Journal of the Nivar Vol. 47, No. 120-121, Spring and Summer 2023, P. 153-165

Homepage: https://nivar.irimo.ir (Research Article)

Efficiency Simultaneous key Exchange-Cryptography Extraction from Public key in Fog-Cloud Federation-based Secure Offloading for Automatic Weather Stations Observing Systems

Salami, Y.[1] | Khajehvand, V.[2] ✉ | Zeinali, E.[3]

1,3. Department of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran. E-mail: yashar.salami@gmail.com , zeinali.es@gmail.com

2. **Corresponding Author**, Department of Computer and Information Technology Engineering, Qazvin Branch, Islamic Azad University, Qazvin, Iran. E-mail: vahidkhajehvand@gmail.com

(Received: 12 May 2023, Revised: 17 Jun 2023, Accepted: 19 Sep 2023, Published online: 19 Sep 2023)

Abstract

Considering that in automatic weather station systems, raw data is collected by sensors by AWSs, and these sensors themselves cannot process raw data. The data is sent to the CPS unsafely for processing, considering that the raw data in the wireless network is sent. No encryption operation or key exchange has been performed between the communication parties. At any moment, there is a possibility that a third party with an identity attack can be placed between AWS and CPS and listen to or manipulate the data sent. In this article, we have presented a new encryption method by combining the Jamal encryption system and the Diffie-Hellman key exchange algorithm, which, unlike the existing method, provides the ability to exchange keys for the sender and receiver from the public key so that there is no longer a need for encryption and key exchange from two algorithms. Be used differently. The simulation results of the proposed method against pervasive search attack show that the proposed method in the first scenario is 0.030141 seconds in the normal way and 1.241097 seconds in the parallel mode, and in the second scenario is, 5.112216 seconds in the normal manner and 6.724856 seconds in the parallel process compared to the ElGamal process against the attack. Comprehensive search resists.

Keywords: Cryptography, key exchange, Meteorology, Cloud.

Cite this article: Salami, Y., khajehvand, V., & Zeinali, E. (2023). Efficiency Simultaneous key Exchange-Cryptography Extraction from Public key in Fog-Cloud Federation-based Secure Offloading for Automatic Weather Stations Observing Systems. Journal of the Nivar, Vol. 47, No. 120-121. 153-165. DOI: https://doi.org/10.30467/nivar.2023.416270.1261

Publisher: Iran Meteorological Organization
DOI: https://doi.org/10.30467/nivar.2023.416270.1261

Print ISSN: 1735-0565
Online ISSN: 2645-3347

نیوار
دوره ۴۷، شماره ۱۲۰- ۱۲۱، بهار و تابستان ۱۴۰۲، صفحه ۱۵۳- ۱۶۵
نشانی اینترنتی مجله: https://nivar.irimo.ir
(مقاله پژوهشی)

بهره وری تبادل کلید همزمان- استخراج رمزنگاری از کلید عمومی در تخلیه ایمن مبتنی بر فدراسیون مه-ابر برای سیستم های رصد ایستگاه های هواشناسی خودکار

یاشار سلامی [۱] | وحید خواجه وند [۲] ✉ | اسماعیل زینالی [۳]

۱و۳. گروه مهندسی کامپیوتر و فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران. رایانامه: yashar.salami@gmail.com و zeinali.es@gmail.com

۲. **نویسنده مسئول**، گروه مهندسی کامپیوتر و فناوری اطلاعات، واحد قزوین، دانشگاه آزاد اسلامی، قزوین، ایران. رایانامه: vahidkhajehvand@gmail.com

(دریافت: ۱۴۰۲/۰۲/۲۲، بازنگری: ۱۴۰۲/۰۳/۲۷، پذیرش: ۱۴۰۲/۰۶/۲۸، انتشار آنلاین: ۱۴۰۲/۰۶/۲۸)

چکیده

باتوجه به اینکه در سیستم های ایستگاه هواشناسی خودکار اطلاعات خام توسط حس گرها توسط AWS ها جمع آوری می‌شود و خود این حسگرها قابلیت پردازش داده‌های خام را ندارند و برای پردازش ، داده‌ها را به سمت CPS در یک ناامن ارسال می‌شود با توجه به اینکه داده‌های خام در شبکه بیسیم ارسال می‌شود و هیچ نوع عملیات رمزنگاری و تبادل کلید بین طرفین ارتباط انجام نشده است هر لحظه این امکان وجود دارد که یک شخص ثالث با هویت حمله کنند بین AWS و CPS قرار گیرد و داده‌های ارسالی را شنود یا دست‌کاری شود. ما در این مقاله با ترکیب سیستم رمزنگاری الجمال و الگوریتم تبادل کلید دیفی هلمن یک روش رمزنگاری جدید ارائه کرده‌ایم که برخلاف روش موجود قابلیت تبادل کلید برای فرستنده و گیرنده از کلید عمومی مهیا می‌کند به‌گونه‌ای که دیگر نیاز نیست برای رمزنگاری و تبادل کلید از دو الگوریتم متفاوت استفاده شود. نتایج شبیه سازی روش پیشنهادی در برابر حمله جستجوی فراگیر نشان میدهد که روش پیشنهادی در سناریو اول به به روش نرمال ۰.۰۳۰۱۴۱ ودر روش موازی ۱.۲۴۱۰۹۷ ثانیه و در سناریو دوم به روش نرمال ۵.۱۱۲۲۱۶ و در روش موازی ۶.۷۲۴۸۵۶ ثانیه بیشتر در مقابل روش الجمل در برابر حمله جستجوی فراگیر مقاومت میکند.

کلمات کلیدی: رمزنگاری، تبادل کلید ، هواشناسی، ابر.

۱. مقدمه

رشد سریع روزافزون شبکه‌های کامپیوتری، خصوصاً اینترنت باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، دولت‌ها،سازمان‌ها و مؤسسات شده است. ازاین‌جهت حفاظت اطلاعات در برابر حملات گوناگون یکی از مسائل ضروری و مهم در این چرخه هست[1]. با اتصال شبکه داخلی سازمان‌ها به شبکه جهانی، داده‌های سازمان‌ها در معرض دسترسی افراد و میزبان‌های خارجی قرار می‌گیرد و در این حالت اطمینان از عدم دستیابی افراد غیرمجاز به اطلاعات حساس از مهم‌ترین چالش‌های امنیتی در رابطه با توزیع اطلاعات در اینترنت و شبکه بلاکچین بوده است[3][2]. دانش رمزنگاری امکان مشاهده، مطالعه و تفسیر پیام‌های ارسالی توسط افراد غیرمجاز را سلب می‌نماید.در رمزنگاری هدف ساختن طرح‌ها یا پروتکل‌هایی است که بتوان با کمک آن‌ها حتی در حضور دشمن نیز کارهای خاصی را انجام داد. یک هدف اساسی در رمزنگاری این است که به افراد این امکان را بدهند که روی یک کانال ناامن با حفظ حریم خصوصی و اصالت داده‌هایشان

استناد: سلامی, یاشار, خواجه وند, وحید, & زینالی, اسماعیل. (۱۴۰۲). بهره وری تبادل کلید همزمان- استخراج رمزنگاری از کلید عمومی در تخلیه ایمن مبتنی بر فدراسیون مه-ابر برای سیستم های رصد ایستگاه های هواشناسی خودکار، مجله نیوار، دوره ۴۷، شماره ۱۲۰- ۱۲۱، ۱۵۳- ۱۶۵. DOI: https://doi.org/10.30467/nivar.2023.416270.1261

ناشر: سازمان هواشناسی کشور.
DOI: https://doi.org/10.30467/nivar.2023.416270.1261

به‌صورت کاملاً امن باهم ارتباط برقرار کنند[4]. بااین‌حال یکی از معضلات سیستم‌های رمزنگاری تحویل یا دریافت کلید از طرف مقابل است در برخی از محیط‌ها ، مسئله به‌سادگی حل و فصل می‌شود (تحویل مستقیم و دستی است).در سیستم‌های بانکی یا اعتباری شخص متقاضی حداقل یک‌بار حضوراً به یکی از نماینده‌ها مربوطه مراجعه کرده و پس از تنظیم اسناد لازم کلید رمز خود را رسماً تحویل می‌گیرد و از آن لحظه به بعد مسئولیت حفظ و نگهداری از آن را بر عهده‌دار دارد[5]. این حالت برای کسانی که از راه دور اقدام به ایجاد حساب کاربری می‌کنند مناسب نیست .زیرا هیچ‌گاه نمی‌توان افراد را حضوراً برای تحویل کلید دعوت کرد بلکه باید از طریق خطوط ناامن کلید رمز را به افراد مختلف تحویل داد. در این حالت وقتی کلید رمز برای اولین و آخرین بار مسیر ناامن شبکه را طی می‌کند می‌تواند استراق سمع شود. سرقت کلید رمز مساوی است با ناامنی مطلق زیرا تمام داده‌های رمز شده توسط فرستنده، برای نفوذ گری که کلید رمز را دزدیده قابل بهره‌برداری است لذا ایجاد یک سیستم رمزنگاری باقابلیت ایجاد کلید سری بین طرفین ارتباط، یکی از چالش‌های مهم در این عرصه است[6]. مسئله لگاریتم گسسته کاربرد فراوانی در برخی از الگوریتم‌های رمزنگاری نامتقارن دارند. توابع لگاریتم گسسته در ریاضیات و جبر، دسته‌ای از توابع هستند که مشابه با تابع لگاریتم معمولی و روی گروه‌های عددی تعریف می‌شوند.حل کردن مسئله لگاریتم گسسته (محاسبه لگاریتم گسسته) از دیدگاه ریاضی معادل با حل کردن مسئله تجزیه اعداد صحیح در نظر گرفته می‌شود و وجوه اشتراکی بین آن دو وجود دارد: هر دو مسئله جزو مسائل دشوار ریاضی هستند، به این معنی که روش سریعی برای حل کردن آن‌ها پیدا نشده است[7]. هر الگوریتم مرتبط با یکی از این دو مسئله، قابل‌تبدیل به الگوریتم مشابهی در ارتباط با مسئله دیگر می‌باشد. از دشوار بودن حل هر دو مسئله، برای طراحی و ایجاد سیستم‌های رمزنگاری مختلفی استفاده شده است.سیستم رمزنگاری الجمل یک الگوریتم رمزنگاری کلید عمومی است که بر پایه پروتکل تبادل کلید دیفی-هلمن ساخته شده است[8], [9] به خاطر نزدیک بودن این دو سیستم از نظر ساختاری ما برآن شودیم که با ترکیب این دو روش یک الگوریتم جدید رمزنگاری با قابلیت تولید کلید از کلید عمومی برای تبادل کلید برای سیستم های هواشناسی پیشنهاد دهیم.

۱-۱. سازمان مقاله

ساختار مقاله به شرح زیر است : در بخش دوم مفاهیم پایه بیان می‌شود و در بخش سوم کارهای گذشته مورد بررسی قرار می‌گیرد . بخش چهارم مدل شبکه مورد استفاده در مقاله را شرح می‌دهد. در بخش پنجم روش پیشنهاد توصیف می‌شود و در بخش ششم اثبات ریاضی طرح پیشنهادی بیان می‌شود . در بخش هفتم شبیه سازی طرح پیشنهادی بیان می‌شود و در آخرین بخش نتیجه گیری اریِه می‌شود.

۲. مفاهیم پایه

این بخش مفاهیم پایه ریاضی از جمله تعریف گروه ، حلقه ، نیم حلقه و سایر موارد را مطرح می‌کند تا به خوانند درک درستی از روش پیشنهادی را اریه کند.

- گروه

گروه (Group) تشکیل شده از یک مجموعه مثل G که به همراه عملگر فرضی $\oplus$ به صورت $(G, \oplus)$ نشان داده می شود و دارای خصوصیات زیر است.

الف. عملگر $\oplus$ روی مجموعه G بسته است. یعنی $\forall a, b \in G \Rightarrow a \oplus b \in G$

ب. عملگر $\oplus$ دارای خصوصیت شرکت پذیری است. یعنی $\forall a, b, c \in G \Rightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$

ج. عملگر $\oplus$ باید در مجموعه G دارای (Identity Element) باشد. یعنی $\forall a \in G, \exists i \Rightarrow a \oplus i = i \oplus a = a$

د. به ازای هر عنصر مثل a از G ، یک عنصر معکوس a^{-1} متعلق به G وجود داشته باشد به قسمی که:

$a \oplus a^{-1} = a^{-1} \oplus a = i$

عملگر $\oplus$ و مجموعه G ، انتزاعی هستند یعنی می‌توانند هر مجموعه دلخواه و هر عملگر متعارف یا نا متعارف را به جای آن‌ها فرض کرده و شرایط گروه بودن یا نبودن را بررسی کرد.

- گروه ابلی

هر گاه مجموعه G و عملگر فرضی $\oplus$، شرایط ذکر شده برای یک گروه را دارا بوده و اضافه بر آن دارای ویژگی جابه جای نیز باشد بدان گروه، گروه ابلی گفته می‌شود. یعنی به غیر از تمام شرایط گروه، شرط زیر بر قرار باشد.

$$\forall a,b \in G \Longrightarrow a \oplus b = b \oplus a$$

- گروه محدود

فرض کنید G به همراه عملگر فرضی $\oplus$ یک گروه و تعداد عناصر G محدود و قابل شمارش باشد. در این صورت به گروه G (گروه محدود) گفته می‌شود.

- زیر گروه

فرض کنید که $(G,\oplus)$ یک گروه باشد اگر H زیر مجموعه ای از G و به همراه عملگر $\oplus$، کماکان شرایط گروه را داشته باشد (H یک زیر گروه G) نامیده می‌شود.

- گروه چرخه‌ای

گروه G را به همراه عملگر $\oplus$ چرخه ای میگویند هر گاه یک مؤلفه مثل a در G پیدا شود به نحوی که توانهای متوالی آن به شکل a^i، تمام عناصر G را تولید کند.

- قضیه لاگرانژ

هر گاه H یک زیر گروه از گروه از گروه محدود G باشد آنگاه خواهیم داشت:

$$ord\ (H)\ |\ ord\ (G)$$

یعنی تعداد عناصر H، تعداد عناصر G را می‌شمارد.

- حلقه

یک حلقه تشکیل شده از یک مجموعه به نام R بر روی عملگر فرضی $\oplus$ و $\otimes$ بر روی آن تعریف و با نماد $(R$ و $\otimes$ و $\oplus)$ معرفی مشود. الزاماً حلقه باید دارای شرایط زیر باشد .

الف. (R و $\otimes$) باید یک گروه ابلی باشد. گروه بودن مجموعه R بر روی عملگر $\oplus$ ایجاب می‌کند که یک (Identity Element) برای این عملگر یافت شود. این عضو همانی بر روی عملگر $\oplus$ را i می‌نامیم.

ب. R بروی عملگر دوم یعنی ($\oplus$) باید دارای خواص شرکت پذیری باشد:

$$\forall a,b,c \in R \Longrightarrow a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

ج. عملگر دوم بر روی عملگر اول باید دارای خصوصیت پخشی از چپ و راست باشد:

$$\forall a,b,c \in R \Longrightarrow a \otimes (b \oplus c) = (b \otimes c) \oplus (a \otimes c)$$

$$\forall a,b,c \in R \Longrightarrow (b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$$

د. عملگر دوم نیز باید به ازای تمام عناصر R، دارای عضو همانی در همین مجموعه باشد.آن را i می‌نامیم.

$$\forall a \in R, \exists i \in R \Longrightarrow a \otimes i = i \otimes a = a$$

- میدان

هر گاه مجموعه F به همراه دو عملگر فرضی $\oplus$ و $\otimes$ یک حلقه جابجای باشد در عین حال می‌توان هر عضو F بر روی عملگر دوم نیز معکوس داشته باشد به آن میدان میگویم . به عبارتی هر گاه ($\oplus$ و $\otimes$ و F) حلقه جابجای باشد که در شرط زیر نیز صدق کند یک میدان را تشکیل می‌دهد.

$$\forall a \in F, \exists a \in R \Longrightarrow a \otimes a = a \otimes a = i$$

- قضیه کوچک فرما

هر گاه P عدد اول و a یک عدد مثبت غیر قابل تقسیم بر P باشد خواهیم داشت $a^{P-1} \overset{P}{\equiv} 1$

قضیه اویلر

هر گاه a و n نسبت به هم اول باشند انگاه خواهیم داشت:

$$a^{\emptyset(n)} \overset{n}{\equiv} 1$$

۳.کارهای گذشته

کارهای گذشته به دو بخش رمزنگاری کلید عموی و تبادل کلید تقسیم می‌شود که در هر قسمت الگوریتم‌های مخصوص به هر قسمت مورد بررسی قرار می‌گیرد و در انتهای هر بخش در جدولی خلاصه از مطالعات همراه نمایش داده شده است.

۳-۱. رمزنگاری کلید عمومی

الگوریتم رمزنگاری RSA جزو اولین الگوریتم‌های کلید عمومی است که برای انتقال داده‌های امن استفاده می‌شود. الگوریتم RSA در سال ۱۹۷۷ توسط Ron Rivest, Adi Shamir, and Leonard Adleman ابداً گردید و به‌طور گسترده استفاده می‌شود[]. امنیت الگوریتم RSA از این حقیقت ناشی می‌شود که هیچ روش مؤثری برای تجزیه (Prime factors) نمی‌شناسیم. ثابت‌شده است که هر عددی را می‌توان به‌صورت حاصل‌ضرب چند عدد اول نوشت[11]. الگوریتم رابین در سال ۱۹۷۸ توسط مایکل رابین توسعه یافت. امنیت

این الگوریتم همانند RSA مبتنی بر سختی تجزیه اعداد بزرگ است[12]. ایراد اصلی الگوریتم رابین پیچیدگی تشخیص متن آشکار مطابق متن اصلی از بین چهار ریشه ممکن در فرآیند رمزگشایی می‌باشد .برای تشخیص درست پیغام مطابق متن اصلی از بین چهار ریشه ممکن از یک کاراکتر میانگیر با فضای خالی جهت پر کردن قبل از رمزنگاری استفاده می‌شود . به طوری که بعد از رمزگشایی فقط یک پیغام از چهار پیغام احتمالی پیغام اصلی خواهد بود [13].اساس کار بدین صورت می‌باشد که برای رمزنگاری عدد تصادفی که در جهت ایمن نمودن الگوریتم در نظر گرفته شده استفاده می‌شود. رمزنگاری منحنی بیضوی (ECC) یک رمزنگاری به روش کلید عمومی می‌باشد که بر اساس ساختاری جبری از منحنی‌های بیضوی بر روی زمینه‌های محدود طراحی شده. استفاده از منحنی‌های بیضوی در رمزنگاری به طور جداگانه توسط Neal Koblitz و Victor S. Mille در سال ۱۹۸۵ پیشنهاد شد[15] ,[14]. رمزنگاری کلید عمومی مبتنی بر اشکالات برخی از مسائل ریاضی است. در اوایل سیستم‌های مبتنی بر کلید عمومی با این فرض که پیدا کردن دو یا بیشتر از دو عامل اول بزرگ برای یک عدد صحیح بزرگ مشکل است امن تلقی می‌شدند. برای پروتکل‌های مبتنی بر منحنی بیضوی، فرض بر این است که پیدا کردن لگاریتم گسسته از یک عنصر تصادفی منحنی بیضوی با توجه به یک نقطه پایه عمومی شناخته شده غیر عملی می‌باشد. الگوریتم امضای دیجیتال یک استاندارد دولت فدرال ایالات متحده یا FIPS برای امضای دیجیتال است. که این الگوریتم در آوت ۱۹۹۱ توسط موسسه ملی استاندارد و تکنولوژی برای استفاده به عنوان استاندارد امضای دیجیتال (DSA) پیشنهاد شد و در ۱۹۹۳ FIPS پذیرفته شد[16]. هنگامی که پیغامی از کانالی ناامن ارسال می‌شود، یک امضای دیجیتال که به شکل صحیح به انجام رسیده باشد می‌تواند برای شخص گیرنده پیام دلیلی باشد تا ادعای شخص فرستنده را باور کند و یا به عبارت بهتر شخص گیرنده از طریق امضای دیجیتال می‌تواند این اطمینان را حاصل کند که همان شخص فرستنده نامه را امضا کرده است و نامه جعلی نیست. الگوریتم رمزنگاری الجمل یک الگوریتم رمزنگاری کلید عمومی است که بر پایه پروتکل تبادل کلید دیفی-هلمن ساخته شده است. این الگوریتم توسط طاهر الجمل در سال ۱۹۸۴ طراحی شد است[17]. رمزنگاری الجمل بر پایه لگاریتم گسسته بنا شده است و ازلحاظ استحکام و اطمینان می‌تواند با RSA رقابت کند ولی بسیار پیچیده و کندتر است.

۳-۲. تبادل کلید

پروتکل تبادل کلید دیفی-هلمن، یک پروتکل رمزنگاری است. با استفاده از پروتکل تبادل کلید دیفی-هلمن ، دو نفر یا دو سازمان، می‌توانند بدون نیاز به هرگونه آشنایی قبلی، یک کلید رمز مشترک ایجاد و آن را از طریق یک مسیر ارتباطی غیر امن، بین خود تبادل نمایند[18]. این پروتکل، اولین روش عملی مطرح شده برای تبادل کلید رمز در مسیرهای ارتباطی غیر امن است و مشکل تبادل کلید رمز در رمزنگاری کلید متقارن را آسان می‌سازد.این پروتکل، در سال ۱۹۷۶ توسط ویتفیلد دیفی و مارتین هلمن و رالف مِرکل طراحی شده است[19]. پروتکل نیدهام – شرودر در سال ۱۹۷۸ مقارن با توسعه روش‌های مدرن امنیت، توسط " راجر نیدهام " و " مایکل شرودر" معرفی شد.پروتکل "نیدهام – شرودر" مبتنی بر مفهوم "چالش و پاسخ " است و به یک مرکز توزیع کلید (KDC) نیاز دارد[20]. پروتکل آتوی ریس در سال ۱۹۸۷ توسط دیوید آتوِی و آوِن ریس معرفی شد. این پروتکل از یک مرکز توزیع کلید برای تبادلات استفاده می‌کند[21] .پروتکل قورباغه دهان‌گشاد توسط مایکل باروز در سال ۱۹۹۰ طراحی شده است این پروتکل برای مقابله با بعضی حملات رایج از مهرزمانی همراه با مرکز توزیع کلید بهره می‌برد[22].

۴. مدل شبکه‌ای

ما از یک مدل سیستم‌های ایستگاه هواشناسی خودکار استاندارد برای رصد اب و هوا است برای کارهای خود استفاده کردیم شکل ۱ مدلی شبکه ای از ایستگاه هواشناسی را نشان میدهد.

مدل شبکه ای ایستگاه هوا شناسی از سه قسمت اصلی تشکیل شده است.

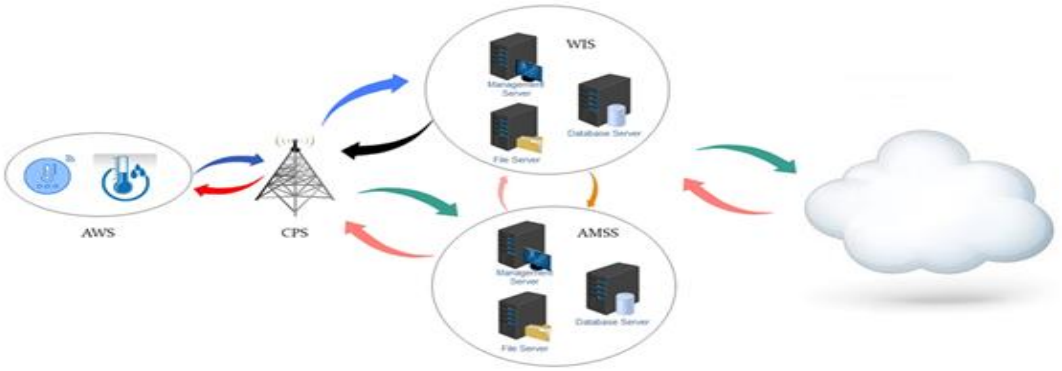
AWS: ایستگاه هواشناسی خودکار است که این ایستگاه تشکیل شده از مجموعه ای از سنسور ها که وظیفه اصلی انها دریافت اطلاعات از محیط پیرامون و ارسال به CPS است.

۱. CPS: مجموعه ای سیستم های پردازشی هستند که اطلاعات خهام دریافتی از cps ها را پردازش کرده و WIS و AMSS ارسال میکنند.

۲. WIS: سیستم جامع از اطلاعات هواشناسی هستند که به کلیه داده های مورد استفاده در خوزه های مختلف هواشناسی دسترسی دارند.

۳. AMSS: یک سیستم پیام خودکار است که به کلیه سیستم های ارسال و دریافت پیام های هواشناسی اطلاق میشود.

۴. CLOUD: مجموعه ای از کامپیوتر های با پردازش قوی هستند که قدرت پردازش و ذخیر سازی بالایی نسبت به سایر سیستم های موجود.



شکل ۱. مدل شبکه

فرض های مدل :

- فرض میشود که در مدل شبکه ای همیشه مهاجم فعالی بین AWS و CPS وجود دارد که میتواند داده های ارسالی بین طرفین ارتباط را شنود یا تغییر دهد.
- فرض میشود که در مدل شبکه ای AWS وCPS و AMSS و WIS یک دیگر را میشناسند.
- فرض میشود که در مدل شبکه ای ارتباط بین CPS و AMSS و WIS امن هست.
- .فرض میشود که تمام اطلاعات پردازش شده در ابر ذخیره میشود و در صورت نیاز میتوان از ابر درخواست اطلاعات کرد.

۴-۱. طرح مسئله

با توجه مدل شبکه تعریف شده اطلاعات خام توسط حس‌گرها توسط AWS ها جمع آوری می‌شود و خود این حسگرها قابلیت پردازش داده‌های خام را ندارند به همین دلیل برای پردازش داده از تکنیک تخلیه بار استفاده می‌کنند و داده‌ها را به سمت CPS برای پردازش در یک ناامن ارسال می‌شود با توجه به اینکه داده‌های خام در شبکه بیسیم ارسال می‌شود و هیچ نوع عملیات رمزنگاری و تبادل کلید بین طرفین ارتباط انجام نشده است هر لحظه این امکان وجود دارد که یک شخص ثالث با

هویت حمله کنند بین AWS و CPS قرار گیرد و داده‌های ارسالی را شنود یا دست‌کاری کند که این عمل باعث می‌شود که هویت داده‌های ارسالی از سمت AWS قابل اطمینان نباشد. ضروری است برای جلوگیری از بروز این نوع حملات قبل از اینکه داده‌ای به سمت CPS ارسال شود طرفین ارتباط برای ایجاد یک کانال امن برای تبادل اطلاعات اقدام کنند . ما در این مقاله یک روش تبادل کلید با قابلیت رمزنگاری را برای تولید کانال امن برای سیستم‌های رصد خودکار ایستگاه‌های هواشناسی پیشنهاد دادیم.

۵. روش پیشنهای

حل کردن مسئله لگاریتم گسسته (محاسبه لگاریتم گسسته) از دیدگاه ریاضی معادل با حل کردن مسئله تجزیه اعداد صحیح در نظر گرفته می‌شود و وجوه اشتراکی بین آن دو وجود دارد. هر دو مسئله جزو مسائل دشوار ریاضی هستند، به این معنی که روش سریعی برای حل کردن آن‌ها پیدا نشده است و هر الگوریتم مرتبط با یکی از این دو مسئله، قابل‌تبدیل به الگوریتم مشابهی در ارتباط با مسئله دیگر می‌باشد . از طرفی چون مسئله لگاریتم گسسته یکی از مسائل دشوار ریاضی است و معکوس آن یعنی محاسبه توان گسسته به‌سادگی قابل انجام است این عدم تقارن در دشواری دو مسئله معکوس، برای تحقق سیستم‌های رمزنگاری نظیر الگوریتم رمز الجمل و پروتکل تبادل کلید دیفی-هلمن و الگوریتم‌های مشابه مورداستفاده قرارگرفته است . سیستم رمزنگاری الجمل یک الگوریتم رمزنگاری کلید عمومی است که بر پایه پروتکل تبادل کلید دیفی هلمن ساخته شده است. به خاطر نزدیک بودن این دو سیستم از نظر ساختاری ما بر آن شودیم که با ترکیب این دو نوع الگوریتم یک روش جدید رمزنگاری با قابلیت تولید کلید از کلید عمومی برای تبادل کلید برای سیستم های هواشناسی پیشنهاد بدهیم.

۵-۱. مراحل روش پیشنهادی

AWS می‌خواهد برای خود یک کلید عمومی و یک کلید خصوصی انتخاب کند و با استفاده از کلید عمومی تبادل کلید انجام دهد و یک کانال ناامن را به یک کانال امن تبدیل کند تا ارتباط امنی با دیگران و ازجمله CPS ایجاد کند و سپس پیام‌های خود را پس از رمزنگاری به کمک کلید عمومی برای او بفرستند و این کار باید طبق روال زیر انجام می‌گیرد.

الف . AWS یک عدد اول بسیار بزرگ انتخاب کرده و آن را (P) می‌نامد. از آنجا که اعداد ۰ تا $p-1$ یک میدان محدوده گالوا را تشکیل می‌دهد لذا Zp قطعاً به تعداد $\partial(p-1)$ ریشه اول (یا همان مولد) دارد که توان‌های متوالی آن‌ها کل مجموعه Zp را با استثنای صفر باز تولید خواهد کرد.

ب. از آنجایی که مجموعه Zp دارای تعداد بسیار زیادی مولد هست AWS یکی از میدان Zp را انتخاب کرده و آن را (G) می‌نامد.

ج. AWS عدد (A) به دلخواه با شرط $1 \leq a \leq p-1$ انتخاب کرده و آن را کلید خصوصی قرار داده و به صورت محرمانه نزد خود نگاه می‌دارد. این عدد سری است و هرگز بر روی خط ارسال نخواهد شود.

د.AWS مطابق رابطه (۱) عدد انتخابی (G) را به تواند کلید خصوصی خود یعنی (A) رساند و پس از محاسبه باقیمانده به پیمانه (P) آن را ß می‌نامد.

$$\beta = G^A \bmod P \qquad (1)$$

ه . در اینجا AWS مجموعه سه تایی (P, G, β) را به عنوان کلید عمومی در اختیار همگان قرار می‌دهد در حالی که کلید خصوصی او (P, G, A) است که از سه تایی فقط (A) را مخفی نگاه داشته است.

کلید عمومی (P, G, β)

کلید خصوصی (P, G, A)

و. حال فرض کنید CPS می‌خواهد پیامی را با در دست داشتن کلید عمومی AWS برای او رمز کرده و ارسال کند ولی قبل از این کار باید کانالی امن بین خود و AWS ایجاد کند برای این کار CPS عدد (y) را انتخاب کرده و (Y) را به از رابطه (۲) زیر حساب می‌کند.

$$Y = G^y \bmod P \qquad (2)$$

ز. CPS (Y) را برای AWS ارسال می‌کند

ح. CPS برای به دست آوردن کلید سری مشترک با AWS از رابطه (۳) عدد(β) را در پیمانه (P) به توان (y)(عدد سری خودش) می‌رساند.

$$K = \beta^{y} \bmod P \qquad (3)$$

زیرا

$$K = \beta^{y} \bmod P = (G^{A})^{y} \bmod P = G^{A.y} \bmod p$$

ط. AWS نیز از رابطه (۴) برای محاسبه کلید سری و مشترک با CPS عدد (Y) را در پیمانه (P) به توان عدد خصوصی خودش می‌رساند.

$$K = Y^{A} \bmod P \qquad (4)$$

زیرا

$$K = Y^{A} \bmod P = (G^{y})^{A} \bmod P = G^{A.y} \bmod p$$

ی. CPS بعد از ایجاد یک کانال امن بین خود و AWS می‌خواهد پیام M را با در دست داشتن کلید عمومی AWS ارسال کند قبل از هر کار باید پیام خود را به بلوک‌های I کاراکتر تقسیم کند و هر بلوک را طبق قاعده کاملاً دلخواه به یک عدد صحیح به نام mi نسبت دهد به نحوی که $0 \leq mi \leq p-1$ باشد.

۱ CPS یک عدد کاملاً تصادفی و دلخواه به نام X انتخاب می‌کند با شرط $1 \leq X \leq p-2$ انتخاب می‌کند.

۲ هر بلوک mi را طبق رابطه (۵) به دو عدد تبدیل می‌کند و برای AWS می‌فرستد.

$$(G^{X} \bmod P) + k\ ,(mi * \beta^{X} \bmod P) + k \qquad (5)$$

بدین ترتیب بلوک‌های متن که رمز می‌شود CPS می‌تواند برای بلوک‌های متوالی X را تغیر دهد

آنچه AWS به ازای هر بلوک رمز شده دریافت می‌کند عبارت است از زوج عدد صحیح (μ, λ) که مطابق با آنچه گفته شد طبق روابط (۶) و (۷) به دست آمده‌اند.

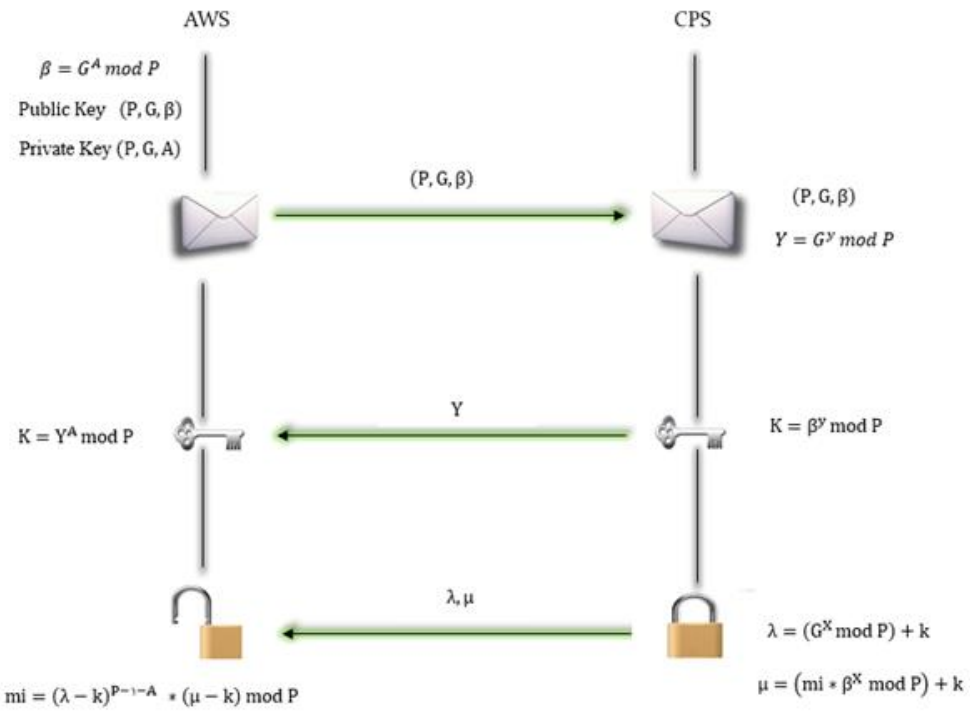
$$\lambda = (G^{X} \bmod P) + k \qquad (6)$$

$$\mu = (mi * \beta^{X} \bmod P) + k \qquad (7)$$

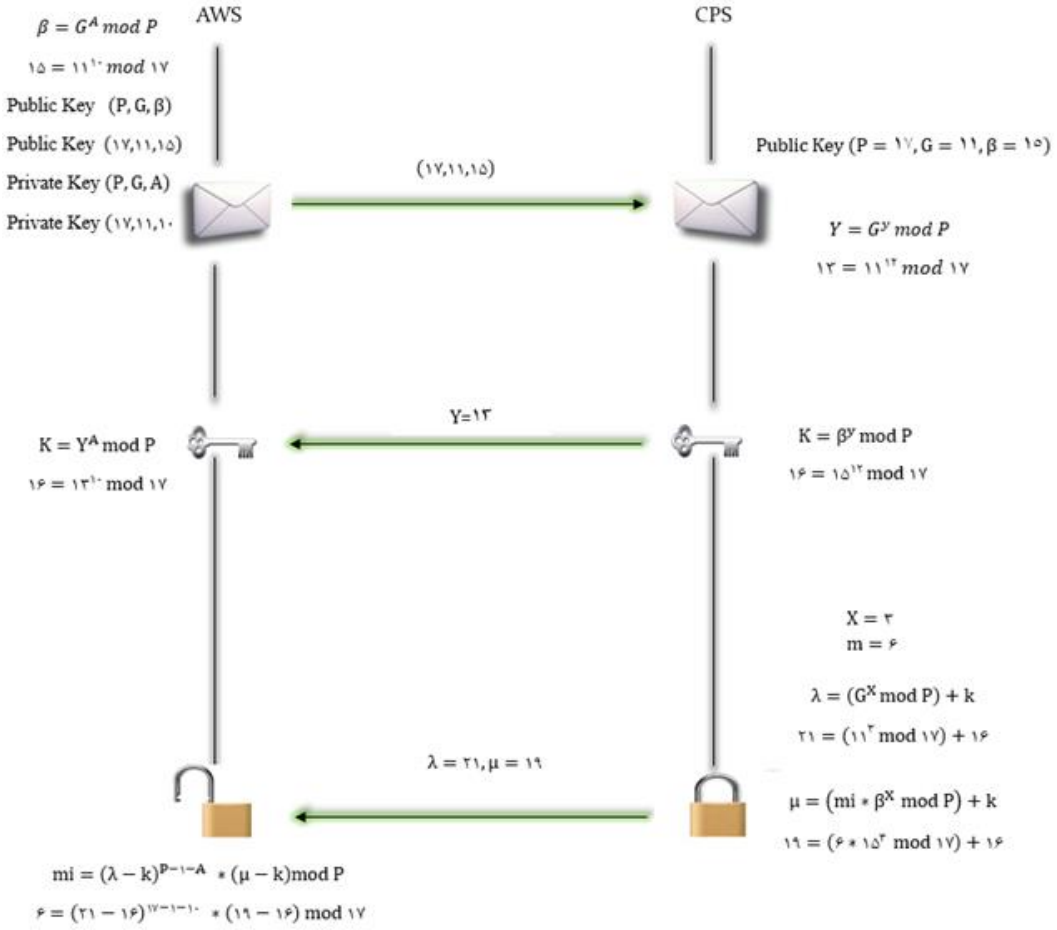
AWS 5 می‌تواند طبق رابطه (۸) داده‌های رمز شده را رمزگشایی کند.

$$mi = (\lambda - k)^{P-1-A} * (\mu - k) \bmod P \qquad (8)$$

در شکل ۲ می‌توان ارتباط AWS و CPS را با روش پیشنهادی را دید و شکل ۳ این ارتباط را با مثلاً عددی نشان می‌دهد.



شکل ۲. روش پیشنهادی بین AWS و CPS را نشان می‌دهد.



شکل ۳ . روش پیشنهادی بین AWS و CPS را با مثال عددی نشان می‌دهد.

۶. اثبات درستی روش رمزنگاری

در سیستم رمزنگاری پیشنهادی یک بلوک عددی به نام **M** با انتخاب عددی تصادفی به نام **X** و محاسبه دو عدد **λ** و **μ** به صورت زیر انجام می‌شود.

$$\mu = mi * \beta^X \bmod P$$

$$\lambda = G^X \bmod P$$

مقادیر $(\mathbf{P}, \mathbf{G}, \boldsymbol{\beta})$ سه تایی مشهور به کلید عمومی هستند. حال رابطه رمزگشایی را در نظر بگیرید.

$$m = (\lambda - k)^{P-1-A} * (\mu - k) \bmod P$$

با جایگذاری مقادیر (P, G, β) در رابطه بالا داریم:

$$m = (G^X \bmod P)^{P-1-A} * (m * (G^A)^x \bmod p) \bmod p$$

باتوجه به آنکه عملگر mod بر روی ضرب (و پیروی آن بر روی توان) خصوصیت پخشی و معکوس آن را دارد خواهیم داشت:

$$m = (G^X)^{P-1-A} * (m * (G^A)^x) \bmod p$$

با بهره‌گیری از ویژگی جابه‌جایی و شرکت پذیری عمل ضرب پیمانه‌ای:

$$= (m * (G^{P-1-A})^x * (G^A)^x) \bmod p$$

$$= (m * (G^{P-1-A} * G^A)^x) \bmod p$$

$$= (m * (G^{P-1})^x) \bmod p$$

طبق قضیه فرما یعنی $A^{P-1} \overset{P}{\equiv} 1$ داریم.

$$= (m * (1)^x) \bmod p$$

$$= m \bmod p$$

۷. شبیه سازی

این بخش نتیجه حاصل از انجام شبیه سازی برای شکستن روش پیشنهاد شده با سایر الگوریتم‌های مشابه با استفاده از حمله جستوجوی فراگیر را اریه می دهد.

۷-۱. محیط شبیه سازی

این بخش محیط شبیه سازی طرح پیشنهادی در برابر حمله جستوجوی فراگیر را شرح میدهد.

برای انجام آزمایشات از یک کامپیوتر Dell با قدر پردازنده core i7 . 2.30 GHz، بار حافظه ۸ گیگابایتی استفاده شده است. تمامی پیاده‌سازی حملات جستجوی فراگیر در نرم‌افزار MATLAB 2013a انجام شده است و به علت بینهایت بودن اعداد و عدم وجود پردازنده قوی تمام آزمایشات روی اعداد ۱ تا ۱۰۰ انجام شده است.

۷-۲. حملات جستجوی فراگیر

در این میان به خاطر اینکه نمی‌توان به‌صورت مستقیم به الگوریتم‌های رمزنگاری که بر پایه لگاریتم گسسته طراحی‌شده‌اند حمله کرد بنابراین از روش‌های مانند جستجوی فراگیر یا حمله جستجوی فراگیر فضای کلید [] استفاده می‌شود. جستجوی فراگیر حمله‌ای است که در آن تمام حالات ممکن تا رسیدن به جواب بررسی می گردد. برای هر الگوی رمزنگاری می‌توان زمان لازم برای آزمودن کلیه حالات ممکن برای کلید را محاسبه نمود و معمولاً الگوهای رمزنگاری آن‌چنان طراحی می‌شوند که آزمودن تمامی حالات ممکن در یک‌زمان قابل قبول غیرممکن و یا غیر مؤثر باشد. جستجو به روش brute-force به سادگی قابل پیاده‌سازی می‌باشد و همیشه جواب مسئله را در صورت وجود می‌یابد. با این حال، به دلیل اینکه هزینه‌های آن متناسب با تعداد نامزدهای حل مسئله است، استفاده از آن در بسیاری از مسائل عملی، که تعداد نامزدهای حل مسئله تمایل به رشد بسیار سریع با افزایش اندازه مسئله را دارد، امکان‌پذیر نیست. این روش هنگامی به کار می‌رود که اندازه مسئله محدود می‌باشد همچنین حمله جستجوی فراگیر یک معیار برای شناخت روش‌های شکستن رمز است به این معنی که هر روشی که سریع‌تر از روش حمله جستجوی فراگیر بتواند رمز را بازگشایی نماید، یک روش شکستن رمز تلقی می‌شود.آزمودن کلیه حالات ممکن روشی برای یافتن گذرواژه نیز به کار می‌رود. به طور معمول نرم‌افزارها پس از چند بار وارد کردن گذرواژه نادرست حساب کاربر را مسدود نموده و یا در فرایند اعتبارسنجی تأخیر زمانی ایجاد می‌کنند تا از آزمودن دیگر حالات جلوگیری شود. شکل ۴ شبه کد استفاده شده برای حمله جستجوی فراگیر فضای کلید نشان می‌دهد.

```
For (P = ۰; P = N; P + +)
{
  For (a = ۰; a = N − ۲; a + +)
{
    For (K = ۰; K = N − ۲; K + +)
{
    CT۱ = C۱ − K
    CT۲ = C۲ − K
M۱ = (CT۱)^(P−۱−a) * (CT۲)
M  = M۱ % P
IF (M == ۶ && P == ۱۷ && a = ۱۰ && K == ۲)
{
Cout << M <</n
Cout << P <</n
Cout << a <</n
Cout << K <</n
}
}
}
```

شکل۴. شبه کد حمله جستجوی فراگیر فضای کلید.

۷-۳. سناریو شبیه سازی حمله جستجوی فراگیر

سناریو حالت اول روش پیشنهادی و روش الجمل رو بدون در نظر گرفتن اعداد اول به صورت کورکورانه به جستوجو می‌پردازد.

سناریو حالت دوم روش پیشنهادی و روش الجمل با در نظر گرفتن اعداد اول صورت می گیرد.

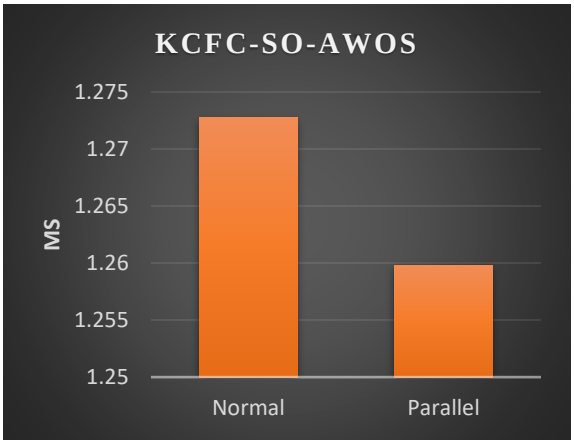
هر دو سناریوهای شبیه سازی در دو وضعیت نرمال و موازی پیاده‌سازی شده است.

۷-۴. نتایج شبیه سازی

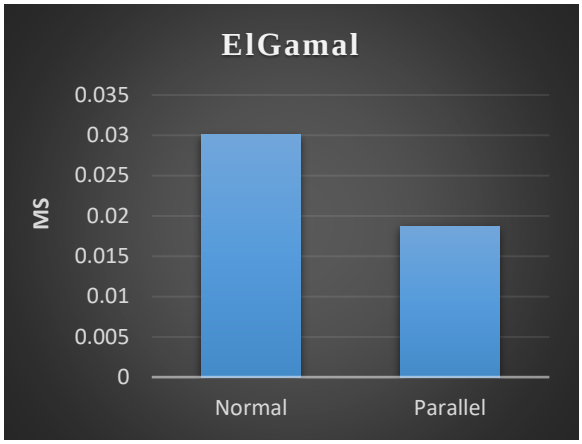
۷-۴-۱. سناریو اول

سناریو اول با درنظر گرفت اعداد اول اجرا میشود. که حالت نرمال روش پیشنهادی برای پیدا کردن کلید رمز در حالت جستوجوی فرا گیر به زمان ۱.۲۷۲۷۳۸ ثانیه نیاز دارد در صورتی زمان شکستن روش الجمل ۰.۰۳۰۱۴۱ ثانیه است و در حالت موازی روش پیشنهادی ۱.۲۵۹۸۰۴ زمان صرف میکند برای پیدا کردن کلید رمز و روش الجمل ۰.۰۱۸۷۰۷ ثانیه است. نتایج شبیه

سازی نشان می دهد روش پیشنهادی در برابر حمله جستوجوی فرا گیری در حالت های نرمال و موازی زمان بیشتری برای پیدا کردن کلید رمز نسبت به روش الجمالی نیاز دارد. شکل ۵ و شکل ۶ زمان پیدا کردن کلید رمز با وضعیت نرمال و موازی را به ترتیب نشان می دهد.



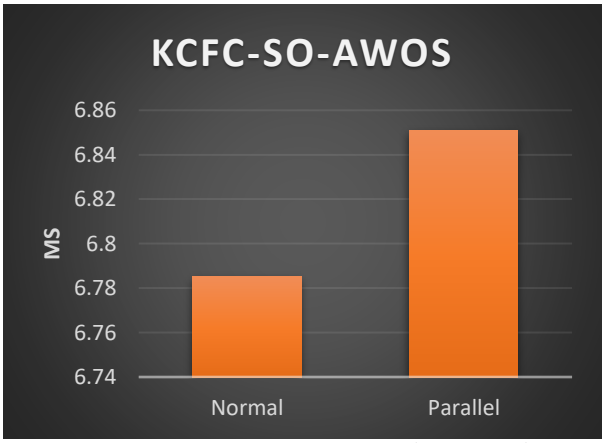
شکل ۵. نتایج عملکرد روش پیشنهادی در سناریو اول را نشان میدهد.



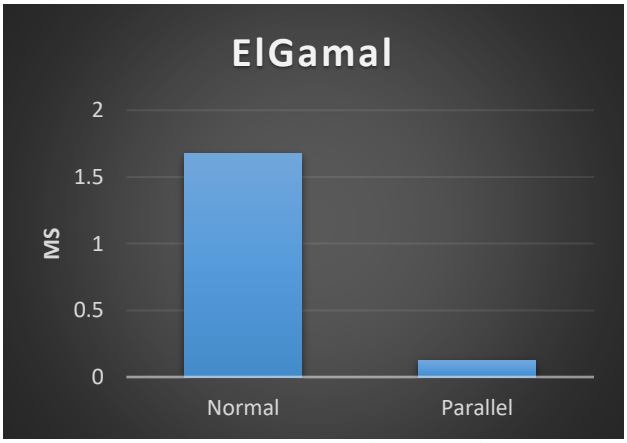
شکل ۶. نتایج عملکرد روش الجمل در سناریو اول را نشان میدهد.

۷-۴-۲. سناریو دوم

سناریو دوم بدون درنظر گرفت اعداد اجرا شده است. روش پیشنهادی در حالت نرمال برای پیدا کردن کلید رمز در حالت جستوجوی فرا گیر به زمان ۶.۷۸۵۱۱۶ ثانیه نیاز دارد در صورتی زمان شکستن روش الجمل ۱.۶۷۲۹۲۴ ثانیه است و در حالت موازی روش پیشنهادی ۶.۸۵۰۸۸۱ زمان صرف میکند برای پیدا کردن کلید رمز و روش الجمل ۰.۱۲۶۰۲۵ ثانیه است. نتایج شبیه سازی نشان میدهد روش پیشنهادی در برابر حمله جستوجوی فرا گیری در حالت های نرمال و موازی زمان بیشتری نیاز دارد برای پیدا کردن کلید رمز نسبت به روش الجمالی. شکل ۷ و شکل ۸ زمان پیدا کردن کلید رمز با وضعیت نرمال و موازی را به ترتیب نشان میدهد .



شکل ۷ نتایج عملکرد روش پیشنهادی در سناریو دوم



شکل ۸ نتایج عملکرد روش الجمل در سناریو دوم

نتیجه گیری

در سراسر دنیا برای رمزنگاری و رمزگشایی اطلاعات از سیستم‌های رمزگذاری متقارن و نامتقارن استفاده می‌شود. الگوریتم‌هایی که بر پایه سیستم‌های متقارن ساخته‌شده‌اند دارای سرعت بسیار بالا برای رمزنگاری و رمزگشایی داده هستند ولی

در عوض الگوریتم‌های نامتقارن دارای انعطاف‌پذیری بالا و همچنین استحکام بیشتر نسبت به الگوریتم‌های متقارن هستند. با وجود الگوریتم‌های رمزنگاری متعدد هیچ یک از این الگوریتم‌ها توانایی ایجاد یک کانال امن بین فرستنده و گیرنده را ندارند ما در این مقاله با ترکیب سیستم رمزنگاری الجمال و الگوریتم تبادل کلید دیفی هلمن یک روش رمزنگاری جدید ارائه کرده‌ایم که برخلاف روش موجود قابلیت تبادل کلید برای فرستنده و گیرنده از کلید عمومی مهیا می‌کند به‌گونه‌ای که دیگر نیاز نیست برای رمزنگاری و تبادل کلید از دو الگوریتم متفاوت استفاده شود و همچنین این قابلیت را برای رمز کننده پیام فراهم می‌آورد که به ازای یکایک بلوک‌های متن پیام مقدار **X** را تغییر بدهد در این حالت هر بلوک با مقادیر متفاوت رمزگذاری خواهد شد. بدون آنکه گیرنده پیام مجبور به انجام هیچ کار اضافی برای رمزگشایی آن‌ها باشد.یکی از نقاط قوت این الگوریتم وجود پارامتر **X** برای تغیر پویایی الگوی رمزنگاری به ازای بلوک‌های متوالی پیام است پارامتری که در سایر روش های رمزنگاری وجود ندارد. الگوریتم پیشنهادی ما توانست در مقایسه با الگوریتم الجمل که بر اساس لگاریتم گسسته طراحی شده است توانست مدت زمان بیشتر در مقابله حملات جستجوی فراگیر مقاومت کند به عبارت دیگر شکستن الگوریتم پیشنهادی نسبت به الگوریتم الجمل هزینه بیشتری را می‌طلبد.

منابع:

1. R. Fotohi, Y. Ebazadeh, and M. S. Geshlag, “A New Approach for Improvement Security against DoS Attacks in Vehicular Ad-hoc Network,” *arXiv*, 2020, doi: 10.14569/ijacsa.2016.070702.
2. Y. Ebazadeh and R. Fotohi, “A reliable and secure method for network-layer attack discovery and elimination in mobile ad-hoc networks based on a probabilistic threshold,” Secur. Priv., vol. 5, no. 1, p. e183, 2022.
3. Y. Salami, F. Taherkhani, Y. Ebazadeh, M. Nemati, V. Khajehvand, and E. Zeinali, “Blockchain-Based Internet of Vehicles in Green Smart City: Applications and Challenges and Solutions,” *Anthropog. Pollut.*, vol. 7, no. 1, 2023.
4. Y. Salami and V. Khajehvand, “LSKE: Lightweight Secure Key Exchange Scheme in Fog Federation,” *Complexity*, vol. 2021, p. 4667586, 2021.
5. M. Wazid and P. Gope, “BACKM-EHA: A novel blockchain-enabled security solution for IoMT-based e-healthcare applications,” *ACM Trans. Internet Technol.*, vol. 23, no. 3, pp. 1–28, 2023.
6. C.-M. Chen, S. Liu, X. Li, S. K. H. Islam, and A. K. Das, “A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT,” *J. Syst. Archit.*, vol. 136, p. 102831, 2023.
7. H. Corrigan-Gibbs and D. Kogan, “The discrete-logarithm problem with preprocessing,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2018, pp. 415–447.
8. D. Boneh, “The Decision Diffie-Hellman problem,” in *Algorithmic Number Theory*, J. P. Buhler, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 48–63.
9. P. C. van Oorschot and M. J. Wiener, “On Diffie-Hellman Key Agreement with Short Exponents,” in *Advances in Cryptology --- EUROCRYPT ’96*, U. Maurer, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 332–343.
10. R. L. Rivest, a Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978, doi: 10.1145/359340.359342.
11. Y. Salami, V. Khajevand, and E. Zeinali, “Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges,” *J. Comput. Robot.*, vol. 16, no. 2, pp. 46–56, 2023.
12. D. Pointcheval, “Rabin Cryptosystem,” in *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg, Ed., Boston, MA: Springer US, 2005, pp. 501–502. doi: 10.1007/0-387-23483-7_339.
13. K. S. Selvi and T. Vaishnavi, “Rabin PublicKey Cryptosystem for mobile authentication,” in *IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012)*, Mar. 2012, pp. 854–860.
14. Y. Salami, V. Khajehvand, and E. Zeinali, “SOS-FCI: a secure offloading scheme in fog–cloud-based IoT,” *J. Supercomput.*, pp. 1–31,

Comput. Robot., vol. 13, no. 1, pp. 11–20, 2020.

15. Y. Salami, Y. Ebazadeh, and V. Khajehvand, "CE-SKE: cost-effective secure key exchange scheme in Fog Federation," *Iran J. Comput. Sci.*, vol. 4, no. 3, pp. 1–13, 2021.
16. G. Lowe, "Breaking and fixing the Needham-Schroeder public-key protocol using FDR," in *International Workshop on Tools and Algorithms for the Construction and Analysis of Systems*, Springer, 1996, pp. 147–166.
17. Y. Salami, V. Khajehvand, and E. Zeinali, "E3C: A Tool for Evaluating Communication and Computation Costs in Authentication and Key Exchange Protocol," 2022, doi: 10.48550/ARXIV.2212.03308.
18. M. Burrows, K. Kas, and T. Ta, "Wide mouthed frog," *Secur. Protoc. Open Repos. http//www. lsv. ens-cachan. fr/Software/spore/wideMouthedFrog. html*, 1989.