ارائه یک طرح امضارمز فاقد گواهینامه‌ی مؤثر، برای ایجاد امنیت در ارتباطات کنتورهای هوشمند با گره متمرکز کننده داده در شبکه هوشمند برق

سیده معصومه سیدی، محمد حسین یغمایی مقدم
شرکت توزیع نیروی برق مشهد
مشهد، ایران
Yaghmaee@ieee.org, m.seyedi2010@gmail.com

چکیده — یکی از مهم‌ترین چالش‌ها در شبکه هوشمند برق، مفاهیم امنیتی و حفظ حریم خصوصی است. یکی از اجزای اصلی در شبکه هوشمند برق، کنتور هوشمند است. در واقع کنتور هوشمند، دروازه بین شبکه خانگی و شبکه خارج از خانه است و داده‌های مصرف انرژی را جمع آوری می‌کند و از طریق شبکه ارتباطی به سرور شرکت برق ارسال می‌نماید. تهدیدات و حملات زیادی بر روی کنتور هوشمند امکان پذیر است که حریم خصوصی مصرف کنندگان و صحت داده‌ها را به خطر می‌اندازد. راهکار پیشنهادی ما، برای حفظ حریم خصوصی و صحت داده‌ها در ارتباطات کنتور هوشمند، ارائه یک طرح امضارمز فاقد گواهینامه[1] است که طرح پیشنهادی فاقد محاسبات زوج سازی دوگانه[2] است. طرح پیشنهادی ما، ویژگی‌های محرمانگی، صحت، عدم جعل، عدم انکار، محرمانگی پیشروی پیام، اعتبار سنجی عمومی را فراهم می‌کند و نسبت به طرح‌های مشابه هزینه محاسباتی کمتری دارد و در برابر حمله تکرار و مردی در میانه مقاوم است.

واژه‌های کلیدی — سیستم اندازه‌گیری پیشرفته؛ رمزنگاری منحنی بیضوی؛ امضارمز فاقد گواهینامه.

۱. مقدمه

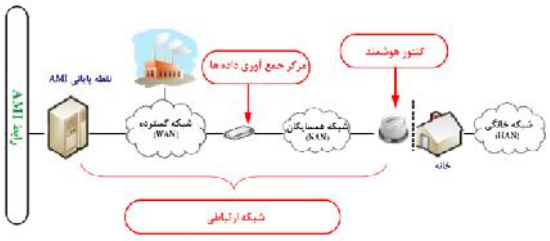
در شبکه هوشمند برق، ارتباطات دو طرفه‌ای بین کنتور هوشمند و شرکت برق برای قرائت دقیق کنتور و تعیین تعرفه وجود دارد. شبکه هوشمند برق متشکل از تعدادی زیر شبکه مانند شبکه خانگی[3](HAN)، شبکه همسایگان[4](NAN)، فراهم‌کنندگان سرویس، انتقال و توزیع است. یکی از اجزای کلیدی در شبکه هوشمند برق، سیستم اندازه‌گیری پیشرفته[5](AMI) است[۲].

زیرساخت اندازه‌گیری پیشرفته «AMI» عبارتند از یک سیستم اندازه-گیری و جمع آوری کامل، شامل کنتورهای هوشمند در محل مشتری؛ شبکه-های ارتباطی بین مشتری و یک ارائه دهنده خدمات، مانند صنعت گاز، آب یا برق؛ و سیستم‌های مدیریت و دریافت داده که اطلاعات موجود را برای ارائه دهنده خدمات فراهم می‌کنند[۳]. در شکل ۱ ساختار اندازه‌گیری پیشرفته(AMI) نشان داده شده است. رمزنگاری منحنی بیضوی «ECC»، یک رمزنگاری به روش کلید عمومی است. برای پروتکل‌های مبتنی بر منحنی بیضوی، فرض بر این است که پیدا کردن لگاریتم گسسته از یک نقطه تصادفی، بر روی منحنی بیضوی با توجه به یک نقطه پایه عمومی، غیر عملی باشد. اندازه منحنی بیضوی تعیین کننده سختی مسئله است. طرح (CLSC[6])،

[1] Certificateless Signcryption
[2] Bilinear Pairing

[3] Home Area Network
[4] Neighborhood Area Network
[5] Advanced Metering Infrastructure
[6] Certificateless signcryption

یکی از مهم‌ترین دستاوردهای رمزنگاری کلید عمومی فاقد گواهینامه است. طرح امضارمز[7]، به طور همزمان محرمانگی و صحت را به وسیله ترکیب رمزنگاری کلید عمومی و امضای دیجیتال فراهم می‌کند.



شکل ۱: ساختار اندازه گیری پیشرفته (AMI)

در طرح امضارمز، نه تنها محرمانگی پیام، احراز هویت، صحت، عدم جعل و عدم انکار فراهم می‌شود، بلکه محرمانگی پیشروی پیام و اعتبار سنجی عمومی نیز برآورده می‌شود. این روش هزینه کمتری را نسبت به روش‌های امضا و سپس رمزنگاری دارد. رمزنگاری کلید عمومی فاقد گواهینامه، برای حل مشکل مدیریت گواهینامه در روش زیرساخت کلید عمومی (PKI) و مشکل سپردن کلید در روش مبتنی بر شناسه(ID-Based) ارائه شده است. به طور کلی در روش امضارمز، از کلید عمومی گیرنده، برای تولید کلید جلسه استفاده می‌شود و پیام با استفاده از کلید جلسه رمزنگاری می‌شود و سپس از کلید خصوصی فرستنده، برای امضای پیام استفاده می‌شود و این دو مرحله در یک مرحله منطقی انجام می‌شود. گیرنده با دریافت پیام امضارمز شده، ابتدا با استفاده از کلید خصوصی خود، کلید جلسه را تولید می‌کند و متن واضح را بدست می‌آورد و سپس امضا را با استفاده از کلید عمومی فرستنده، اعتبار سنجی می‌کند.

طرح پیشنهادیِ ما، ارائه یک طرح امضارمز فاقد گواهینامه‌ی مؤثر، برای ایجاد امنیت در ارتباطات کنتور هوشمند با گره متمرکز کننده داده در شبکه هوشمند برق است، طرح پیشنهادیِ ما، مبتنی بر منحنی بیضوی است و فاقد محاسبات زوج سازی[8] است. ساختار مقاله به این ترتیب سازماندهی شده است که: در بخش دوم کارهای مرتبط، در بخش سوم روش پیشنهادی، در بخش چهارم ارزیابی طرح پیشنهادی و مقایسه با طرح‌های قبلی، و در نهایت در بخش پنجم نتیجه گیری بیان شده است.

۲. کارهای مرتبط

در [۱]، تهدیدات امنیتی و انواع حملات به کنتور هوشمند در شبکه هوشمند برق، مورد بررسی قرارگرفته است. [۲]، به تحلیل آسیب‌پذیری‌ها و تهدیدات در زیرساخت اندازه‌گیری پیشرفته می‌پردازد. در [۳]، کاربردهای AMI و ملاحظات امنیتی در شبکه خانگی (HAN) بیان می‌شود.از تکنولوژی Zigbee به دلیل مصرف کم انرژی و پیکربندی ساده آن، به عنوان بهترین راه حل برای شبکه HAN نام برده شده است. دراین مقاله، لوازم برقی هوشمند، بر اساس بار مصرفی دسته بندی می‌شوند و حملات Jamming، تکرار، جعل هویت لوازم برقی و انکار، در سطح HAN بررسی می‌شوند. در [۴]، اجزای شبکه هوشمند برق مانند(AMI)، شبکه‌های ارتباطی، سیستم مرکزی، متمرکز کننده داده و ... مورد بررسی قرار می‌گیرد.

شروع تحقیق و بررسی بر روی سیستم رمز نگاری منحنی بیضوی به دهه ۱۹۸۰ میلادی بر می‌گردد. منحنی‌های بیضوی که نقش مهمی در این سیستم‌های رمزنگاری بازی می‌کنند و اولین بار توسط میلر و کوبلیتز[۵]، معرفی شدند. ژنگ[۶]، اولین ارائه کننده تکنیک جدید امضارمز است که با هدف فراهم نمودن همزمان محرمانگی صحت ارائه شده است. این تکنیک، ترکیبی از امضای دیجیتال و الگوریتم رمزنگاری است. طرح اولیه ژنگ، مبتنی بر حل مسئله لگاریتم گسسته (DLP) است. در [۷]، یک طرح امضارمز، مبتنی بر منحنی بیضوی با صرفه جویی در هزینه محاسباتی ۵۸٪ و صرفه جویی در هزینه ارتباطی ۴۰٪ نسبت به طرح‌های امضا و سپس رمزنگاری ارائه شده است. طرح ارائه شده شامل ویژگی محرمانگی، صحت و عدم انکار است. این طرح مبتنی بر حل مسئله لگاریتم گسسته بر روی منحنی بیضوی(ECDLP) است. در [۸]، یک طرح امضارمز مبتنی بر شناسه(ID-Based) بر روی منحنی بیضوی، با هدف برقراری محرمانگی و صحت در شبکه های هوشمند برق ارائه شده است. مدل پیشنهادی شامل کنتور هوشمند، وسایل برقی هوشمند و سنسورهای نظارتی می‌باشد. در سال ۲۰۰۳، الریامی و پترسون [۹]، مفهوم رمزنگاری کلید عمومی فاقد گواهینامه، را معرفی کردند. برخلاف سیستم رمزنگاری کلید عمومی سنتی، رمزنگاری کلید عمومی فاقد گواهینامه، نیاز به گواهینامه برای ضمانت اعتبار کلیدهای عمومی ندارد و از طرف دیگر برای حل مشکل سپردن کلید، در روش‌های مبتنی بر شناسه (ID-Based) بکار می‌رود. طرح رمزنگاری کلید عمومی فاقد گواهینامه‌ی ارائه شده در [۹] مبتنی بر زوج سازی دوگانه بر روی سیستم رمزنگاری منحنی بیضوی است. مفهوم «CLSC» در سال ۲۰۰۸ [۱۰] معرفی شد. بیشترین تمرکز طرح‌های ارائه شده در [۱۱،۱۰] بر اساس زوج سازی

[7] Signcryption
[8] pairing

دوگانه است. در[۱۳,۱۲]، طرح‌های «CLSC» ارائه شده، فاقد محاسبات زوج سازی است و این دو طرح مبتنی بر حل مسئله لگاریتم گسسته (DLP) هستند. طرح [۱۳]، نیاز به ۶ عملیات به توان رسانی پیمانه‌ای، برای فرستنده و ۸ عملیات به توان رسانی پیمانه‌ای، برای گیرنده دارد و طرح [۱۲]، ۳ عملیات به توان رسانی پیمانه‌ای، برای فرستنده و ۲ عملیات به توان رسانی پیمانه‌ای، برای گیرنده دارد. رمزنگاری مبتنی بر زوج سازی بین عناصر دو گروه است و حاصل گروه سوم است. اگر دو گروه یکسان باشد زوج سازی متقارن و در غیر این‌صورت نامتقارن است. در رمزنگاری منحنی بیضوی، زوج سازی دوگانه توابعی هستند که برای نگاشت یک جفت از نقاط منحنی بیضوی به یک عنصر از گروه ضربی بر روی میدان گالوا و برای کاهش سختی حل مسائل بکار می‌رود و باعث افزایش سرعت محاسبات می-شود[۱۵]. اما هزینه محاسباتی آن، هنوز باقی مانده است که بسیار وقت گیر است[۱۳,۱۲]. به طور کلی هزینه محاسباتی زوج سازی ۲۰ برابر عملیات ضرب اسکالر بر روی منحنی بیضوی است[۱۴].

۳. روش «CLSC» پیشنهادی

در این قسمت ما یک طرح جدید امضارمز فاقد گواهینامه، مبتنی بر منحنی بیضوی و فاقد محاسبات زوج سازی دوگانه را ارائه می‌دهیم. کلید عمومی و خصوصی هر موجودیت در طرح پیشنهادی ما، بر اساس رمزنگاری کلید عمومی فاقد گواهینامه، تولید می‌شود و انتقال داده بین موجودیت‌ها، براساس تکنیک امضارمز است. طرح پیشنهادی شامل ۳ موجودیت است که عبارتند از: مرکز تولید کلید[۹](KGC)، فرستنده و گیرنده.

ما در طرح پیشنهادی، برای اجتناب از حمله تکرار از برچسب زمانی، استفاده کرده‌ایم.در طرح پیشنهادی فرض شده است که زمان جاری دقیق، توسط یک سرور برچسب زمانی تعیین می‌شود و هم‌زمان سازی زمان، بین سرور KGC، فرستنده و گیرنده وجود دارد.

در طرح پیشنهادی ما، فرض شده است که هر دستگاهی (مانند کنتور هوشمند، گره متمرکز کننده داده، سرور KGC، ...) دارای یک شماره شناسایی ماشین منحصر به فرد مانند شماره سریال ساخت یکتا است. در ابتدا هر دستگاهی باید برای دریافت کلید خصوصی جزئی خود به KGC، مراجعه کند تا بتواند پیام‌های دریافتی را رمزگشایی و یا پیام را امضا کند. KGC، یک کلید اصلی دارد که، آن‌را به صورت سری نگه می‌دارد و با استفاده از آن کلید خصوصی جزئی هر دستگاه تولید می‌شود.

۳.۱. نمادگذاری‌ها در طرح پیشنهادی

در *جدول ۱* نمادگذاری طرح پیشنهادی نشان داده شده است.

جدول ۱: نمادگذاری‌ها درطرح پیشنهادی

نماد گذاری	
علائم	*توضیح*
p,n	دو عدد اول بزرگ
GF(q)	میدان گالوا
E	یک منحنی بیضوی بر روی میدان گالوای F_q
P	نقطه پایه در منحنی بیضوی
$H_1(0)$	تابع درهم سازی برای تبدیل شناسه به عددی در بازه [1-n-1]
$H_2(0)$	تابع درهم سازی برای پیام‌ها با طول m
ID_i	شناسه موجودیت i
(s,Q)	کلید خصوصی و کلید عمومی KGC
d_i	کلید خصوصی جزئی i
(SK_i,Q_i)	کلید خصوصی و کلید عمومی i
t_1	برچسب زمانی

۳.۲. روش پیشنهادی

در طرح پیشنهادی شامل ۸ الگوریتم است که عبارتند از:

۱)آماده سازی سیستم:در این الگوریتم پارامترهای عمومی منحنی بیضوی و یک جفت کلید اولیه برای هر دستگاه در شبکه هوشمند برق تعیین می-شود. مراحل این الگوریتم به شرح ذیل می‌باشد:

- انتخاب اندازه و نوع میدان گالوا GF(q). q می‌تواند به دو صورت بکار رود:
  - اگر $q = p$ انتخاب شود، باید p یک عدد اول بزرگ باشد. برای پیاده‌سازی نرم‌افزاری از این میدان استفاده می‌شود.
  - اگر $q = 2^k$ انتخاب شود (k بیان کننده اندازه میدان است) از آنجایی که جمع در این میدان گالوا بدون رقم نقلی انجام می-شود، برای پیاده‌سازی سخت افزاری مناسب است.
- انتخاب دو پارامتر $a,b \in q$، به منظور تعریف معادله‌ی منحنی بیضوی E روی میدان GF(q) در (۱) نشان داده شده است:

$$y^2 + xy = x^3 + ax^2 + b \qquad (۱)$$

[9] Key Generation Center

- مشخص ساختن نقطه‌ی اساسی (P) برای منحنی بیضوی مورد نظر (منظور از نقطه‌ی اساسی، نقطه‌ای روی منحنی بیضوی است که بیشترین مرتبه را داشته باشد).
- تعیین مرتبه‌ی نقطه‌ی اساسی منحنی بیضوی (n).
- ۲ تابع درهم سازی امن: m ، طول پیامی است که برای عملیات امضارمز، بکار می‌رود. توابع درهم سازی مانند: MD5، SHA، HMAC

$$H_1 : \{0,1\}^* \to Z_n^*$$

$$H_2 : \{0,1\}^m \to Z_n^*$$

- KGC، عدد تصادفیs را در بازه‌ی [1-n-1]، به عنوان کلید اصلی انتخاب می‌کند.
- KGC، کلید عمومی خود را به صورت زیر محاسبه می‌کند:

$$Q_{KGC} = s.P \qquad (۲)$$

- خروجی این الگوریتم Params و کلید اصلی s است و Params، به صورت عمومی منتشر می‌شود. Params، شامل پارامترهای عمومی سیستم است.

$$Params = \{F_q, E/F_q, p, Q_{KGC}, H_1, H_2\}$$

۲) تولید کلید اولیه در هر دستگاه:

در طی ساخت یک دستگاه (کنتور هوشمند، گره متمرکز کننده داده و ...) یک جفت کلید اولیه به همراه پارامترهای سیستم در هر دستگاهی قرار داده می‌شود. این دو کلید $ID-DR_i$ و $KGC-DR_i$ می‌نامیم. کلید $ID-DR_i$، شماره شناسایی یکتای هر دستگاه است. کلید $KGC-DR_i$، در (۳) محاسبه می‌کند: KGC، عدد تصادفی s_1را در بازه‌ی [1-n-1] انتخاب می‌کند.

$$KGC-DR_i = s + H_1(ID-DR_i).s_1 \qquad (۳)$$

در شبکه هوشمند برق، فرستنده قبل از برقراری ارتباط با گیرنده، برای دریافت کلید خصوصی جزئی خود به KGC، مراجعه می‌کند و برای برقراری ارتباط اولیه از کلیدهای اولیه استفاده می‌کند. این مرحله فقط یک‌بار و در کارخانه سازنده و یا شرکت برق توسط KGC، انجام می‌شود.

۳) ***تولید کلید خصوصی جزئی:*** فرستنده (i)، برای دریافت کلید خصوصی جزئی خود باید با KGC، ارتباط کند و KGC، کلید خصوصی جزئی را از طریق کانال امن برای i ارسال می‌کند. برای دریافت کلید خصوصی جزئی مراحل زیر انجام می‌شود:

۱- فرستنده یک پیام حاوی $ID-DR_i$ و Params را با کلید، $KGC-DR_i$ امضا می‌کند و پیام امضا شده را به KGC، ارسال می‌کند که این اقدامات طبق مراحل زیر انجام می‌شود:

- انتخاب عدد تصادفی $r \in [1-n-1]$
- محاسبه‌ی نقطه R: $R = r \times P = (x_1, y_1)$
- $v = x_1 \bmod n$، اگر $v = 0$ باشد بازگشت به مرحله اول.
- پیام: $m = (params \,||\, ID-DR_i)$
- تولید چکیده پیام: $e = H_2(m)$
- تولید امضا: $Sig = (vKGC-DR_i + re) \bmod n$
- ارسال (m,R,Sig) به KGC

۲- KGC، پس از دریافت Sig، امضا را اعتبار سنجی می‌کند:

- با داشتن نقطه R، محاسبه: $v = x_1 \bmod n$
- تولید چکیده پیام: $e = H_2(m)$
- اعتبار سنجی امضا: $Sig \times P - R \times e = vKGC - DR_i \times P$

۳- در صورت صحیح بودن تساوی،KGC، کلید خصوصی جزئی d_i را محاسبه می‌کند.

- محاسبه $Z_i = H_1(ID-DR_i)$.
- انتخاب عدد تصادفی $y \in [1, n-1]$ و محاسبه $Y = y \times P$
- تولید کلید خصوصی جزئی برای(i): $d_i = s + Z_i . y$

۴- KGC، d_i را با کلید $ID-DR_i$ رمزنگاری می‌کندو پیام رمزشده را با کلید خصوصی خودش امضا می‌کند و برای (i) ارسال می‌کند.

$$d_i^{'} = E_{ID-DR_i}(d_i)$$

امضای $d_i^{'}$ مانند مرحله ۱ است و پیام امضا شده را Sig_1می نامیم.

۵- i، پس از اعتبار سنجی امضا Sig_1، اقدامات زیر را انجام می‌دهد.

- رمزگشایی پیام دریافتی $d_i = E_{ID-DR_i}(d_i^{'})$
- اعتبار سنجی صحت کلید خصوصی جزئی دریافتی:

$$d_i \times P = Q_{KGC} + Y \times H_1(ID - DR_i)$$

جفت کلید اولیه‌ی هر دستگاه فقط یک‌بار و برای دریافت کلید خصوصی جزئی بکار می‌رود. KGC، استفاده مجدد از جفت کلید اولیه را نادیده می‌گیرد. الگوریتم ۱ تا ۳ به وسیله KGC، اجرا می‌شود. الگوریتم ۴ تا ۸ توسط کاربر اجرا می‌شود.

۴) *تعیین مقدار سری:* انتخاب عدد تصادفی $x_i \in [1, n-1]$.

۵) *تعیین کلید خصوصی کامل:* از ترکیب کلید خصوصی جزئی و مقدار سری، کلید خصوصی کامل تولید می‌شود و این قسمت توسط کاربر اجرا می‌شود. $sk_i = x_i + d_i$

۶) *تعیین کلید عمومی:* کلید عمومی به صورت $Q_i = (x_i + d_i) \times p$ تولید می‌شود.

۷) ***Signcrypt***: در این مرحله، برای ارسال پیام از کنتور هوشمند به گره متمرکز کننده داده یا برعکس عملیات زیر انجام می‌شود. در این قسمت، فرض می‌کنیم که فرستنده A و گیرنده B است. A، متن امضارمز شده (C, R, S, t_1) را طبق مراحل زیر تولید می‌کند:

۱. انتخاب عدد تصادفی $r \in [1, n-1]$

۲. محاسبه: $R = r \times P = (x_1, y_1)$

۳. $v = x_1 \bmod n$ اگر v=0 باشد بازگشت به مرحله اول.

۴. استفاده از توابع درهم سازی برای تبدیل برچسب زمانی به یک عدد: $T_A = H_1(t_1) \bmod n$.

۵. محاسبه کلید جلسه: $L = T_A.r \times Q_B = (k_A, j_A)$.

۶. با استفاده از الگوریتم رمزنگاری متقارن AES، متن اصلی را رمزنگاری می‌کنیم. K_A، مختصات x، نقطه L است که در مرحله ۴ تولید شده است.

$$C = E_{k_A}(m)$$

۷. محاسبه چکیده پیام: $e = H_2(M \| T_A \| ID_A \| ID_B)$.

۸. محاسبه امضا: $S = (vsk_i + re) \bmod n$

۹. ارسال $\pm = (C, R, S, t_1, ID_A)$ به B.

۸) ***Unsigncrypt***: B، پس از دریافت $\pm = (C, R, S, t_1, ID_A)$، متن رمز شده C را، با استفاده از الگوریتم AES و با استفاده از کلید جلسه k، رمزگشایی می‌کند و سپس امضا را برای صحت پیام ارسالی، اعتبار سنجی می‌کند. گیرنده در این قسمت، مراحل زیر را انجام می‌دهد:

۱. با داشتن نقطه R، محاسبه $v = x_1 \bmod n$

۲. محاسبه $T_A = H_1(t_1) \bmod n$ و $T_B = H_2(t_2) \bmod n$

در صورتی که $0 < T_B - T_A < \sim$ باشد، رمزگشایی پیام و اعتبار سنجی امضا انجام می‌شود. ~، تأخیر زمانی بین ارسال و دریافت پیام در لینک ارتباطی است. اگر اختلاف زمانی بیشتر از ~ شود، متن امضا رمز شده، غیر قابل قبول است.

۳. محاسبه کلید جلسه: $L = R \times sk_B.T_A = (k_B, j_B)$.

۴. با استفاده از الگوریتم AES، متن رمز شده را رمزگشایی می‌کنیم: $m = D_{k_A}(C)$.

۵. محاسبه چکیده پیام: $e = H_2(M \| T_A \| ID_A \| ID_B)$.

۶. اعتبار سنجی: $SP - \mathrm{Re} = vQ_A$.

۷. در صورت صحت رابطه ۶، به این نتیجه می‌رسیم که پیام از منبع معتبری ارسال شده و جعلی نیست، در غیر این صورت الگوریتم علامت $\perp$ به عنوان خروجی بر می‌گرداند.

۴. ارزیابی و تحلیل

طرح پیشنهادی۷ ویژگی امنیتی را فراهم می‌کند. بیشتر این نتایج مبتنی بر حل مسئله لگاریتم گسسته بر روی منحنی بیضوی(ECDLP) است که این مسئله بسیار سخت است.

۴.۱. امنیت روش پیشنهادی

۱) *محرمانگی:* در طرح ما، اگر مهاجم بخواهد متن اصلی(M) را بدست آورد، نیاز به رمزگشایی متن رمز شده(C)، با کلید مخفی k_A دارد. کلید مخفی k_A، مختصات x نقطه L است و برای استخراج کلید مخفی k_A، نیاز به حل مسائل ECDLP است. در صورتی که مهاجم بخواهد نقطه‌ی L را از روی (۴) بدست آورد، باید در ابتدا پارامتر مخفی r را از (۵) بدست آورد. با توجه به این که مهاجم، فقط Q_B و P را می‌داند، بنابراین ملزم به حل مسئله (ECDLP) است که یک مسئله بسیار دشوار است.

$$L = T_A.r \times Q_B = (k_A, j_A) \quad (۴)$$

$$R = r \times P = (x_1, y_1) \quad (۵)$$

۲) *احراز هویت:* گیرنده پس از دریافت متن رمز شده (C) و رمزگشایی آن، متن اصلی (M) را بدست می‌آورد. گیرنده می‌تواند از (۶) برای احراز هویت پیام دریافتی استفاده کند. اگر تساوی در(۶)، برقرار باشد، آنگاه گیرنده از عدم تغییر پیام در فرایند انتقال اطمینان حاصل می‌کند. بنابراین، طرح پیشنهاد در برابر حمله مردی در میانه (MITM) مقاوم است.

$$SP - \mathrm{Re} = vQ_A \quad (۶)$$

۳) *صحت:* صحت طرح پیشنهادی توسط (۷) قابل اثبات است.

$$L_A = T_A.r \times Q_B = T_A.r \times (x_B + d_B) \times P = T_A.r(x_B + s + yZ_B) \times P$$
$$L_B = R \times sk_B.T_A = r \times P \times (x_B + d_B) \times T_A = T_A.r(x_B + s + yZ_B) \times P \quad (۷)$$

۴) *عدم جعل:* در طرح ما، مهاجم نمی‌تواند مقادیر معتبر (M, R, S) را بدون دانستن کلید خصوصی فرستنده جعل کند. فرض کنید که مهاجم (M', R, S') جعلی را تولید کرده است. (M', R, S') جعلی باید شرایط (۸) را برآورده کند. مهاجم باید چکیده پیام e' و امضای S' را برای متن M' از (۹) و (۱۰) بدست آورد. با توجه به این که مهاجم پارامتر مخفی v را ندارد، نمی‌تواند S' صحیح را تولید کند. اگر مهاجم بخواهد پارامتر تصادفی و مخفی v، را از رابطه $R = r \times G$ بدست آورد، باید مسئله ECDLP را حل نماید که بسیار دشوار است. بنابراین، طرح پیشنهادی در برابر حمله جعل مقاوم است.

$$S'P - R'e' = vQ_A \quad (۸)$$

$$e = H_2(M' \| T_A \| ID_A \| ID_B) \quad (۹)$$

$$S' = (vsk_i + re') \bmod n \quad (۱۰)$$

۵) *عدم انکار:* اثبات این ویژگی مانند عدم جعل است.

۶) *محرمانگی پیشرو:* محرمانگی پیشروی پیام به این معنی است که اگر کلید خصوصی فرستنده، مورد تهدید قرار گیرد، مهاجم نتواند پیام‌های ارسال شده قبلی را بازیابی کند. مهاجم برای بدست آوردن متن اصلی M، نیاز به رمزگشایی متن رمز شده C با استفاده از کلید مخفی k_A، دارد که، نیاز به حل مسئله(ECDLP) دارد که، بسیار دشوار است.

۷) *اعتبار سنجی عمومی:* در طرح ما، هر شخصی (M, R, S, t_1) و کلید عمومی فرستنده را داشته باشد، می‌تواند اعتبار سنجی پیام ارسالی را توسط (۶) انجام دهد.

۴.۲ هزینه محاسباتی روش پیشنهادی

در این قسمت به ارزیابی طرح پیشنهادی «CLSC»، می‌پردازیم. تمام نمادهایی که برای مقایسه و سنجش به کار رفته، در جدول ۲ نشان داده شده است. در *جدول* ۳ پیچیدگی زمانی اجرای واحدهای عملیاتی مختلف بر حسب زمان اجرای ضرب پیمانه‌ای در[۵] مشخص شده است.

جدول ۲: نمادگذاری‌ها درطرح پیشنهادی

نماد	تعریف
T_{MUL}	پیچیدگی زمانی برای اجرای ضرب پیمانه‌ای
T_{EXP}	پیچیدگی زمانی برای اجرای به توان رسانی پیمانه‌ای
T_{ADD}	پیچیدگی زمانی برای اجرای جمع پیمانه‌ای
T_{EC_MUL}	پیچیدگی زمانی برای اجرای ضرب اسکالر
T_{EC_ADD}	پیچیدگی زمانی برای اجرای جمع نقطه‌ی منحنی بیضوی
T_{INV}	پیچیدگی زمانی برای اجرای معکوس در میدان

جدول ۳: پیچیدگی زمانی [۵]

واحد عملیاتی	بر حسب ضرب پیمانه‌ی
T_{EXP}	$240T_{MUL}$
T_{ADD}	ناچیز و قابل چشم پوشی
T_{EC_MUL}	$29T_{MUL}$
T_{EC_ADD}	$0.12T_{MUL}$
T_{INV}	$3T_{MUL}$

در *جدول* ۴ *پیچیدگی زمانی* روش پیشنهادی با طرح‌های قبلی مقایسه شده است. ابتدا مجموع هزینه‌های زمانی مورد نیاز، با توجه به زمان اجرای هر کدام از عملگرها برای طرح‌های مختلف مشخص می‌شود. سپس با توجه به *جدول* ۳ تمام زمان‌ها، بر حسب زمان لازم برای اجرای ضرب پیمانه‌ای بیان می‌شود. با توجه به *جدول* ۴، طرح پیشنهادی نسبت به طرح-های[۱۳,۱۲,۱۱,۸]، کمترین پیچیدگی زمانی و هزینه محاسباتی را در Signcryption و Unsigncryption دارد. به علاوه طرح پیشنهادی ما، نیاز به محاسبات زوج سازی ندارد، اما طرح‌های [۱۳,۸] که مبتنی بر زوج سازی هستند، در طرف فرستنده و گیرنده هزینه محاسباتی زیادی را تحمیل می-کنند. به طوری که این محاسبات،۲۰ برابر عملیات ضرب معمولی بر روی منحنی بیضوی هزینه دارند. مزیت دیگر طرح پیشنهادی ما، فاقد گواهینامه

بودن آن است که این عامل باعث می‌شود سربار ارتباطی که وارسی گواهینامه‌ها در طرح‌های[۷,۶] در هر نشست به فرستنده و گیرنده تحمیل می‌کند، حذف شود. علاوه بر آن طرح ما، در برابر حمله تکرار و حمله مردی در میانه، مقاوم است.

جدول۴: مقایسه پیچیدگی زمانی طرح پیشنهادی با طرح‌های ارائه شده

مرجع	پیچیدگی زمانی		بر حسب T_{MUL}	
	SG	UG	SG	UG
[۶]	$T_{EXP}+T_{INV}+T_{ADD}$	$2T_{EXP}+2T_{MUL}$	T_{MUL} 243	538 T_{MUL}
[۷]	$T_{EC-MUL}+T_{INV}+T_{MUL}+T_{ADD}$	$2T_{EC-MUL}+2T_{MUL}+T_{EC-ADD}$	33 T_{MUL}	60.12 T_{MUL}
[۸]	$3T_{EC-MUL}+T_{MUL}+T_{ADD}+2pa$	$4T_{EC-MUL}+3pa$	88 $T_{MUL}+2pa$	116 $T_{MUL}+3pa$
[۱۱]	$3T_{EXP}$	$2T_{EXP}$	$720T_{MUL}$	$538T_{MUL}$
[۱۲]	$6T_{EXP}$	$8T_{EXP}$	1440 T_{MUL}	1920 T_{MUL}
[۱۳]	$T_{EC-MUL}+2T_{MUL}+3T_{ADD}+pa$	$4T_{EC-MUL}+pa$	31 T_{MUL} +pa	116 T_{MUL} +3pa
طرح ما	$2T_{EC-MUL}+3T_{MUL}+T_{ADD}$	$4T_{EC-MUL}+T_{MUL}$	61 T_{MUL}	T_{MUL} 117

۵. نتیجه گیری

در این مقاله، ما یک طرح جدید امضارمز فاقد گواهینامه‌ی مبتنی بر منحنی بیضوی «CLSC» را ارائه دادیم. طرح پیشنهادی برای ایجاد امنیت در ارتباطات کنتور هوشمند و گره متمرکز کننده داده در سطح NAN، در شبکه هوشمند برق مناسب است. طرح پیشنهادی ما نیاز به محاسبات اضافه برای گواهینامه ندارد و نسبت به طرح‌های[۷,۶] که مبتنی بر زیر ساخت کلید عمومی هستند، بار مخابراتی کمتری دارد. علاوه بر این طرح پیشنهادیِ ما، مبتنی بر زوج سازی نیست. به دلیل آن که عملیات زوج سازی بر روی منحنی بیضوی بسیار پرهزینه است، طرح ما نسبت به طرح‌های[۱۳,۸] هزینه محاسباتی کمتری دارد. امنیت طرح پیشنهادی ما، بر اساس حل مسئله لگاریتم گسسته بر روی منحنی بیضوی است. طرح پیشنهادی ما، برای «Signcryption»، نیاز به دو عملیات ضرب نقطه‌ای، سه عملیات ضرب پیمانه‌ای و یک عملیات جمع پیمانه‌ای دارد و برای «Unsigncryption»، به چهار عملیات ضرب نقطه‌ای و یک عملیات ضرب پیمانه‌ای نیاز دارد.

منابع

[1] S. Florian and M. Zhendong,” Attack Vectors to Metering Data in Smart Grids under Security Constraints”,in 36th International Conference on - Computer Software and Applications Workshops, IEEE pp134-139, 2012.

[2] S. Florian ,M. Zhendong, B.Thomas and G.Helmut ”A Survey on Threats and Vulnerabilities in Smart Metering Infrastructur”,in Science Direct,Elsevier, p.8, 2012.

[3] V. Araavinthan, V. Namboodiri, S. Sunku,W. Jewell and Fellow ,”Wireless AMI application and security for controlled home area networks”, in Power and Energy Society General Meeting, IEEE,2011.

[4] F. Tony and M.justin,”Securing The Smart Grid Next Generation Power Grid Security”,Elsevier,pp. 19-43, 2011.

[5] K.Neal,M. ALFRED, v. Scott,” The state of elliptic curve cryptography”. Designs, Codes and Cryptography 2000: p. 173-193.

[6] Z. Yuliang, “Digital signcryption or how to achieve Cost(Signature & Encryption) _ Cost(Signature)+ Cost(Encryption)”, in: dvances in Cryptology—Crypto_97LNCS 1294, Springer-Verlag, pp. 165–179, 1997.

[7] Z. Yuliang and I. Hideki,”How to construct efficient signcryption schemes on elliptic curves”,in Elsevier Science B.C. 1998.

[8] S. Hayden,.H.M. Sammy,L.Edmund and K.Lui,”Zero-configuration Identity-based Sign-cryption Scheme for Smart grid”,International Conference on Smart Grid Communications, IEEE,pp.321-326,2010.

[9] S.AlRiyami and k.Paterson ,”Certificateless public key cryptography”. Advances in Cryptology (ASIACRYPT 2003), Springer-Verlag, LNCS, p. 452-473.

[10] M.Farshim and P.Barbosa, “Certificateless signcryption”. ACM Symposium on Information, Computer and Communications Security (ASIACCS 2008), 2008: p. 369-372.

[11] J.Xiaofei, “Provably Secure Certificateless Signcryption Scheme without Pairing”, in International Conference on Electronic & Mechanical Engineering and Information Technology,2011. p. 4753-4756.

[12] X.Wenjian and Z.Zhang,”Certificateless Signcryption without Pairing”. Cryptology ePrint Archive: Report 2010/187, Available from: http://eprint.iacr.org/2010/187.pdf.

[13] L.Fagen, S.Masaaki and T.Tsuyoshi,” Certificateless hybrid signcryption”. Elsevier Science Direct, 2013: p: 324–343.

[14] H.Debiao , J.Chen and R. Zhang. “An effient identity-base blind signature scheme with out billinear pairings”. Computer and Electical Engineering Elsevier,2011, 444-450. doi: 10.1016.

[15] S.Caroline.”Privacy Enhanced Protocols using Pairing Based Cryptography”, (January, 2010).