمند با منابع محدود بهینه نیست. همچنین این طرح در مدل CK-Adversary [10] امن نبود و با نشت مقدار تصادفی، کلید نشست فاش می‌شد. برای جلوگیری از بار سنگین محاسباتی جفت‌های دوسویی خلید محمود [۵] و همکارانش یک طرح توافق کلید به کمک خم‌های بیضوی ارائه دادند [11]. برخلاف ادعای ارائه‌کنندگان این طرح که آن را بسیار مناسب برای پیاده‌سازی بر روی تجهیزات شبکه‌های هوشمند می‌دانند، طرح گمنام بودن تجهیزات را در نظر نگرفته است و شناسه تجهیزات نیز به‌راحتی توسط مهاجم قابل‌دسترسی است. ازآنجایی‌که طرح آن‌ها نیز در مدل CK-Adversary امن نبود، نیکوقدم [۶] و عباسی نژاد [۷] در طرح [12] یک حمله به آن اعمال کردند که در این حمله با نشت مقدار تصادفی تولیدشده، کلید نشست آشکار می‌شد. در این طرح در مرحله ثبت تجهیزات در TA محاسبات زیادی برای تولید پارامترهای امنیتی صورت می‌گیرد که باوجود انجام محاسبات زیاد، همچنان راهکاری برای مخفی نگه‌داشتن شناسه افزاره‌ها دیده نشده است.

در سال ۲۰۱۸ یک طرح احراز اصالت دوطرفه و توافق کلید بین افزاره اندازه‌گیری هوشمند و دروازه همسایگی (NAN) [۸] برای بستر شبکه هوشمند به نام LAKA توسط پاردپ کومار و همکارانش ارائه شد [13]. در این طرح از NAN به‌عنوان TA [۹] استفاده‌شده است که از مزایای این طرح محسوب می‌شود؛ به این معنی که پارامترهای مرحله ثبت افزاره‌ها، توسط NAN محاسبه می‌شود. در این طرح از رمزنگاری مبتنی بر خم بیضوی به همراه رمزنگاری متقارن AES و همچنین از MAC استفاده‌شده است. این نامتجانس بودن توابع رمزنگاری باعث می‌شود که حجم حافظه زیادی برای پیاده‌سازی توابع مختلف اشغال شود. همچنین ما دریافتیم برخلاف ادعای طراحان، طرح ارائه‌شده به‌خوبی گمنامی را برآورده نمی‌کند و با توجه به آشکار بودن شناسه NAN برای افزاره‌های عضو در شبکه، یک افزاره خرابکار می‌تواند بقیه افزاره‌ها را ردگیری [۱۰] کرده و تشخیص دهد آیا دو نشست متعلق به یک افزاره هوشمند است یا خیر.

در سال ۲۰۱۹ نراج کومار و همکارانش یک پروتکل احراز هویت و توزیع کلید مبتنی بر خم بیضوی برای بستر شبکه هوشمند بین افزاره اندازه‌گیری هوشمند و ارائه‌دهنده خدمات طراحی کرده‌اند [14]. ما دریافتیم پروتکل ارائه‌شده در گام دوم هیچ‌گونه بررسی روی صحت‌وسقم پیام‌های دریافتی انجام نمی‌دهد و همین امر موجب اعمال حمله منع سرویس به پروتکل خواهد شد.

۳- بررسی طرح پاردپ کومار و همکاران

طرح LAKA شامل سه فاز است. ۱) فاز راه‌اندازی، ۲) فاز ثبت افزاره و ۳) فاز احراز اصالت و تبادل کلید. نمادهای بکار رفته در این طرح مطابق با جدول ۱ آورده شده است.

جدول ۱: نمادهای طرح LAKA [13]

Symbols	Descriptions
N_{ID}	Neighborhood Area Network (NAN) identity
SM_{ID}	Smart meter identity
ST, id_{ST}	Secret token and its identity
$E_K[ms]$	Encrypt ms using key (K)
$D_K[ms]$	Decrypt ms using key (K)
p, n	Large prime numbers
F_q	A finite field
E	Elliptic curve defined on finite field F_q with prime order n
G	Group of elliptic curve points on E
P	A point on elliptic curve E with order n
$H(.)$	One-way hash function (e.g., SHA-1, SHA-2, MD5, etc.)
MAC, $\|\|$	Message authentication code, and concatenation operation
ϕ, ϕ_N	SM's and NAN's pseudo random numbers, respectively

[۱] Pardeep Kumar
[۲] Neeraj Kumar
[۳] L.Tsai
[۴] Bilinear paring
[۵] Kh. Mahmood
[۶] M.Nikooghadam
[۷] D.Abbasinezhad
[۸] Neighbourhood Area Network
[۹] Trusted Authority
[۱۰] Trace

۳-۱- فاز راه‌اندازی

در این طرح دروازه NAN، به‌عنوان یک نهاد قابل اعتماد، وظایف یک TA برون‌خط[۱۱] را از قبیل اختصاص پارامترهای امنیتی و اختصاص هویت به افزاره‌های هوشمند، به‌صورت امن انجام می‌دهد. در این مرحله، دروازه همسایگی NAN پارامترهای امنیتی را به شرح زیر تنظیم می‌کند.

NAN یک منحنی بیضوی E و یک نقطه P از مرتبه n را روی منحنی E انتخاب می‌کند. یک کلید اصلی با آنتروپی بالا M_k و کلید عمومی $P_s = M_k P$ تولید می‌کند. سپس یک تابع چکیده ساز امن یک‌طرفه را انتخاب کرده (به‌عنوان‌مثال ، H()) و در انتها، M_k را در پایگاه امن خود ذخیره می‌کند و $\{H(), n, E, P, F_P, Ps\}$ را منتشر می‌کند.

۳-۲- فاز ثبت افزاره‌های هوشمند

افزاره‌های اندازه‌گیری هوشمند باید قبل از شرکت در نشست در دروازه NAN ثبت شوند و پارامترهای امنیتی را به شرح زیر دریافت کنند.

برای هر افزاره هوشمند (مثلاً j)، NAN یک شناسه مخفی و منحصربه‌فرد (SM_{ID_j}) و یک کلید مخفی ST_j را با شناسه آن (id_{ST_j}) تولید و اختصاص می‌دهد. از SM_{ID_j} برای محاسبه $\sigma_j = H(SM_{ID_j})$ و کلید عمومی $SM_{pub_j} = (\sigma_j + M_k)P = \sigma_j P + P_s$ استفاده می‌کند. سپس از کلید اصلی M_k برای محاسبه کلید خصوصی مربوط به SM یعنی $SM_{pr_j} = \frac{1}{M_k + \sigma_j}.p \in G$ استفاده می‌کند سرانجام NAN تمام پارامترهای امنیتی $\{F_p؛ P؛ E؛ n؛ ST_j ؛ id_{ST_j} ؛ H() ؛ \sigma_j ؛ SM_{pr_j}\}$ را در حافظه امن افزاره ذخیره می‌کند. علاوه بر این ، دروازه NAN همچنین SM_{ID_j} و N_{ID} را در حافظه امن افزاره قرار می‌دهد تا بتواند دروازه NAN مربوطه را تشخیص دهد. سرانجام ، دروازه NAN کلیه پارامترها را در پایگاه داده خود نگه می‌دارد تا سوابق افزاره مستقر را نگه دارد.

۳-۳- فاز احراز اصالت متقابل و تبادل کلید

برای دستیابی به اهداف LAKA، یعنی احراز اصالت سبک و تبادل یک کلید، روند فاز در شکل ۱ نشان داده‌شده است.

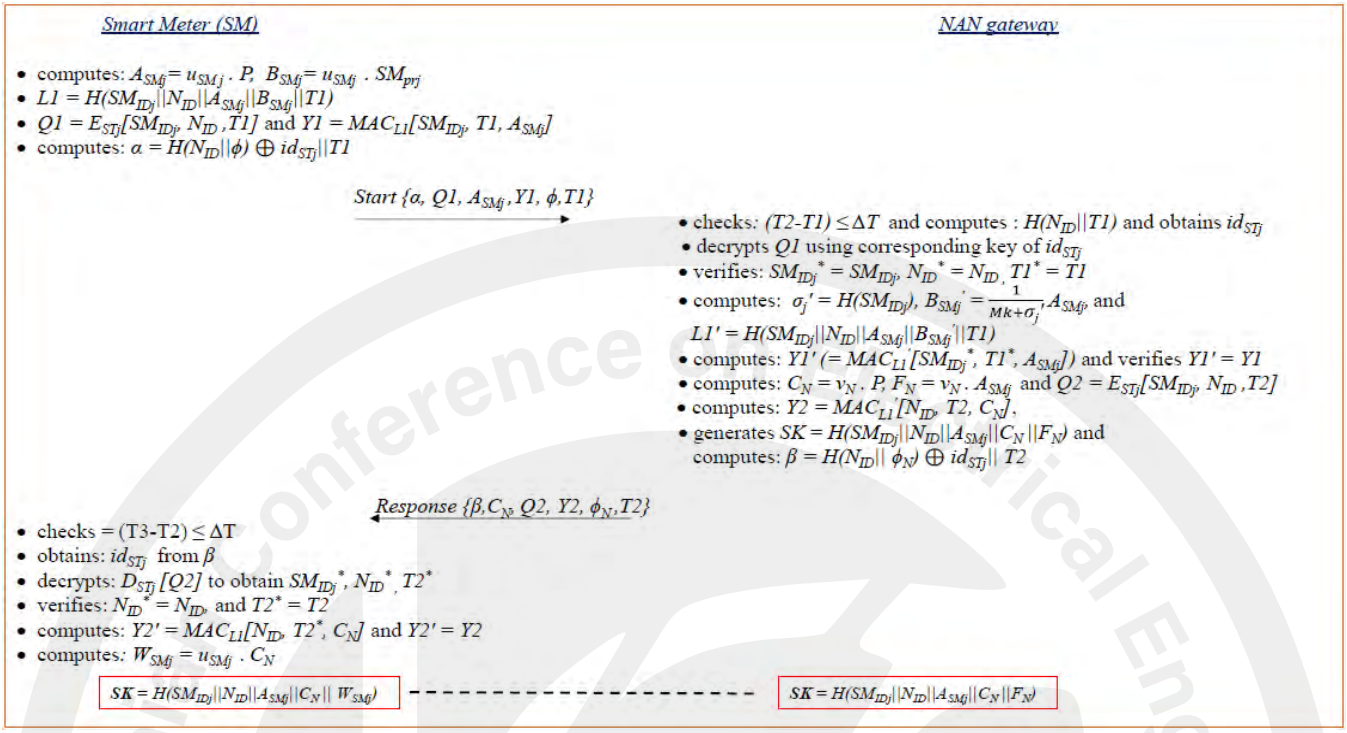
گام اول: SM به صورت تصادفی $u_{SM_j} \in Z_n^*$ را انتخاب کرده و $A_{SM_j} = u_{SM_j}.\mathrm{P}$ و $B_{SM_j} = u_{SM_j}.\mathrm{SM}_{pr_j}$ را محاسبه می‌کند. سپس افزاره SM، $L1 = H(SM_{ID_j} \| N_{ID} \| A_{SM_j} \| B_{SM_j} \| T1)$ و $\mathrm{Q1} = E_{ST_j}[SM_{ID_j}, N_{ID}, T1]$ را محاسبه می‌کند که $T1$ بیانگر مهر زمانی فعلی SM است. به منظور ارائه یکپارچگی پیام، افزاره هوشمند، $Y1 = MAC_{L1}[SM_{ID_j}, T1, A_{SM_j}]$ را محاسبه می‌کند. سپس SM، عدد تصادفی ϕ را ایجادکرده و $\alpha = H(N_{ID} \| \phi) \oplus id_{ST_j} \| T1$ را محاسبه می‌کند. در آخر پیام شروع را به NAN ارسال می‌کند که شامل $\{\alpha, \mathrm{Q1}, A_{SM_j}, \mathrm{Y1}, \phi, \mathrm{T1}\}$ می‌باشد.

گام دوم: NAN پس از دریافت پیام، ابتدا اعتبار مهر زمانی را با استفاده از $(T2 - T1) \leq \Delta T$ بررسی می‌کند و در صورت عدم تطابق، سیستم را متوقف می‌کند. T2 بیانگر مهر زمان فعلی NAN است و ΔT تأخیر انتقال است. در غیر این صورت، $\mathrm{H}(N_{ID} \| \phi)$ را محاسبه کرده و id_{ST_j} را از α به دست می‌آورد و کلید مربوط به آن یعنی ST_j را از پایگاه داده خود دریافت کرده و به کمک آن $\mathrm{D}_{ST_j}[\mathrm{Q1}]$ را رمزگشایی کرده و $SM_{ID_j}^* = SM_{ID_j}$ ، $N_{ID}^* = N_{ID}$ و $(\mathrm{T1} = \mathrm{T1}^*)$ را بررسی می‌کند. اگر تأیید نشود، درخواست را متوقف می‌کند. در غیر این صورت NAN، $B'_{SM_j} = \frac{1}{M_k + \sigma_j'} A_{SM_j}$ ، $\sigma_j' = \mathrm{H}(\mathrm{SM_{ID_j}})$ و به کمک آن‌ها $L1' = H(SM_{ID_j} \| N_{ID} \| A_{SM_j} \| B'_{SM_j} \| T1)$ را محاسبه کرده و در ادامه، $Y1' = MAC_{L1'}[SM_{ID_j}, T1, A_{SM_j}]$ را محاسبه می‌کند. سپس $Y1' = Y1$ را بررسی می‌کند اگر درست بود، گام بعدی را انجام می‌دهد.

گام سوم: دروازه NAN یک عدد تصادفی $\mathrm{v}_N \in Z_n^*$ را انتخاب می‌کند. $\mathrm{C}_N = v_N.\mathrm{P}$ و $F_N = v_N.A_{SM_j}$ را محاسبه کرده و سپس $\mathrm{Y1}' = \mathrm{MAC}_{L1'}[N_{ID}, \mathrm{T2}, C_N]$ و $\mathrm{Q2} = E_{ST_j}[SM_{ID_j}, N_{ID}, T2]$ را محاسبه می‌کند که در اینجا ، T2 بیانگر مهر زمان فعلی NAN است. NAN، کلید جلسه $\mathrm{SK} = \mathrm{H}(SM_{ID_j} \| N_{ID} \| A_{SM_j} \| \mathrm{C}_N \| F_N)$ را ایجاد می‌کند. سرانجام، یک عدد تصادفی ϕ_N را تولید می‌کند و $\beta = H(N_{ID} \| \phi_N) \oplus id_{ST_j} \| T2$ را محاسبه کرده و پیام پاسخ $\{\beta, Q2, C_N, Y2, \phi_N, T2\}$ را ارسال می‌کند.

گام چهارم: SM، $(T3 - T2) \leq \Delta T$، را چک می‌کند در صورت منفی بودن نتیجه تأیید مهر زمانی، جلسه را به پایان می‌رساند. در غیر این صورت، id_{ST_j} را از β به دست می‌آورد، $\mathrm{D}_{ST_j}[\mathrm{Q2}]$ را رمزگشایی می‌کند تا $SM_{ID_j}^*$ و N_{ID}^* را مشاهده کند و $N_{ID}^* = N_{ID}$ و $T2 = T2^*$ را بررسی می‌کند. اگر شرایط صحیح نباشد، جلسه را خاتمه می‌دهد. در غیر این صورت ، $Y2' = MAC_{L1}[N_{ID}, T2^*, C_N]$ را محاسبه کرده و $Y2' = Y2$ را بررسی می‌کند، اگر شرط صحیح باشد، جلسه را ادامه می‌دهد. در غیر این صورت NAN یک نهاد قانونی نیست. سرانجام SM، $W_{SM_j} = u_{SM_j}.C_N$ را محاسبه کرده و کلید جلسه $\mathrm{SK} = \mathrm{H}(SM_{ID_j} \| N_{ID} \| A_{SM_j} \| \mathrm{C}_N \| F_N)$ را به‌منظور برقراری ارتباط با دروازه همسایگی NAN تولید می‌کند.

[۱۱] offline



شکل ۱: فاز تبادل کلید و احراز اصالت متقابل طرح LAKA [13]

۴- اعمال حمله ردگیری افزاره‌های اندازه‌گیری هوشمند

روش اعمال این حمله طبق چند مرحله زیر توضیح داده می‌شود.

مرحله۱: مهاجم پیام‌های ارسالی α، ϕ و $T1$ در گام اول اجرای طرح که از افزاره هوشمند به سمت دروازه همسایگی NAN فرستاده‌شده را شنود می‌کند.

مرحله۲: مهاجم برای اعمال این حمله نیاز به شناسه NAN یعنی N_{ID} دارد که این شناسه در اختیار تمام افزاره‌های عضو در شبکه قرار داده می‌شود. بنابراین برای دستیابی به N_{ID} مهاجم می‌تواند یک افزاره خودی و عضو در شبکه باشد یا باهدف اعمال این حمله و ردگیری افزاره‌های دیگر، به‌راحتی در شبکه عضو گردد.

مرحله۳: مهاجم با استفاده از α، ϕ، $T1$، N_{ID} و با کمک رابطه (۱) می‌تواند به‌راحتی شناسه کلید ST_j یعنی id_{ST_j} را به دست آورد.

$$\alpha = H(N_{ID} \parallel \phi) \oplus id_{ST_j} \parallel T1 \qquad (۱)$$

مرحله۴: مهاجم با به دست آوردن id_{ST_j} با توجه به این‌که این مقدار توسط NAN در مرحله ثبت تجهیز در اختیار افزاره قرار داده می‌شود و در تمام نشست‌های مربوط به افزاره j ام و NAN مقدار ثابتی دارد، موجب ردگیری افزاره توسط مهاجم خواهد شد.

مشابه همین حمله را می‌توان در گام چهارم نیز انجام داد و مهاجم می‌تواند با شنود پیام ارسالی از طرف دروازه NAN، یعنی پیام پاسخ و در اختیار داشتن مقادیر β، ϕ_N، T2، N_{ID} و به کمک رابطه (۲) ، شناسه کلید id_{ST_j} را به دست آورد و مطابق روش گفته‌شده افزاره را ردگیری کرد.

$$\beta = H(N_{ID} \parallel \phi_N) \oplus id_{ST_j} \parallel T2 \qquad (۲)$$

۵- بررسی طرح نراج کومار و همکاران

این طرح شامل چهار فاز است. ۱) فاز راه‌اندازی، ۲) فاز ثبت افزارها، ۳) فاز ثبت ارائه‌دهندگان خدمات و ۴) فاز احراز اصالت و تبادل کلید. نمادهای بکار رفته در این طرح در جدول ۲ آورده شده است.

جدول ۲: نمادهای طرح نراج کومار [14]

Symbol	Description
TA	Trusted authority
SD_i	i^{th} SG device
ID_i	Unique identity of SD_i
UC_j	j^{th} utility or remote control center
ID_i	Unique identity of UC_j
$\mathcal{A}$	Adversary
$h(\cdot)$	Collision-resistant one-way cryptographic hash function
p	A large prime number
Z_p	$Z_p = \{0, 1, \cdots, p-1\}$, a finite field
$E_p(a,b)$	A non-singular elliptic curve $y^2 = x^3 + ax + b \pmod p$ over finite field Z_p with $4a^3 + 27b^2 \neq 0 \pmod p$
G	A base point on $E_p(a,b)$
$k.G$	An elliptic curve point multiplication; $k \in Z_p^*$ being a scalar and $G \in E_p(a,b)$
x	Secret key of the TA
Q	$Q = x.G$, the public key of the TA
T_1, T_2, T_3	Current system timestamps
RTS_i, RTS_j	Registration timestamps of SD_i and UC_j, respectively
ΔT	Maximum transmission delay
SK_{ij}	Session key between SD_i and UC_j
$\oplus$, $\|\|$	Bitwise XOR and concatenation operations, respectively

۵-۱- فاز راه‌اندازی

در این طرح TA به‌عنوان یک نهاد قابل اعتماد بوده و به‌صورت

برون‌خطی قبل از شروع نشست، توابع و پارامترهای لازم را برای احراز اصالت و تبادل یک کلید در اختیار طرفین پروتکل قرار می‌دهد. در این فاز TA خم بیضوی E و یک نقطه G از مرتبه n را روی خم E انتخاب کرده و یک کلید اصلی x و کلید عمومی $Q = x.G$ تولید می‌کند. سپس یک تابع چکیده ساز امن یک‌طرفه را انتخاب می‌کند (به‌عنوان‌مثال ، H()) و در انتها، x را در حافظه امن خود ذخیره کرده و $\{H(), n, E, G, F_G, Q\}$ را منتشر می‌کند.

۵-۲- فاز ثبت افزاره‌های هوشمند

به‌عنوان‌مثال برای ثبت افزاره i ام یعنی SD_i، $(i = 1, 2, \dots, l)$ که l تعداد دستگاه‌های مستقر در محیط شبکه هوشمند است، فاز ثبت به این صورت انجام می‌گیرد که TA به‌عنوان یک نهاد قابل اعتماد یک شناسه منحصربه‌فرد ID_i انتخاب کرده و شناسه مستعار $RID_i = h(ID_i \| x)$ و گواهینامه زمانی $TC_i = h(x \| RTS_i)$ را محاسبه می‌کند که RTS_i زمان ثبت SD_i است. سپس TA اطلاعات فوق را در حافظه امن SD_i قرار می‌دهد.

۵-۳- فاز ثبت ارائه‌دهندگان خدمات

این فاز نیز دقیقاً مانند فاز ثبت افزاره‌ها است و TA برای j امین ارائه‌دهنده خدمات یعنی UC_j ، ID_j را انتخاب کرده و RID_j و TC_j را محاسبه می‌کند. با این تفاوت که TA شناسه‌های مستعار تمام افزاره‌های مستقر در شبکه هوشمند و ثبت‌شده در TA که در فاز قبل ایجاد شدند را نیز در حافظه امن ارائه‌دهنده خدمات ثبت می‌کند.

۵-۴- فاز احراز اصالت متقابل و توزیع کلید

در این فاز، یک افزاره اندازه‌گیری هوشمند (SD_i) و یک ارائه‌دهنده خدمات (UC_j)، یکدیگر را مطابق شکل ۲ احراز اصالت کرده و یک کلید مشترک را به اشتراک می‌گذارند.

گام اول: SD_i ، مقدار تصادفی $u \in Z_p^*$ را انتخاب کرده و $U_i = u.G$ و $C_i = h(TC_i \| T_1) \oplus h(RID_i \| U_i \| T_1)$ را محاسبه می‌کند. سپس مهر زمانی فعلی T_1 را تولید کرده و پیام $\{U_i, C_i, T_1\}$ را از طریق کانال عمومی به UC_j ارسال می‌کند.

گام دوم: UC_j پس از دریافت پیام با بررسی $(T_1 - T_1^*) \le \Delta T$، مهر زمانی T_1 را در پیام تأیید می‌کند، جایی که ΔT حداکثر تأخیر در انتقال و T_1^* زمان دریافت پیام توسط UC_j است. اگر شرط برقرار باشد، UC_j، $D_j = C_i \oplus h(RID_i \| U_i \| T_1)$ را با استفاده از RID_i مربوط به افزاره i ام که در پایگاه داده خود ذخیره کرده، محاسبه می‌کند که در اصل با توجه به عبارت C_i، عبارت D_j برابر $h(TC_i \| T_1)$ می‌شود.

گام سوم: سپس UC_j مهر زمان فعلی T_2 و مقدار تصادفی $v \in Z_p^*$ را می‌سازد. بعدازآن، $W_j = v.U_i = (uv).G$ و $V_j = v.G$ را محاسبه کرده و کلید جلسه $SK_{ij} = h(W_j \| D_j \| h(RID_j \| TC_j \| T_2))$ را محاسبه می‌کند. سپس مقادیر $SKV_{ij} = h(SK_{ij} \| RID_i \| T_2)$ و $Z_j = h(RID_j \| TC_j \| T_2) \oplus h(RID_i \| U_i \| V_j \| T_2)$ را محاسبه کرده و پیام پاسخ تأیید اصالت $\{V_j, Z_j, SKV_{ij}, T_2\}$ را به SD_i از طریق کانال عمومی ارسال می کند.

گام چهارم: SD_i بعد از دریافت پیام با بررسی $(T_2 - T_2^*) \le \Delta T$، مهر زمانی T_2 در پیام را تائید می‌کند. اگر شرط برقرار نباشد، فاز خاتمه می‌یابد. در غیر این صورت، SD_i عبارات E_i، W_i'، و کلید جلسه مشترک با UC_j را به کمک روابط (۱)،(۲) و (۳) محاسبه می‌کند.

$$E_i = Z_j \oplus h(RID_i \| U_i \| V_j \| T_2) = h(RID_i \| TC_j \| T_2) \quad (۱)$$

$$W_i' = u.V_j = (uv).G \quad (۲)$$

$$SK_{ij}' = h(W_i' \| h(TC_i \| T_1) \| E_i) (= SK_{ij}) \quad (۳)$$

در ادامه SD_i، $SKV_{ij}' = h(SK_{ij}' \| RID_i \| T_2)$ را محاسبه و $SKV_{ij}' = SKV_{ij}$ را بررسی می‌کند. در صورت عدم برقراری شرط، فاز فوراً خاتمه می‌یابد. در غیر این صورت ، SD_i همچنان به تولید مهر زمانی فعلی T_3 و محاسبه $SKV_{ij}^* = h(SK_{ij}' \| RID_i \| V_j \| T_3)$ می‌پردازد. سپس پیام تأیید اعتبار احراز اصالت $\{SKV_{ij}^*, T_3\}$ را از طریق کانال عمومی به UC_j ارسال می‌کند.

گام پنجم: پس از دریافت پیام در زمان T_3، UC_j اعتبار مهر زمانی T_3 را با شرط $(T_3 - T_3^*) \le \Delta T$ بررسی می‌کند و در صورت عدم برقراری شرط مذکور، UC_j فاز را خاتمه می‌دهد. در غیر این صورت $SKV_{ij}^{**} = h(SK_{ij} \| RID_i \| V_j \| T_3)$ را محاسبه می‌کند و اگر تساوی $SKV_{ij}^{**} = SKV_{ij}^*$ برقرار باشد، SD_i و UC_j هر دو کلید $SK_{ij} = SK_{ij}'$ را برای ارتباطات امن آینده خود ذخیره می‌کنند.

SG device (SD_i)	UC_j
Select random secret $u \in Z_p^*$. Generate current timestamp T_1. Calculate $U_i = u.G$, $C_i = h(TC_i \| \|T_1) \oplus h(RID_i \| \|U_i \| \|T_1)$. $\langle U_i, C_i, T_1 \rangle$ (via public channel)	Verify if $\|T_1 - T_1^*\| \le \Delta T$? If so, calculate $D_j = C_i \oplus h(RID_i \| \|U_i \| \|T_1)$. Generate current timestamp T_2, random secret $v \in Z_p^*$ & compute $V_j = v.G$, $W_j = v.U_i = (uv).G$, $SK_{ij} = h(W_j \| \| D_j \| \| h(RID_j \| \| TC_j \| \| T_2))$, $SKV_{ij} = h(SK_{ij} \| \|RID_i \| \|T_2)$, $Z_j = h(RID_j \| \|TC_j \| \|T_2) \oplus h(RID_i \| \|U_i \| \|V_j \| \|T_2)$. $\langle V_j, Z_j, SKV_{ij}, T_2 \rangle$ (via public channel)
Check if $\|T_2 - T_2^*\| \le \Delta T$? Compute $E_i = Z_j \oplus h(RID_i \| \|U_i \| \|V_j \| \|T_2) = h(RID_j \| \|TC_j \| \|T_2)$, $W_i' = u.V_j = (uv).G$, $SK_{ij}' = h(W_i' \| \| h(TC_i \| \|T_1) \| \| E_i)$, $SKV_{ij}' = h(SK_{ij}' \| \|RID_i \| \|T_2)$. Check if $SKV_{ij}' = SKV_{ij}$? If so, generate current timestamp T_3 and compute $SKV_{ij}^* = h(SK_{ij}' \| \|RID_i \| \|V_j \| \|T_3)$. $\langle SKV_{ij}^*, T_3 \rangle$ (via public channel) Store session key SK_{ij}' $(= SK_{ij})$.	Check if $\|T_3 - T_3^*\| \le \Delta T$? If so, calculate $SKV_{ij}^{**} = h(SK_{ij} \| \|RID_i \| \|V_j \| \|T_3)$. Verify if $SKV_{ij}^{**} = SKV_{ij}^*$? Store session key SK_{ij} $(= SK_{ij}')$.

شکل ۲: احراز اصالت و تبادل کلید طرح [14]

۶- اعمال حمله منع سرویس به طرح نراج کومار و همکاران

همان‌طور که در بخش ۱ اشاره کردیم، این طرح در گام دوم هیچ‌گونه بررسی رو صحت‌وسقم پیام‌های دریافتی انجام نمی‌دهد و مهاجم یا مهاجمان می‌توانند با ارسال پیام‌های نادرست، بار محاسباتی زیادی را به ارائه‌دهنده خدمات اعمال کرده و موجب کند شدن شبکه و عدم خدمت‌رسانی صحیح به افزاره‌های مجاز گردند. در ادامه شرح دقیق حمله توضیح داده می‌شود.

مهاجم مطابق با فاز احراز اصالت در شکل ۲ پیام‌های تصادفی را تحت عناوین $U_i^{"}$ و $C_i^{"}$ تولید کرده و مهر زمانی هماهنگ با آن‌ها را تحت عنوان $T_1^{"}$ قرار داده و برای ارائه‌دهنده خدمات مدنظر ارسال می‌کند. در طرف دوم ارائه‌دهنده خدمات به‌محض دریافت پیام‌ها و بدون بررسی صحت پیام‌های دریافتی و تنها با چک کردن مهر زمانی، شروع به محاسبه $D_j^{"}$، $V_j^{"}$ و $W_j^{"}$ کرده و کلید $SK_{ij}^{"}$ را می‌سازد و همچنین پیام‌های $SKV_{ij}^{"}$ و $Z_j^{"}$ را نیز محاسبه کرده و به همراه پیام‌های $W_j^{"}$ ، $V_j^{"}$ و مهر زمانی $T_2^{"}$ برای مهاجم ارسال می‌کند. در ادامه روند کار پروتکل، مطابق با زیر بخش ۵-۴، ارائه‌دهنگان خدمات درنهایت در گام پنجم با بررسی تساوی $SKV_{ij}^{**}=SKV_{ij}^{*}$ و عدم برقراری آن، متوجه نادرست بودن پیام‌ها خواهد شد؛ ولی این عدم بررسی صحت پیام‌ها در گام دوم موجب اعمال بار محاسباتی زیاد و حتی موجب اعمال حمله منع سرویس توسط مهاجمان خواهد شد.

در بسیاری از پروتکل‌های ارائه‌شده، طراحی به‌گونه‌ای است که درگام دوم، صحت‌وسقم پیام‌های دریافتی با چک کردن عباراتی که درستی پیام‌ها را احراز می‌کند بررسی می‌شود تا جلوی اشغال شبکه توسط پیام‌های بی‌معنی که توسط مهاجم یا مهاجمان ارسال می‌شوند گرفته شود؛ و یا حتی سعی می‌شود در همان گام دوم عمل احراز اصالت طرف مقابل صورت پذیرد. به‌عنوان مثال می‌توان به طرح‌های [5,6]، [8,9]، [11,12]، [15-17] و همچنین طرح پاردپ کومار و همکاران که در ابتدای مقاله بررسی شد اشاره کرد.

۷- نتیجه‌گیری

در این مقاله پروتکل‌های پاردپ کومار و نراج کومار موردبررسی قرار گرفتند و با بررسی امنیت پروتکل‌ها، نشان داده شد طرح پاردپ کومار‌در برابر حمله ردگیری افزاره‌ها و برقراری صحیح گمنامی و طرح نراج کومار در برابر حمله منع سرویس آسیب‌پذیر هستند. برای بهبود هرکدام از طرح‌ها پیشنهادهای گوناگونی را می‌توان مطرح کرد که در مقاله‌های آینده به نحوه بهبود ضعف‌های مطرح شده و ارائه پروتکلی امن و سبک‌وزن، مناسب برای پیاده‌سازی در بستر شبکه هوشمند انرژی خواهیم پرداخت.

مراجع

[1] Liehuang Zhu, Meng Li, Zijian Zhang, Chang Xu, Ruonan Zhang, Xiaojiang Du, Nadra Guizani, “Privacy-Preserving Authentication and Data Aggregation for Fog-Based Smart Grid” *IEEE Communications Magazine*, Vol. 57, pp. 80 - 85, 2019.

[2] Wenye Wang, Zhuo Lu, “Cyber security in the Smart Grid: Survey and challenges” *Computer Networks*, Vol. 57, pp. 1344-1371, 2013.

[3] Pardeep Kumar, Yun Lin, Guangdong Bai, Andrew Paverd, Jin Song Dong, Andrew Martin. “Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues” IEEE Communications Surveys & Tutorials, Vol. 21, and Issue: 3 pp. 2886 - 2927, 2019.

[4] Muhammad Rizwan Asghar, György Dán, Daniele Miorandi, Imrich Chlamtac, “Smart Meter Data Privacy: A Survey” *IEEE Communications Surveys & Tutorials*, Vol. 19, Issue: 4, pp. 2820-2835, 2017.

[5] Vanga Odelu, Ashok Kumar Das, Mohammad Wazid, Mauro Conti, “Provably Secure Authenticated Key Agreement Scheme for Smart Grid” *IEEE Transactions on Smart Grid*, Vol. 9, Issue: 3, pp. 1900-1910, 2016.

[6] Yuwen Chen, José-Fernán Martínez, Pedro Castillejo, Lourdes López, “A Bilinear Map Pairing Based Authentication Scheme for Smart Grid Communications: PAuth” *IEEE Access*, Vol. 7, pp. 22633-22643, 2019.

[7] Hakan Kilinc, Tugrul Yanik, “A Survey of SIP Authentication and Key Agreement Schemes” *IEEE Communications Surveys & Tutorials*, Vol. 16, Issue: 2, pp. 1005 - 1023, 2014.

[8] Liping Zhang, Lanchao Zhao, Shuijun Yin, Chi-Hung Chi, Ran Liu, Yixin Zhang, “A lightweight authentication scheme with privacy protection for smart grid communications” *Future Generation Computer Systems*, Vol. 100, pp. 770 - 778, 2019.

[9] Jia-Lun Tsai, Nai-Wei Lo, “Secure Anonymous Key Distribution Scheme for Smart Grid” *IEEE TRANSACTIONS ON SMART GRID*, Vol. 7, NO. 2, pp. 906 - 914, 2016.

[10] R. Canetti and H, Krawczyk, “Analysis of key-exchange protocols and their use for building secure channels” *in Advances in Cryptology–EUROCRYPT*, Austria, pp. 453–474, 2001.

[11] Kh. Mahmood, Sh. Ashraf Chaudhry, H. Naqvi, S. Kumari, Xi. Li, Ku. Sangaiah, “An elliptic curve cryptography based lightweight authentication schemefor smart grid communication” *Future Generation Computer Systems*, Vol. 81, pp. 557-565, 2018.

[12] D. Abbasinezhad-Mood and M.Nikooghadam, “Design and hardware implementation of a security enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications” *Future Generation Computer Systems*, Vol. 84, pp. 47-57, 2018.

[13] Pardeep Kumar, A. Gurtov, M. Sain, A. Martin, P. Hoai, “Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks” *IEEE Transactions on Smart Grid*, Vol. 10, and Issue: 4, pp. 4349 - 4359, 2018.

[14] Neeraj Kumar, Ga. Singh Aujla, A. Kumar Das, M. Conti, “ECCAuth: Secure Authentication Protocol for Demand Reponse Management in Smart Grid Systems” *IEEE Transactions on Industrial Informatics*, (Early Access) 13 June 2019

[15] Sahil Garg, Kuljeet Kaur, Georges Kaddoum, François Gagnon, Syed Hassan Ahmed, Dushantha Nalin K. Jayakody, “A Lightweight and Secure Authentication Mechanism for Smart Metering Infrastructure” *publication in the IEEE Global Communications Conference*, Waikoloa: 2019.

[16] Alireza Esfahani; Georgios Mantas; Rainer Matischek; Firooz. Saghezchi; Jonathan Rodriguez, “A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment” *IEEE Internet of Things Journal*, Vol. 6, and Issue: 1, pp. 288 - 296, 2017.

[17] Xiong Li, Maged Hamada Ibrahim, Saru Kumari, Arun Kumar Sangaiah, Vidushi Gupta, Kim-Kwang, “Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks” *Computer Networks*, Vol. 129, Part 2, pp. 429 - 443, 2017.