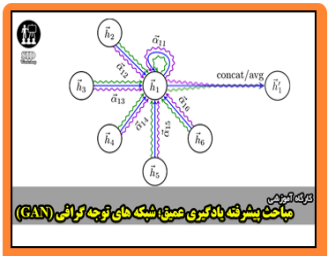
کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین مکالمه روزمره انگلیسی

کارگاه آنلاین آموزش استفاده از وب آو ساینس



مباحث پیشرفته یادگیری عمیق؛
شبکه های توجه گرافی
(Graph Attention Networks)

ارائه مکانیزم احراز اصالت در پست‌های برق مبتنی بر استاندارد IEC61850

نسترن اکبری، محمدحسین یغمایی مقدم، داود نوری
شرکت توزیع نیروی برق شهرستان مشهد
مشهد – ایران

چکیده — با توجه به گسترش شبکه‌های هوشمند برق و استفاده از زیرساخت‌های اترنت و اینترنت در سیستم‌های اتوماسیون پست مبتنی بر استاندارد IEC 61850، امکان بروز حملات سایبری افزایش یافته است. احراز اصالت که یکی مکانیزم‌های مهم امنیتی است، جزء نیازمندی‌های اصلی و اساسی در سیستم‌های اتوماسیون پست مبتنی بر استاندارد IEC 61850 به‌حساب می‌آید زیرا می‌توان از این مکانیزم برای سنجش صحت و اصالت پیام‌ها و هم‌چنین تشخیص بروز خطا در سیستم استفاده کرد. علی رغم اهمیت احراز اصالت در اتوماسیون‌های پست مبتنی بر استاندارد ۶۱۸۵۰، در حال حاضر توجه چندانی به این مکانیزم امنیتی مهم نشده است. به علاوه روش‌های ارائه شده تاکنون مشکلاتی از قبیل پیچیدگی محاسباتی بالا، زیاد بودن طول کلید و امضاء، عدم توجه به ارتباطات چندپخشی و غیره دارند.

در مکانیزم احراز اصالت پیشنهادی در این مقاله مشکلات قبلی تا حد امکان رفع شده است و مکانیزم کارایی برای احراز اصالت تک پخشی و چندپخشی در سیستم‌های اتوماسیون پست مبتنی بر استاندارد IEC61850 ارائه شده است. در روش پیشنهادی ما، سایز امضاء نسبت به روش‌های پیشین $\frac{1}{k}$ کاهش یافته است که نتیجه‌ی آن کاهش قابل توجه پهنای باند مورد استفاده ، کاهش هزینه‌ی اعتبارسنجی و حافظهٔ مورد نیاز در سمت گیرنده شده است.

واژه‌های کلیدی — شبکه‌های هوشمند برق؛ سیستم اتوماسیون پست؛ IEC 61850؛ امنیت؛ احراز اصالت

۱. مقدمه

شبکه‌های هوشمند با اجتماع شبکه‌های برق به‌وجود می‌آیند. در این شبکه‌ها به دلیل استفاده از تکنولوژی‌های ارتباطی امکان مدیریت کارای شبکه‌ها فراهم شده است. از طرفی شبکه‌های ارتباطی نقشی کلیدی در پایداری و عملکرد شبکه‌های هوشمند برق ایفا می‌کنند [۱-۳]. به همین دلیل، استاندارد IEC 61850 به پست‌ها اضافه شد و ارتباطات داخلی پست‌ها، ارتباطات خارجی بین پست‌ها و سیستم اسکادا را تحت تأثیر قرار داد[۴]. هدف اصلی در استفاده از IEC 61850 رفع مشکلات همگام‌سازی دستگاه‌های پست می‌باشد، لذا در این استاندارد به مسائل امنیتی توجه چندانی نشده است. از طرفی سیستم‌ها و شبکه‌های برق متفاوت از محیط ایمن اینترنت می‌باشند به طوریکه به عنوان مثال بروز حمله منع سرویس در شبکه ارتباطی سیستم برق اثرات بسیار مخربی بر شبکه خواهد گذاشت[۵].

باید توجه داشت پست‌های برق اهمیت بسیار زیادی دارند؛ هسته‌ی اتوماسیون پست‌ها، سیستم‌های ارتباطی هوشمندی هستند که تمام اجزاء سیستم را به صورت کارا به یکدیگر متصل می‌کنند در نتیجه حمله به این ساختار ارتباطی سبب نقض و به خطر افتادن امنیت ملی و اقتصادی می‌شود.

در این سیستم‌های ارتباطی هوشمند، ارتباطات چندپخشی نقشی کلیدی دارند، زیرا امکان ارتباط بین یک فرستنده و چندین گیرنده را به صورت کارا فراهم می‌کنند. اگرچه احراز اصالت چندپخشی در اینترنت و شبکه‌های حسگر بیسیم [۶] به طور گسترده‌ای مورد مطالعه قرار گرفته است، اما به مسأله احراز اصالت چندپخشی در پست‌های برق توجه چندانی نشده است.

از جمله پیام‌های چندپخشی می‌توان به داده‌های اندازه‌گیری شده یا فرامین کنترلی اشاره کرد. به علاوه قابل ذکر است که در پست‌های برق از ارتباطات چندپخشی برای ارسال پیام‌های بحرانی مثل پیغام‌های خطا در شبکه‌های محلی پست استفاده می‌شود و با توجه به اهمیت این پیام‌ها، پیام‌ها باید در مدت زمان بسیار کوتاهی به گیرنده‌ها که قطع کننده‌های جریان هستند ارسال شوند[۷]. احراز اصالت این پیام‌ها اهمیت بسیار زیادی دارد زیرا با احراز اصالت آن‌ها، هر گیرنده می‌تواند تشخیص دهد آیا پیام ارسال شده از فرستنده خاصی بوده است یا خیر وآیا پیام در بین راه تغییر کرده است یا نه و حتی می‌توان بروز خطا در سیستم را تشخیص داد. در صورتیکه عمل احراز اصالت انجام نشود، مهاجم می‌تواند به‌راحتی پیام‌های ارسال شده را تغییر دهد یا آن‌ها را جعل کند و یا حتی یک پیام قدیمی را مجدداً ارسال نماید[۷].

همانگونه که ذکر شد علی‌رغم اهمیت احراز اصالت چندپخشی در پست‌ها، به دلیل وجود نیازمندی‌ها و محدودیت‌های منحصر به فرد پست‌های برق به اندازه‌ی کافی به این مسأله توجه نشده است. به این دلیل که بسیاری از پیام‌های چندپخشی از قبیل GOOSE نسبت به زمان حساسند و برخی تجهیزات موجود در پست‌ها دارای منابع محدودی می‌باشند، احراز اصالت باید با سرعت بالا و به صورت کارآمد انجام شود. بنابراین روش‌هایی از قبیل امضای دیجیتال مبتنی بر کلید عمومی [۸]، روش‌های احراز اصالت چندپخشی مبتنی بر پخش امضاء بین چند پیام [۹, ۱۰] و روش‌های احراز اصالت مبتنی بر آشکارسازی تأخیری کلید [۱۱] به دلایل مختلف برای استفاده در پست‌های برق مناسب نیستند. در سال‌های اخیر روش‌هایی بر پایه‌ی امضای یکبار مصرف ارائه شده‌اند که امکان سنجش بلادرنگ پیام‌های چندگانه را فراهم می‌کنند [۱۲, ۱۳] و هزینهٔ محاسباتی مناسبی دارند [۷, ۱۲–۱۵]؛ با این حال، سربار حافظه و طول امضای روش‌های موجود برای استفاده در شبکه‌های هوشمند و پست‌های برق که دارای منابع محدود هستند بسیار زیاد است.

در این مقاله مکانیزم احراز اصالت جدیدی بر مبنای امضای یک‌بار مصرف ارائه کردیم که مشکل زیاد بودن سایز امضای یکبار مصرف روش‌های پیشین [۷, ۱۲–۱۶] را رفع کرده است. در روش پیشنهادی طول امضاء در مقایسه با روش‌های دیگر به نسبت $\frac{1}{k}$ کاهش یافته است؛ با کاهش طول امضاء نیاز به پهنای باند ارتباطی به شدت کاهش می‌یابد و به دنبال آن سایز پیام ارسالی نیز کاهش قابل ملاحظه‌ای خواهد یافت. در نتیجه روش پیشنهادی برای استفاده در کاربردهایی با محدودیت طول پیام و نیاز به فرکانس بالا مناسب می‌باشد.

در ادامهٔ این مقاله ابتدا به مرور روش‌های احراز اصالت و مزایا و معایب هر یک می‌پردازیم، سپس روش پیشنهادی احراز اصالت که برای استفاده در پست‌های برق طراحی شده است را شرح خواهیم داد. در ادامه روش پیشنهادی را از نظر کارایی و امنیت مورد ارزیابی قرار خواهیم داد و در انتها به مقایسهٔ روش پیشنهادی با روش‌های موجود خواهیم پرداخت.

۲. مرور کارهای پیشین

یکی از روش‌های معروف و متداول در احراز اصالت چندپخشی استفاده از امضای دیجیتال مبتنی بر کلید عمومی می‌باشد [۱۷]، اما باید توجه داشت هزینه‌های محاسباتی این روش‌ها برای استفاده در شبکه‌های برق و مخصوصاً اتوماسیون پست‌های مبتنی بر استاندارد IEC 61850 بسیار زیاد است، زیرا تجهیزات الکتریکی هوشمند به‌کار رفته در پست‌ها محدودیت‌های فراوانی دارند و از طرفی دیگر پیام‌هایی که بین تجهیزات پست‌ها مبادله می‌شوند نسبت به تأخیر بسیار حساسند.

روش‌های دیگری که برای احراز اصالت مورد استفاده قرار می‌گیرند روش‌های متقارن هستند [۱۸, ۱۹]، این روش‌ها سرعت بالایی دارند اما استفاده از آن‌ها در پست‌های برق مناسب نیست زیرا در این روش‌ها باید کلید محرمانه بین فرستنده و گیرنده به اشتراک گذاشته شود. با توجه به اینکه در پست‌ها تجهیزات زیادی داریم که با یکدیگر در ارتباطند و پیام‌های چندپخشی نیز بخش مهمی از این ارتباطات را تشکیل می‌دهند، اگر بخواهیم احراز اصالت را با استفاده از روش‌های متقارن انجام دهیم باید تعداد زیادی کلید محرمانه بین تمام فرستنده‌ها و گیرنده‌ها مبادله کنیم که این کار هزینه‌ی بالایی به سیستم اعمال می‌کند. لذا استفاده از این روش‌ها در ارتباطات چندپخشی نه تنها مقرون به صرفه نمی‌باشد بلکه در بعضی موارد میزان امنیت را به شدت کاهش می‌دهد.

محققین در تحقیق دیگری [۱۵] برای احراز اصالت روش تسلا را ارائه کردند، این روش و روش‌هایی که برپایهٔ آن می‌باشند [۲۰, ۲۱] کاملاً مبتنی بر روش‌های متقارن هستند و اساس کار آن‌ها آشکارسازی تأخیری کلید می‌باشد. این روش‌ها نیز به دلیل بافر کردن پیام‌ها تأخیر زیادی به سیستم اعمال می‌کنند در نتیجه برای استفاده در پست‌های برق مبتنی بر استاندارد IEC 61850 مناسب نیستند.

در تحقیقات دیگری که صورت گرفته‌است [۱۰, ۲۲]، برای احراز اصالت پیام‌ها روش‌هایی با عنوان روش‌های ترکیبی ارائه شده است. در این روش‌ها از ترکیب ایده‌ی روش‌های کلید عمومی و توابع یکطرفه استفاده شده است لذا هزینهٔ محاسباتی کاهش یافته است. مزیت این روش‌ها پخش هزینهٔ امضاء و اعتبارسنجی روش‌های کلید عمومی روی چند پیام می‌باشد اما مشکل آن‌ها در این است که تمام پیام‌هایی که امضاء بین آن‌ها پخش شده است باید تا زمان دریافت آخرین پیام حاوی امضاء در فرستنده یا گیرنده بافر شوند. در نتیجه تأخیر حاصل از بافر کردن پیام‌ها سبب نقض محدودیت زمانی پیام‌ها می‌شود، لذا استفاده از این روش‌ها در پست‌های برق که حاوی پیام‌هایی با محدودیت زمانی بالا می‌باشند، صحیح نخواهد بود.

نوع دیگری از روش‌های احراز اصالت که دارای سرعت بالایی هستند روش‌های امضای یکبار مصرف می‌باشند [۲۳, ۲۴]. در این روش‌ها مشابه روش‌های کلید عمومی، برای امضاء کردن و اعتبارسنجی از کلید خصوصی و عمومی استفاده می‌شود. در این روش‌ها علی‌رغم وجود کلید عمومی و خصوصی، سرعت امضاء کردن و اعتبارسنجی به دلیل استفاده از توابع درهم‌ساز بالا می‌باشد و از طرفی دیگر چون در این روش‌ها نیازی به بافر کردن بسته‌ها نمی‌باشد، از نظر زمانی بسیار کارا می‌باشند. اما این روش‌ها معایبی نیز دارند که از جملهٔ آن‌ها می‌توان به سایز بالای کلید و امضاء اشاره کرد. روش‌های متعددی برای رفع این مشکلات ارائه شده‌اند [۷, ۱۲–۱۴, ۱۶]، اما برخی از آن‌ها به دلایل فوق مناسب پست‌های برق مبتنی بر استاندارد IEC61850 که دارای ملزومات زمانی خاص و محدودیت‌های زیادی هستند، نمی‌باشد.

در ادامه به ارائه روش پیشنهادی که بر پایه‌ی روش‌های امضای یکبار مصرف و روش ارائه شده در [۱۴] می‌باشد، می‌پردازیم؛ قابل ذکر است در روش پیشنهادی حجم امضای ارسالی به سمت گیرنده در مقایسه با دیگر روش‌ها به نسبت $\frac{1}{k}$ کاهش می‌یابد.

۳. روش پیشنهادی

در روش پیشنهادی از نمادهایی که در ادامه به ذکر آن پرداخته شده است، استفاده می‌شود. مقادیر k، z، l و t پارامترهای امنیتی هستند. تابع $f:\{0,1\}^l \to \{0,1\}^l$ تابع جایگشت یکطرفه است که روی رشته‌های l بیتی اعمال می‌شود. از $f^k(x)$ برای نشان دادن تعداد دفعات اعمال تابع f روی مقدار x استفاده می‌شود و $H(.)$ تابع درهم‌ساز یکطرفه است که ورودی را به خروجی با طول $klog_2t$ تبدیل می‌کند. $G(.)$ نیز تابع درهم‌ساز یکطرفه در مدل رندم اراکل است که به صورت $G:\{0,1\}^* \to \left[0,\binom{z-1}{k-1}\right]$ نشان داده می‌شود[۱۴]. تابع دیگری نیز با نام $C_{k,z}$ وجود دارد که ورودی آن برابر با خروجی تابع G می‌باشد. از این تابع برای بدست آوردن ترکیبات مختلفی که حاصل جمع آن‌ها برابر z باشد استفاده می‌شود. همانطور که در [۱۴] ذکر شده است، برای پیاده‌سازی این تابع از رابطهٔ زیر استفاده می‌شود. در این رابطه، هر جمله نشان‌دهنده مقدار یکی از اعداد حاصل از ترکیب می‌باشد.

$$\sum_{i=1}^{k} a_i = z \qquad (۱)$$

حال که با مفاهیم اولیه و نمادگذاری موجود در طرح پیشنهادی آشنا شدیم، به ارائه‌ی روش پیشنهادی ارائه شده در این مقاله می‌پردازیم. قابل ذکر است در روش پیشنهادی هم احراز اصالت پیام‌های یک به یک و هم احراز اصالت پیام‌های چندپخشی مورد توجه قرار گرفته‌اند. طرح پیشنهادی از سه فاز اصلی تولید کلید، تولید امضاء و اعتبارسنجی تشکیل شده است که فاز تولید کلید در هر دو بخش روش به صورت مشابهی انجام می‌شوند.

۳.۱. احراز اصالت برای یک پیام

همانگونه که پیش‌تر بیان شد طرح پیشنهادی از سه گام تولید کلید، تولید امضاء و اعتبارسنجی تشکیل شده است که در ادامه به ذکر جزئیات هر گام می‌پردازیم.

- ***تولید کلید:*** ابتدا t رشتهٔ تصادفی با طول l بیت به صورت $(s_1,s_2,\ldots,s_t)$ تولید می‌شود. سپس برای هر رشته، زنجیره‌ی درهمی با طول d تولید می‌شود؛ داریم: $s_i \to f^1(s_i) \to \cdots \to f^{d-1}(s_i)$. t زنجیره‌های تشکیل دهندهٔ کلید خصوصی هستند و کلید عمومی برای تمام iهایی که $1 \le i \le t$ هستند برابر است با $v_i = f^d(s_i)$.
- ***تولید امضاء:*** فرستنده باید برای امضاء کردن پیام m ابتدا با اعمال تابع G روی پیام، مقدار g را محاسبه کند، سپس g به‌دست آمده به همراه پارامترهای امنیتی z و k وارد تابع $C_{k,z}$ می‌شوند تا gُمین ترکیب سازنده z که به صورت $\sum_{i=1}^{k} a_i$ نمایش داده می‌شود، محاسبه گردد. سپس باید از مقدار پیام و شمارندهٔ c، مقدار درهم

تهیه شود یعنی $h=H(m|c)$ و مقدار h به k زیر رشتهٔ $log_2 t$ بیتی به صورت $h_1,\ldots,h_k$ شکسته شود. پس از این مرحله، تمام h_iها به اعداد i_j به طوریکه $1 \le i_j \le t$ و $1 \le j \le k$ ترجمه می‌شوند. در این مرحله باید مجزا بودن مقادیر بدست آمده بررسی گردد؛ در صورتیکه مقادیر حاصل مجزا از یکدیگر نبودند مقدار شمارندهٔ c یک واحد افزایش می‌یابد و روال فوق تکرار می‌گردد. در صورتیکه تمامی مقادیر به‌دست آمده از یکدیگر مجزا باشند بایداز بین k عنصر حاصل، یک عنصر انتخاب شود به طوریکه در سمت گیرنده نیز با اعمال همین اَعمال به عنصر یکسانی دست پیدا کنیم. برای این منظور به صورت زیر عمل می‌کنیم؛ ابتدا ترتیب k مقدار انتخاب شده (i_j) با استفاده از توابع shuffling به هم می‌ریزد، سپس با حذف اولین و آخرین عنصر از آن‌ها، k-2 عنصر باقی می‌ماند، ترتیب عناصر باقی مانده نیز با توابع shuffling به هم ریخته می‌شوند و عنصر اول و آخر آن‌ها حذف می‌گردد و روال فوق برای عناصر باقیمانده تکرار می‌شود. این روال تا جایی ادامه پیدا می‌کند که به یک عنصر دست یابیم. باید توجه داشت اگر مقدار k عددی زوج باشد، درنهایت دو مقدار از k تا i_j باقی خواهند ماند که از بین این دو پارامتر، سمت چپ‌ترین پارامتر به همراه اندیس موجود در آن انتخاب خواهد شد. در این بخش فرض می‌کنیم پارامتر انتخاب شده i_p و اندیس مربوط به آن p باشد. در این حالت امضاء به صورت زیر محاسبه می‌گردد.

$$sig_p = f^{d-a_p}(s_{i_p}) \qquad (۲)$$

به این ترتیب تنها یک امضاء به جای k امضاء به سمت فرستنده ارسال می‌شود.

- ***اعتبارسنجی:*** برای اعتبارسنجی امضاء دریافتی در سمت گیرنده که به صورت (sig_p) می‌باشد، باید ابتدا روالی مطابق روال انجام شده در سمت فرستنده انجام شود. یعنی ابتدا توابع G و $C_{k,z}$ روی پیام اعمال گردد، سپس با استفاده از تابع H، از حاصل الحاق پیام و c' مقدار درهم تهیه شود. سپس مقدار بدست آمده به k بخش تقسیم شده و هر بخش به عددی بین ۱ تا t ترجمه گردد. سپس بررسی می‌شود که آیا مقادیر حاصل کاملاً مجزا از یکدیگر هستند یا خیر؛ در صورتیکه تمام مقادیر مجزا از یکدیگر نباشند، اعتبار سنجی متوقف می‌شود و پیغامی مبنی بر وجود مشکل در فایل log سیستم پست‌ها قرار می‌گیرد. در نهایت روال تعیین یک پارامتر و اندیس آن دقیقاً مطابق با الگوریتم موجود در فرستنده انجام می‌شود(در صورت سالم بودن پیام و عدم بروز خطا و حمله، مقدار بدست آمده در این مرحله دقیقاً با مقدار بدست آمده در فرستنده یکسان خواهد بود).سپس برابری رابطه‌ی زیر بررسی می‌گردد.

$$f^{a_p}(sig_p) = v_{i_p} \qquad (۳)$$

در صورتیکه رابطهٔ ۳ برقرار نباشد، بروز حمله یا بروز خرابی تشخیص داده می‌شود. بدین‌صورت بنا بر سیاست اعمال شده در پست‌های برق، یا پیغام خطایی به مهندس سیستم ارسال می‌شود و یا بروز مشکل در فایل لاگ سیستم ثبت می‌گردد تا در آینده به‌توان با مراجعه به این فایل به تعداد دفعات بروز مشکل یا تاریخ وقوع حمله پی برد.

۳.۲. احراز اصالت برای پیام‌های چندپخشی

بیشتر مراحل احراز اصالت پیام‌های چندپخشی نیز مطابق با روال احراز اصالت پیام‌های تک پخشی می‌باشد با این تفاوت که فرستنده و گیرنده حالات داخلی سیستم را نگه‌داری می‌کنند؛ به این مفهوم که فرستنده تعداد زنجیره‌های درهم مورد استفاده تا کنون را به‌عنوان حالت داخلی سیستم درخود ذخیره می‌کند و گیرنده کلید عمومی فعلی را در خود نگاه می‌دارد؛ بدین‌صورت می‌توان پیام‌های چندپخشی را به راحتی امضاء کرد. در این بخش نیز مطابق بخش قبل سه فاز اصلی برای احراز اصالت پیام‌ها تعریف شده است که در ادامه به ذکر جزئیات هر یک پرداخته می‌شود.

- ***تولید کلید:*** دقیقاً مطابق با تولید کلید در احراز اصالت پیام‌های یک به یک می‌باشد.
- ***تولید امضاء:*** در مرحله تولید امضاء، همانطور که ذکر شد فرستنده برای هر یک از t رشته‌ی تولید شده در مرحله‌ی امضاء، تعداد زنجیره‌های استفاده شده تا کنون را به عنوان حالت داخلی خود در پارامترهای $(b_1,\ldots,b_t)$ ذخیره می‌کند. سپس مطابق روال تولید امضاء برای پیام‌های یک به یک، توابع G و $C_{k,z}$ را روی پیام و تابع H را روی حاصل الحاق پیام و شمارندهٔ c اعمال می‌کند. در ادامه مقادیر $(a_1,\ldots,a_k)$ که خروجی تابع $C_{k,z}$ هستند، در فرستنده نگهداری خواهند شد. سپس حاصل تابع H به k زیر بخش h_1 تا h_k تقسیم می‌شود و هر زیر بخش به عددی بین ۱ تا t ترجمه می‌گردد، در صورتیکه مقادیر بدست آمده مجزا از یکدیگر نباشند، مقدار شمارنده یک واحد افزایش یافته و روال فوق تکرار می‌شود. در نهایت دقیقاً با استفاده از الگوریتم انتخاب یک پارامتر و اندیس که در بخش تولید امضاء پیام‌های تک پخشی شرح داده شد، یک پارامتر (i_p)و اندیس آن (p) انتخاب می‌شود. حال، حالت داخلی

سیستم b_{i_p} ومقدار a بدست آمده از تابع $C_{k,z}$ که مربوط به پارامتر انتخاب شده هستند با یکدیگر جمع می‌شوند یعنی $b_{i_p} = b_{i_p} + a_p$. در نهایت امضاء برابر است با:

$$sig_p = f^{d-a_p}(s_{i_p}) \qquad (۴)$$

- ***اعتبارسنجی:*** در مرحلهٔ اعتبارسنجی پیام‌های چندپخشی، حالت داخلی گیرنده برابر کلید عمومی فعال می‌باشد و با $(u_1,\ldots,u_t)$ نشان داده می‌شود. در این گام نیز مطابق گام فوق توابع G و $C_{k,z}$ روی پیام اعمال می‌شوند و مقادیر $(a_1,\ldots,a_k)$ بدست می‌آیند. سپس مقدار $h=H(m|c')$ که c' مقدار شمارنده ارسالی توسط فرستنده است، محاسبه می‌شود. پس از آن مقدار h به k زیر رشتهٔ h_1 تا h_k شکسته می‌شود و هر بخش به عدد صحیح i_j ترجمه می‌گردد. در این مرحله بررسی می‌شود که آیا مقادیر بدست آمده از یکدیگر مجزا هستند یا خیر. اگر مقادیر از یکدیگر مجزا نبودند، عملیات اعتبارسنجی با شکست مواجه می‌شود در غیر این‌صورت روال ادامه می‌یابد. حال طبق الگوریتم انتخاب یک پارامتر و اندیس که پیش‌تر بیان شد، پارامتر (i_p) و اندیس p از بین k پارامتر انتخاب می‌شود و در نهایت برابری رابطهٔ زیر بررسی می‌گردد.

$$f^{a_p}(sig) = u_{i_p} \qquad (۵)$$

اگر رابطه برقرار نبود یعنی یا خطایی در حین کار رخ داده است و یا مهاجمی به سیستم حمله کرده است. در این حالت نیز بنا بر سیاست‌های تعیین شده در پست‌های برق، یا پیغام خطایی برای مهندس سیستم ارسال می‌شود و یا بروز خطا و تاریخ رخداد آن در سیستم ثبت می‌گردد. در صورتیکه رابطه برقرار بود، مقدار حالت داخلی سیستم مطابق (۶) برابر امضای جاری قرار خواهد گرفت تا مهاجم بعدها نتواند از امضای آشکار شده سوء استفاده کند.

$$u_{i_p} = sig_p \qquad (۶)$$

۴.تحلیل روش پیشنهادی

در این بخش روش پیشنهادی را از جنبه‌های گوناگون مورد ارزیابی قرار خواهیم داد و در نهایت آن را با دیگر روش‌های موجود مقایسه خواهیم کرد.

۴.۱. ارزیابی کارایی

در این قسمت به بررسی هزینهٔ تولید کلید، تولید امضاء و اعتبارسنجی روش پیشنهادی بر حسب تعداد جایگشت‌های یکطرفه و توابع درهم‌ساز مورد استفاده می‌پردازیم.

در مرحلهٔ تولید کلید روش پیشنهادی این مقاله نیاز به dt بار تخصیص تابع جایگشت f می‌باشد، زیرا t مقدار اولیه داریم که با اعمال d تابع f روی هر یک از آن‌ها، کلیدهای مد نظر تولید می‌شود. به دلیل اینکه طول هر یک از t مقدار اولیه l بیت می‌باشد، طول کلید خصوصی dtl بیت و طول کلید عمومی tl بیت خواهد بود. با توجه به [۷] احتمال آنکه مقادیر حاصل از $H(m|c)$ مجزا از یکدیگر باشند برابر p_c و مقدار c برابر با $\frac{1}{p_c}$ می‌باشد.

$$P_c = \left(\frac{t}{t}\right)\left(\frac{t-1}{t}\right)\cdots\left(\frac{t-k+1}{t}\right) = \frac{t(t-1)\cdots(t-k+1)}{t^k} \qquad (۷)$$

طبق [۷] و [۱۴] اگر سایز کلید خصوصی برای استفاده در کاربردی خاص بزرگ باشد می‌توان آن را به صورت $(s_1,\ldots,s_t)$ به t کلید کاهش داد؛ در این حالت سایز کلید خصوصی از dtl بیت به tl بیت کاهش خواهد یافت اما هزینهٔ امضاء کردن پیام به $\frac{t^k}{t(t-1)\cdots(t-k+1)} + w + 1$ خواهد رسید که برای برخی کاربردها بسیار زیاد می‌باشد. برای رفع این مشکل، در [۷] روشی بهینه ارائه شده است که هم سایز کلیدخصوصی و هم هزینهٔ امضاء کاهش می‌یابد. در این حالت هزینهٔ امضاء برابر $\frac{t^k}{t(t-1)\cdots(t-k+1)} + \log w + 1$ و سایز امضاء در روش پیشنهادی برابر $l+log|c|$ بیت خواهد بود. با توجه به روال پیشنهادی، عمل اعتبارسنجی در سمت گیرنده نیاز به اعمال یک تابع G، یک تابع H و a_p بار تابع f دارد، لذا هزینهٔ اعتبارسنجی برابر با a_p+2 خواهد بود.

۴.۲. ارزیابی امنیتی

در این قسمت به ارزیابی امنیتی روش پیشنهادی در مقابل حملهٔ متن انتخابی غیرتطبیقی می‌پردازیم؛ فرض می‌کنیم مهاجم برای پیام دلخواه خود، مقدار امضاء را به صورت مستقل از توابع H و G داشته باشد. مهاجم با داشتن این اطلاعات سعی در جعل امضاء برای هر پیام دلخواه دیگر می‌کند.

فرض می‌کنیم مهاجم امضای معتبر sig را داشته باشد، می‌خواهیم احتمال آنکه مهاجم بتواند با یکبار تخصیص H و G روی هر پیام دلخواه

m'، امضاء را جعل کند بدست آوریم. فرض می‌کنیم H رشته‌های تصادفی تولید کند و H و f هر دو توابعی برگشت‌ناپذیر باشند. به دلیل اینکه امضاء با عددی تصادفی که حاصل ترکیبات مختلف سازنده‌ی z است، تولید می‌شود، نمی‌توان از $f^i(sig_p)$ به طوریکه $i \geq 1$، برای جعل امضاء استفاده کرد. برای جعل امضاء باید مقدار معکوس تابع f محاسبه شود که با توجه به تعریف تابع f این امر امکان‌پذیر نخواهد بود ، لذا مهاجم برای جعل امضاء باید تنها از خود امضاء یعنی sig استفاده کند.

در روش پیشنهادی، مهاجم باید پیام دلخواه m' را دقیقاً به sig نگاشت کند، برای این منظور باید ابتدا پیام را به k پارامتر $s_{1,\ldots,}s_k$ نگاشت دهد و سپس یکی از این پارامترها را با استفاده از روالی مشخص انتخاب نماید. احتمال اینکه حاصل درهم‌سازی پیام و شمارنده برابر h دلخواه باشد یعنی $H(m'|c) = h$، برابر است با $\frac{1}{2^{|H(.)|}}$ و چون $|H(.)|$ برابر است با $k\log_2 t$، حاصل کسر فوق برابر با $\frac{1}{t^k}$ خواهد بود و چون h دلخواه به s_{i_j}های دلخواه نگاشت می‌شوند، احتمال وجود s_{i_j} ها نیز برابر $\frac{1}{t^k}$ خواهد بود؛ از طرفی احتمال آنکه پارامتر انتخابی ما از بین k پارامتر انتخاب شود برابر با $\frac{1}{k}$ می‌باشد و همچنین احتمال انتخاب g مناسب در رابطهٔ $G(m)=g$ برابر $\frac{1}{\binom{z-1}{k-1}} = \frac{1}{\frac{(z-1)!}{(k-1)!(z-k)!}} = \frac{(k-1)!(z-k)!}{(z-1)!}$ خواهد بود.

در نتیجه احتمال جعل امضاء در روش پیشنهادی برابر است با:

$$\frac{(k-1)!(z-k)!}{k(z-1)!t^k} \qquad (۸)$$

۴.۱. مقایسه با روش‌های موجود

در جدول ۱، روش پیشنهادی از نظر هزینه محاسباتی و امنیت با روش‌های بیبا، HORS، TSV و HORSIC مقایسه شده است. همانطور که در این جدول قابل مشاهده است سایز امضای پیشنهادی نسبت به تمامی روش‌های موجود به نسبت $\frac{1}{k}$ کاهش یافته است، همچنین هزینهٔ اعتبارسنجی به خاطر استفاده از یک مقدار a که $a << z$، به $a+2$ کاهش یافته است. برای کاهش حجم جدول فوق از نمادهای $\mu = \frac{t^k}{t(t-1)\cdots(t-k+1)}$ ، $\xi = \mu\prod_{r=1}^{g}(n_r!)$ و $z = \sum_{i=1}^{k} a_i$ برای $a_i \geq 1$ استفاده شده است.

جدول ۱:مقایسه روش پیشنهادی با روش‌های موجود

روش	هزینهٔ تولید کلید	هزینهٔ تولید امضاء	هزینهٔ اعتبارسنجی	طول امضاء	طول کلید عمومی
Biba [۱۳]	t	$2t$	$2k+1$	kl	tl
HORS [۱۲]	t	1	$k+1$	kl	tl
TSV [۷]	$(\max\{w_1+\ldots+w_g\}+1)t$	ξ	$1+k+\sum_{r=1}^{g} n_r w_r$	$kl+\log\xi$	tl
HORSIC [۱۴]	wt	$\mu+1$	$z+2$	$kl+\log\mu$	tl
روش پیشنهادی	wt	$\mu+1$	a_p+2	$l+\log\mu$	tl

۵. نتیجه‌گیری

در این مقاله مکانیزم احراز اصالت مناسبی برای استفاده در پست‌های برق مبتنی بر استاندارد IEC61850 ارائه شد. روش ارائه شده علاوه بر پشتیبانی از احراز اصالت پیام‌های معمولی، از احراز اصالت ارتباطات چندپخشی و همه‌پخشی نیز پشتیبانی می‌کند. برای این منظور سه گام اصلی در نظر گرفته شد که در هرکدام از آن‌ها بخشی از عملیات اصلی مکانیزم احراز اصالت انجام شده است. در فاز اول عملیات تولید کلید، در فاز دوم تولید امضاء بر اساس پیام، شمارنده افزایشی و کلید خصوصی و ارسال امضای تولید شده و پیام به سمت گیرنده و در فاز سوم اعتبارسنجی پیام در

سمت گیرنده انجام می‌شود. در صورتیکه اعتبارسنجی با موفقیت به اتمام برسد بقیه روال مطابق معمول انجام خواهد شد؛ در غیر این‌صورت روال متوقف شده و پیغام خطا به مسئول سیستم ارسال می‌شود.

با توجه به اینکه در طرح پیشنهادی به جای ارسال k امضاء به گیرنده، تنها یک مقدار برای گیرنده ارسال شده است، حجم امضا به میزان قابل توجهی کاهش یافته است و در نتیجه نیاز به پهنای باند کم‌تری می‌باشد. مزیت دیگری که به دنبال کاهش حجم امضاء به‌دست آمده است، نیاز به حافظه‌ی کم‌تر در سمت فرستنده و گیرنده است؛ همچنین روش پیشنهادی قابلیت پشتیبانی از پیام‌های چندپخشی که بخش مهم و قابل توجهی از ارتباطات پست‌های مبتنی بر IEC 61850 را تشکیل می‌دهند، دارد.

منابع

[1] S. M. Amin and B. F. Wollenberg. (2005, September) Toward a Smart Grid: Power Delivery for 21st Century. *IEEE Power and Energy Magazine*. 34–41.

[2] A. L. G. N. S. Prasanna, S. Sumanth, V. Simha,J. Bapat, and G. Koomullil, "Data Communication over the Smart Grid," presented at the in Proc. of IEEE Int. Sump.Power Line Communications and Its Applications, 2009.

[3] G. R. E. Santacana, T. Tang, and F. Xiaoming. (2010, March) Getting Smart. *IEEE Power and Energy Magazine*. 41–48.

[4] S.-W. Z. S.-J. Rim,and S.-J. Lee, "Development of an Intelligent Station HMI in IEC 61850 Based Substation," *Journal of Electrical Engineering & Technology*, vol. 4, pp. 13-18, 2009.

[5] S.-S. K. Hyo-Sik Yang, Hyuk-Soo Jang, "Optimized Security Algorithm for IEC 61850 based Power Utility System," *Journal of Electrical Engineering & Technology*, vol. 7, pp. 443-450, 2012.

[6] S. Lu, D. Bolin, Y. Yong, T. F. Abdelzaher, C. Guohong, and J. C. Hou, "oCast: Optimal multicast routing protocol for wireless sensor networks," in *Network Protocols, 2009. ICNP 2009. 17th IEEE International Conference on*, 2009, pp. 151-160.

[7] Q. L. a. G. Cao, "Multicast Authentication in the Smart Grid With One-Time Signature," *IEEE TRANSACTIONS ON SMART GRID*, vol. 2, 2011.

[8] W. Ertel, *Angewandte Kryptographie*: Hanser Verlag, 2007.

[9] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, 2000, pp.73-56.

[10] D. Song, D. Zuckerman, and J. Tygar, "Expander graphs for digital stream authentication and robust overlay networks," in *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*, 2002, pp. 258-270.

[11] A. Perrig, D. Song, R. Canetti, J.Tygar, and B. Briscoe, "Timed efficient stream loss-tolerant authentication (TESLA): multicast source authentication transform introduction," RFC 4082, June2005.

[12] L. Reyzin and N. Reyzin, "Better than BiBa: Short one-time signatures with fast signing and verifying," in *Information Security and Privacy*, 2002, pp. 144-153.

[13] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in *Proceedings of the 8th ACM conference on Computer and Communications Security*, 2001, pp. 28-37.

[14] J. Lee, S. Kim, Y. Cho, Y. Chung, and Y. Park, "HORSIC: An efficient one-time signature scheme for wireless sensor networks," *Inf. Process. Lett.*, vol. 112, pp. 783-787, 2012.

[15] Q. Wang, H. Khurana, Y. Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *INFOCOM 2009, IEEE*, 2009, pp. 1233-1241.

[16] W. D. Neumann, "HORSE: an extension of an r-time signature scheme with fast signing and verification," in *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, 2004, pp. 129-134 Vol.1.

[17] M. Branchaud, "A survey of public-key infrastructures," McGill University, 1997.

[18] N. FIPS, "180-2: Secure hash standard (SHS)," Technical report, National Institute of Standards and Technology (NIST), 2 001. http://csrc. nist. gov/publications/fips/fips180-2/fips180-2withchangenotice. pdf2001.

[19] F. Pub, "198, the keyed-hash message authentication code (hmac)," *Federal Information Processing Standards Publication*, vol. 198, 2002.

[20] D. Liu and P. Ning, "Multilevel μTESLA: Broadcast authentication for distributed sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, pp. 800-836, 2004.

[21] D. Liu, N. Peng, Z. Sencun, and S.Jajodia, "Practical broadcast authentication in sensor networks," in *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*, 2005, pp. 118-129.

[22] C. Karlof, N. Sastry, Y. Li, A. Perrig, and J. Tygar, "Distillation codes and applications to DoS resistant multicast authentication," in *Proceedings of the ISOC Symposium on Network and Distributed System Security (SNDSS)*, 2004, pp. 37-56.

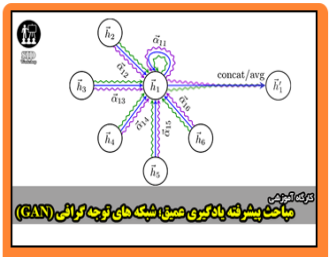
[23] L. Lamport, "Constructing digital signatures from a one-way function," Technical Report CSL-98, SRI International1979.

[24] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, pp. 281-308, 1988.

کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین مکالمه روزمره انگلیسی

کارگاه آنلاین آموزش استفاده از وب آو ساینس



مباحث پیشرفته یادگیری عمیق؛ شبکه های توجه گرافی (Graph Attention Networks)