همگام‌سازی مجدد کلید در بستر اینترنت اشیای بُرد بلند و توان پایین

امیر جلالی بیدگلی* و عباس دهقانی

گروه مهندسی رایانه و فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه قم، قم، ایران

گروه مهندسی رایانه، دانشکده فنی و مهندسی، دانشگاه یاسوج، یاسوج، ایران

چکیده

اینترنت اشیای برد بلند و توان پایین (LPWAN) به دسته‌ای از فناوری‌های ارتباطی در اینترنت اشیا گفته می‌شود که دارای مصرف بسیار پایین و در عین حال برد ارتباطی بلند هستند. در کنار مزایای مختلف، این فناوری‌ها محدودیت‌های بسیاری نیز از جمله پهنای باند کم، ارسال بدون اتصال و قدرت پردازشی پایین دارند که روش‌های رمزنگاری در این بستر را دچار چالش کرده است. یکی از مهم‌ترین این چالش‌ها، زنجیره‌سازی رمز در این بستر است. حجم بسیار کوچک پیام و احتمال ازدست‌رفتن بسته بدون اطلاع دروازه و دستگاه، باعث می‌شود هیچ از یک روش‌های متداول زنجیره‌سازی رمز مانند CBC، OFB و یا CTC در بستر اینترنت اشیا توان پایین امکان‌پذیر نباشد؛ چون هر یک از این روش‌ها یا باید بر روی یک بستر اتصال‌گرا باشد و یا بخشی از حجم بسته ارسالی را با روش‌های مانند ارسال شمارنده و یا HMAC مصرف کند. در این مقاله، روشی جدیدی جهت همگام‌سازی مجدد فرستنده و گیرنده در صورت از دست رفتن یک بسته ارائه می‌شود که به وسیله آن قادر خواهیم بود در محدویت‌های LPWAN، رمزنگاری را در حالت زنجیره‌ای انجام داد. روش پیشنهادی قادر است بدون استفاده از فضای پیام ارسالی، همگام‌سازی طرفین را انجام دهد. نتایج شبیه‌سازی بیان‌گر این است که روش پیشنهادی در محیط‌های که احتمال ازدست‌رفتن چند بسته پشت سر هم، پایین است، کارآیی قابل قبولی دارد.

واژگان کلیدی: اینترنت اشیای توان پایین و دوربرد، رمزنگاری، همگام‌سازی کلید، چکیده‌سازی

Key Resynchronizing in Low Power Wide Area Networks

Amir Jalaly Bidgoly* & Abbas Dehghani

Department of Computer Engineering and Information Technology,
University of Qom, Qom, Iran.
Department of Computer Engineering, Faculty of Engineering,
Yasouj University, Yasouj, Iran

Abstract

LPWANs are a class of technologies that have very low power consumption and high range of communication. Along with its various advantages, these technologies also have many limitations, such as low bandwidth, connectionless transmission and low processing power, which has challenged encryption methods in this technologies. One of the most important of these challenges is encryption. The very small size of the message and the possibility of packet loss without the gateway or device awareness, make any of the cipher chaining methods such as CBC, OFB or CTC impossible in LPWANs, because either they assume a connection oriented media or consume part of the payload for sending counter or HMAC. In this paper, we propose a new way to re-synchronize the key between sender and receiver in the event of a packet being lost that will enable us to perform cipher chaining encryption in LPWAN limitation. The paper provides two encryption synchronization methods for LPWANs. The first method can be synchronized in a similar behavior as the proof of work in the block chain. The second proposed method is able to synchronize the sender and receiver with the least possible used space of the message payload. The proposed method is able to synchronize the parties without

* Corresponding author

* نویسندهٔ عهده‌دار مکاتبات

•تاریخ ارسال مقاله: ۱۳۹۷/۱۰/۲۹ •تاریخ پذیرش: ۱۳۹۹/۰۵/۲۸ •تاریخ انتشار: ۱۴۰۰/۰۳/۰۱ •نوع مطالعه: پژوهشی

using the payload. The proposed method is implemented in the Sigfox platform and then simulated in a sample application. The simulation results show that the proposed method is acceptable in environments where the probability of missing several consecutive packets is low.

Keywords: LPWAN, Encryption, Key Re-Synchronization, Hashing

۱- مقدمه

اینترنت اشیای یک شبکه از اشیای فیزیکی است که امکان برقراری ارتباط اشیا با یکدیگر و همچنین تعامل با محیط بیرون را فراهم می‌کند. اشیا اطلاعات مفید را با کمک فناوری‌های مختلف جمع‌آوری می‌کنند، داده‌ها را سپس به‌صورت خودکار بین دستگاه‌های دیگر به جریان می‌اندازد. کاربردهای اینترنت اشیا روزبه‌روز فزونی می‌یابد. طبق پیش‌بینی گارتنر[1] تا سال ۲۰۲۰، ۲۵ میلیون شیء به اینترنت متصل خواهند شد [1] و بیش از نیمی از کسب و کارهای جدیدی به‌نحوی به اینترنت اشیا مرتبط هستند [2]. تصویرسازی اینتل حتی بزرگ‌تر از این است. این شرکت دویست میلیارد دستگاه متصل به اینترنت را تا سال ۲۰۲۰، پیش‌بینی می‌کند. Business Insider پیش‌بینی می‌کند که کل هزینه‌های کسب و کار در اینترنت اشیا، تا سال ۲۰۲۱ به شش تریلیون دلار خواهد رسید. پیش‌بینی‌ها بیان‌گر این است که در سال ۲۰۱۷، ۶۰ درصد از تولیدکنندگان جهانی از تجزیه و تحلیل داده‌های جمع‌آوری‌شده از دستگاه‌های متصل به اینترنت برای تحلیل فرایندها و شناسایی امکانات بهینه استفاده خواهند شد [3].

فناوری‌های ارتباطی اینترنت اشیا بر اساس دو ویژگی محدوده ارتباطاتی و مصرف انرژی دسته‌بندی می‌شوند (شکل۱). هر دسته مشخص می‌کند که یک شیء حداکثر در چه فاصله‌ای از دروازه[2] قادر به اتصال به شبکه خواهد بود و همچنین مصرف انرژی لازم برای اتصال به دروازه چه مقدار است. بر همین اساس، فناوری‌های ارتباطی اینترنت اشیا به چهار دسته تقسیم می‌شود که در زیر آمده است:

۱) برد کوتاه و توان بالا که مهم‌ترین فناوری‌های آن می‌توان به WiFi – ۸۰۲,۱۱ اشاره کرد که مشکل اصلی این فناوری، این است که لازم است یک نقطه اتصال[3] در محدوده ارتباطی آنتن شیء که حداکثر صد متر است در دسترس باشد؛ علاوه‌براین مصرف انرژی در این فناوری بالاست؛

۲) برد کوتاه و توان کم که از مهم‌ترین فناوری‌های آن را می‌توان به LR-WPAN[4] و BLE[5] اشاره کرد. این فناوری‌ها مصرف انرژی دستگاه برای اتصال به دروازه را به مقدار قابل‌توجهی کاهش داده‌اند و اما هنوز برد کوتاهی دارند و در اشیای متحرک و محیط‌های گسترده قابل استفاده نیستند؛

۳) برد بلند و توان بالا که مهم‌ترین آن‌ها 2G/3G/4G است؛ از این فناوری می‌توان در کاربردهای گسترده و اشیای متحرک استفاده کرد؛ اما نقطه ضعف آن‌ها مصرف بالای انرژی است؛ به‌نحوی که یک شیء متکی به باتری نمی‌تواند بیش از چند ساعت بدون شارژ مجدد باتری به فعالیت خود ادامه دهد؛

۴) برد بلند و توان کم که مهم‌ترین نمونه این فناوری‌ها LoRaWAN، SigFox و NB-IOT هستند. این فناوری‌ها، نه‌تنها قادر هستند که ارتباط یک شیء با دروازه را حتی در بردهای چند ده کیلومتری امکان‌پذیر سازند، بلکه مصرف انرژی بسیار پایینی دارند و می‌توانند با یک باتری معمولی تا چندین سال کار کنند.

(شکل-۱): مقایسه فناوری‌های ارتباطی در اینترنت اشیا

(Figure-1): Comparison of communication technologies in the Internet of Things.

ویژگی‌های برجسته فناوری‌های ارتباطی دوربرد و توان پایین، شبکه LPWAN[6] را بسیار مورد توجه و مستعد استفاده در بسیاری از کاربردها کرده و درعمل در کاربردهای صنعتی، شهری و بازرگانی تنها گزینه مطرح در اینترنت اشیا هستند. در [4] گزارش شده است ۵۵٪ سهم بازار در حوزه اینترنت اشیا به محصولات LPWAN اختصاص داده شده است. به‌عنوان نمونه فناوری Sigfox یک شیء را قادر می‌سازد با یک باتری تا دوازده سال

[1] http://www.gartner.com
[2] Gateway
[3] Access point
[4] Low-Rate Wireless Personal Area Networks
[5] Bluetooth Low Energy
[6] Low Power Wide Area Network

فعالیت داشته باشد. از همین ویژگی می‌توان در ساخت ردیاب‌هایی با قابلیت عملکرد تا ده سال بدون نیاز به شارژ یا تعویض باتری استفاده کرد. چنین ردیابی در صنایع مختلفی مانند ردیابی بار، کودکان و سالمندان کاربرد دارد. کسب و کارها در حوزه اینترنت اشیا در ایران نیز به‌سرعت رو به گسترش و رشد هستند [4, 5]. پژوهشکده ارتباطات و فناوری اطلاعات وزارت ارتباطات و فناوری اطلاعات[1] متولی رسمی اینترنت اشیا در ایران است. طبق گزارش‌های رسمی و پیش‌بینی این پژوهشکده در مورد اینترنت اشیای توان پایین و دوربرد در ایران [4] «فناوری‌هایLPWAN تا سال ۱۴۰۰ در ایران به تکامل خواهند رسید و سهم غالب اینترنت اشیا را در ایران تصاحب خواهند کرد». در حال حاضر نخستین درگاه اختصاصی اینترنت اشیای توان پایین و دوربرد کشور از سال ۱۳۹۴ در منطقه نارمک تهران بر بستر LORAWAN راه‌اندازی شده است. همچنین در همکاری انجام‌شده بین ایران و فرانسه با سرمایه‌گذاری بیش از ۱۶۰ میلیون دلار برنامه‌ریزی جهت پوشش سرتاسری ایران طی یک سال آینده با Sigfox در حال انجام است [6]. در پیشنهادهای رسمی مطرح‌شده توسط نهادهای دولتی نیز به‌طوررسمی از اینترنت اشیای توان پایین به‌عنوان یک از قیود لازم برای انجام پروژه یاد شده است [5].

برخلاف جذابیت و کاربردهای روزافزون اینترنت اشیای توان پایین، محدودیت‌های این بستر چالش‌های بسیاری را نیز به‌وجود آورده است. یکی از مهم‌ترین این چالش مسائل مربوط به رمزنگاری ارتباطات است. محدودیت شدید حجم پیام‌های ارسالی، محدودیت‌های تعداد ارسال و دریافت پیام و همچنین احتمال ازدست‌رفتن بسته در حین ارسال باعث می‌شود، هیچ‌یک از روش‌های زنجیره‌سازی رمز در این بسترها قابل اجرا نباشند. به‌عنوان نمونه جهت پیاده‌سازی روش مبتنی بر شمارنده (CTR) لازم است، شماره پیام به همراه بسته ارسال شود که حتی اگر طول آن، دو بایت هم باشد، یک‌ششم از حجم بسته ارسالی در بستری مانند Sigfox را اشغال می‌کند. بدون ارسال اطلاعاتی مانند شمارنده گیرنده در صورت ازدست‌رفتن یک پیام، پیام‌های بعدی را با کلید اشتباه باز خواهند کرد. در حال حاضر هیچ روش زنجیره‌سازی رمزی وجود ندارد که قادر باشد بدون مصرف پهنای باند، همگام‌سازی کلید فرستنده و گیرنده را در رمزنگاری زنجیره‌ای انجام دهد.

[1] https://www.itrc.ac.ir

در این مقاله با الگوگرفتن از شیوه تولید اثبات کار در زنجیره بلاک، روشی جهت همگام‌سازی کلید در رمزنگاری ارائه شده است که می‌تواند حتی در صورت ازدست‌رفتن پیام نیز مجدد کلید طرفین را به حالت همگام برگرداند. این روش با تعریف ماژولی به نام AKF[2] به هر پیام یک کلید اختصاصی منتسب می‌کند؛ ازاین‌رو قادر است، با دریافت یک پیام حتی اگر پیام‌های قبلی از دست رفته باشد، کلید صحیح را جهت رمزنگاری/رمزگشایی بیابد.

نوآوری‌های مقاله به‌صورت دقیق به‌شرح زیر است:

ارائه دو روش همگام‌سازی زنجیره رمز برای اینترنت اشیا دوربرد و توان پایین (LPWAN).

روش نخست (حالت کاری صفر) با الگوگرفتن از اثبات کار در زنجیره بلاک بدون نیاز به ارسال شمارنده یا ارسال گواهی دریافت پیام[3] می‌تواند در صورت ازدست‌رفتن یک پیام از زنجیره مجدد آن را همگام‌سازی کند. روش پیشنهادی دوم (حالت کاری یک) قادر است فرستنده و گیرنده را با مصرف کمینه فضای ممکن از پیام همگام سازد.

روش پیشنهادی می‌تواند در هر بستر پهنای باند کم و بدون اتصال[4]، برای زنجیره‌سازی رمز استفاده شود.

مقاله بدین‌صورت ادامه پیدا می‌کند. در بخش دوم چالش‌های رمزنگاری در اینترنت اشیای توان پایین و انگیزه پژوهش به‌صورت جزئی‌تر بررسی خواهد شد. بخش سوم به مدل‌سازی مسأله و روش پیشنهادی می‌پردازد. بخش چهارم ارزیابی‌های انجام‌شده جهت ارائه کارایی روش را بررسی می‌کند و مقاله درنهایت در بخش آخر با جمع‌بندی و نتیجه‌گیری پایان می‌پذیرد.

۲- پیشینه پژوهش

به رغم مزایای بسیار شبکه‌های LPWAN، برخی محدودیت‌ها مانند حجم بسیار محدود پیام، قدرت محاسبات پایین و شبکه ارتباطی بدون اتصال (عدم امکان ارسال تصدیق پیام[5])، پروتکل‌های رمزنگاری را با چالش‌های جدید مواجه کرده‌اند. توان پایین فرستنده‌های این بستر، نیاز به طراحی الگوریتم‌های سبک‌وزنی دارند که بتواند با مصرف پایین انرژی، سرعت پایین پردازنده و حافظه محدود عمل کنند. پژوهش‌گران حوزه امنیت،

[2] Appropriate Key Finder
[3] Acknowledgement
[4] Connection-less
[5] Acknowledgment

روش‌های رمزنگاری سبک‌وزن بسیاری را برای این حوزه معرفی کرده‌اند. این روش‌ها نسبت به روش‌های متداول به‌طورمعمول تعداد دور کمتر و کلید کوتاه‌تر دارند. PRESENT [7]، TEA [8]، RC5 [9]، ECDH [10]، LEDs [11]، HISEC [12]، HIGHT [13]، OLBCA [14]، DLBCA [15]، TWINE [16]، PRINCE [17]، PRINT [18]، Lblock [19] و KLEIN [20] مهم‌ترین کارها در این زمینه هستند. برای مثال PRESENT که یکی از سبک‌ترین روش‌های رمزنگاری است بر پایه SPN[1] چهار بیتی است. تعداد دور این روش ۳۲ دور، کلید رمزنگاری آن ۸۰ یا ۱۲۸ بیتی و بلوک ورودی آن ۶۴ بیتی است. این روش را می‌توان در ۹۳۶ خط کد در میکروکنترلرهای معمولی پیاده‌سازی کرد که نسبت به سایر پروتکل‌های رمزنگاری بسیار کمتر است. Simon and speck [21] نیز یکی از خانواده‌های مهم در روش‌های رمزنگاری سبک‌وزن است که با حمایت سازمان امنیت آمریکا طراحی شده است. ویژگی منحصربه‌فرد این خانواده از روش‌های رمزنگاری، پشتیبانی از حالات مختلفی طول کلید و طول بلوک ورودی است که آن را قابل استفاده در هر کاربردی می‌سازد. ارائه‌دهندگان این روش نشان دادند که Simon and speck بر روی همه سخت‌افزارهای مطرح در حوزه اینترنت اشیا پیاده‌سازی می‌شود. در [22]، روش‌های رمزنگاری سبک‌وزن از دیدگاه اندازه بلوک، اندازه کلید و تعداد دور، ارزیابی و بررسی شده است.

مسأله مدیریت کلید نیز از مسائل مورد علاقه پژوهش‌گران بوده است. اغلب این پژوهش‌ها بر روی LoraWAN انجام شده است. علت این امر، متن‌بازبودن این بستر و همچنین به‌روزبودن پروتکل‌های آن است. درحالی‌که بسترهای مختلفی مانند Sigfox هنوز هیچ سازوکاری جهت رمزنگاری ارائه نداده‌اند، بستر LoRaWAN سازوکار رمزنگاری دوسطحی برای رمزکردن پیام‌ها بین دستگاه و سرور و همچنین رمزنگاری نقطه‌به‌نقطه[2] پیاده‌سازی کرده است. LoRaWAN دو حالت OTAA و ABP را به این منظور پیاده‌سازی کرده است. Jaehyu و همکاران [23] روشی را جهت به‌روزرسانی کلید در هر دو حالت بالا به نام Dual Key-Based ارائه داده است. این روش یک جفت کلید جدید برای حالات بالا بر اساس DevAddr و DevNonce تولید می‌کند. Sarra و همکاران [24] از نظام‌های شهرت[3] برای افزایش امنیت مدیریت کلید و کاهش مصرف انرژی کمک گرفته‌اند. Kevin و همکارانش [25] با ترکیب روش‌های رمزنگاری متقارن و کلید عمومی، روشی جهت رمزنگاری پیام‌های درخواست پیوستن به شبکه[4] ارائه داده است. پیام‌های درخواست پیوستن به شبکه در LoRaWAN رمز نمی‌شود و باعث حملات مختلفی به این شبکه شده است. SeLPC[5] [26] با استفاده از D-Box روشی جهت کاهش تعداد دور در AES است که قادر به تولید کلید و رمزنگاری پیام است. در [27]، روش‌های RSA، Diffie-Hellman و ECC[6] جهت تبادل کلید در شبکه‌های توان پایین و دوربرد اینترنت اشیا مقایسه شده‌اند.

برخلاف پژوهش‌های بسیاری که در حوزه روش‌های رمزنگاری در شبکه LPWAN مطرح شده، اما چالش‌های زنجیره‌سازی رمز کمتر مورد توجه پژوهش‌گران قرار گرفته است. برای زنجیره‌سازی رمز، هر بلوک از پیام باید وابسته به بلوک‌های قبلی و بعدی رمز شود؛ به این صورت که تغییر در یک بلوک از پیام بر روی رمز بلوک‌های دیگر تأثیر بگذارد. روش‌های ارائه‌شده توسط پژوهش‌گران بیشتر به ارائه یک روش رمزنگاری بلوکی توجه دارد. بدون زنجیره‌سازی رمز این روش‌ها باید در حالت دفترچه رمز (ECB[7]) استفاده شوند. در این حالت یک پیام مستقل از پیام‌های دیگر رمز می‌شود؛ از این رو رمز یک پیام مانند x همیشه کدی مثل y خواهد شد؛ مستقل از این‌که چند بار و در چه زمانی ارسال شود. در این حالت اگرچه هرچند محرمانگی پیام حفظ‌شده و شکستن رمز با توجه به استفاده از الگوریتم‌های رمزنگاری استاندارد به‌سادگی میسر نیست، اما با درنظرگرفتن حجم وسیعی پیام‌های ارسالی و دنباله آن‌ها این مسأله چالش‌های بسیاری را برای این رده از اینترنت اشیا ایجاد می‌کند.

به‌عنوان نمونه فرض کنید ما روش رمزنگاری بلوکی X را که در آن $E_K(m)$ و $D_K(m)$ نماد تابع رمزگذاری و رمزگشایی با استفاده از کلید K است، در اختیار داریم، X می‌تواند هرگونه رمزگذاری مطرح و یا سبک‌وزن باشد. فرض کنید این روش قرار است در رمزنگاری یک کاربرد اینترنت اشیای توان پایین و برد بلند مانند اندازه‌گیری مصرف آب در شبکه Sigfox استفاده شود. حس‌گر مصرف آب (w: مقدار اعشاری به طول چهار بایت)، فشار (p: مقدار اعشاری به طول چهار بایت)، وضعیت دستگاه و درجه حرارت (t,s: مقادیر صحیح به طول دو بایت) را اندازه‌گیری و هر سی دقیقه در شبکه ارسال می‌کند. حجم پیام ارسالی به‌طوردقیق دوازده معادل بیشینه حجم پیام در

[1] Substitution-permutation network
[2] End to end encryption
[3] Reputation Systems
[4] Joint Request
[5] Secure Low Power Communication
[6] Elliptic Curve Cryptography
[7] Encryption Code Book

Sigfox است. حال رمزنگاری پیام‌های ارسالی به‌وسیلهٔ رمزنگاری X، می‌تواند به‌صورت شکل (۲) استفاده شود. نخستین چالش برای رمزگذاری بین پیام‌های دو و سه ایجاد می‌شود. همان‌طور که مقادیر متغیرها در طی سی دقیقه گذشته تغییر نکرده است، محتوای پیام و به همین ترتیب رمزها یکسان هستند؛ بنابراین یک مهاجم با شنود به‌سادگی می‌تواند نتیجه‌گیری کند چیزی تغییر نکرده و بر این اساس، استنباط می‌شود که آبی در این مدت مصرف نشده و خانه به‌احتمال خالی است.

برای حل این چالش، دو راه موجود است، نخست آن‌که که یک مقدار تصادفی به هر پیام اضافه و دوم آن‌که از روش زنجیره‌سازی رمز استفاده شود. قراردادن یک مقدار تصادفی به‌وضوح غیرممکن است؛ زیرا فضای موجود در پیام پر شده است و امکان قراردادن داده بیشتری در پیام‌های حس‌گر نیست. جهت زنجیره‌سازی رمز می‌تواند از روش‌های مطرح در این حوزه مانند روش CTR[1] استفاده کرد. نتیجه اجرای این روش در شکل (۳) نمایش داده شده است.

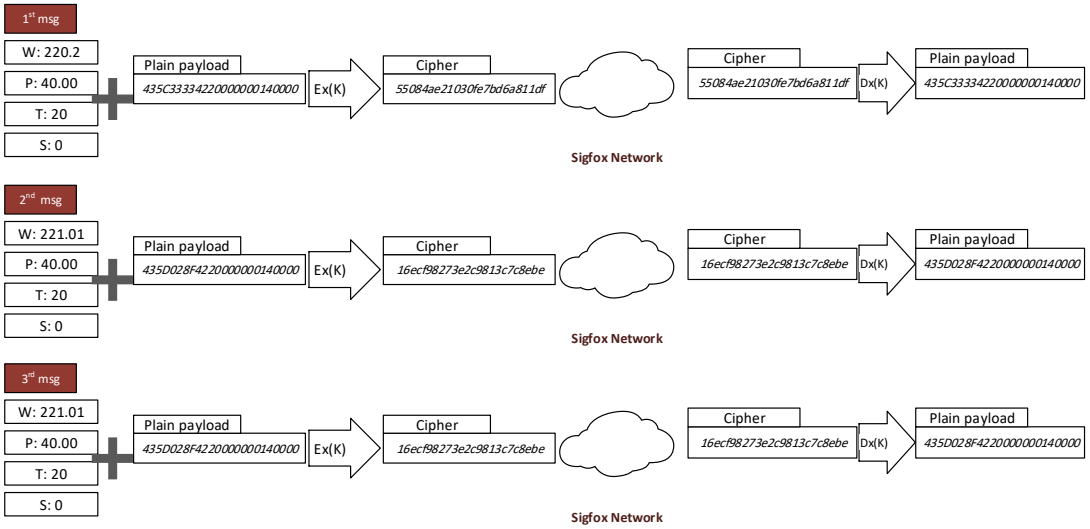
همان‌طور که در شکل (۳) مشاهده می‌کنید، اگر یک پیام در حین انتقال از دست برود مشکل دیگری را در رمزنگاری به‌وجود می‌آورد. LPWAN جهت حفظ ویژگی مصرف پایین خود باید از سازوکارهای خاصی جهت ارسال پیام استفاده کند؛ برای مثال، پیام از سوی دستگاه به‌صورت ناهماهنگ[2] ارسال می‌شود. دستگاه پیام را با فرکانس و زمان تصادفی[3] منتشر می‌کند. دروازه‌های شبکه مسئول دریافت پیام‌های بسیاری از اشیا هستند که ممکن است پیام خود را از راه دور، به‌طورمعمول چند کیلومتر، حتی ده کیلومتر، ارسال کنند. با درنظرگرفتن همه این موارد، ازدست‌دادن یک پیام در شبکه‌های LPWAN بسیار محتمل است، هرچند ازدست‌رفتن یک پیام به‌خودی‌خود مشکلی ایجاد نمی‌کند؛ چون این دستگاه‌ها به‌طورمعمول برای ارسال اطلاعات بحرانی و اورژانسی استفاده نمی‌شوند؛ علاوه‌براین، با توجه به ویژگی‌های LPWAN و محدودیت‌های دریافت و ارسال پیام، پیام تصدیق دریافت نیز وجود ندارد؛ ازاین‌رو، نه فرستنده و نه گیرنده متوجه ازدست‌رفتن پیام در حین ارسال نخواهند شد. با توجه به این موارد، در شکل (۳) پس از ازدست‌رفتن پیام دوم، شمارنده گیرنده افزایش نمی‌یابد؛ درحالی‌که شمارنده فرستنده به سه افزایش یافته است. درنتیجه گیرنده نه‌تنها پیام بعدی را به‌اشتباه باز می‌کند، بلکه تمام پیام‌های آینده را نیز نخواهد توانست به‌درستی رمزگشایی کند.

تمامی روش‌های زنجیره‌سازی رمز مانند زنجیره‌سازی بلوکی (CBC[4]) یا بر اساس بازخورد (CFB[5]) نیاز به بستر بااتصال و حفظ ترتیب پیام‌ها دارد؛ بنابراین درصورت ازدست‌رفتن یک پیام دچار چالش می‌شوند. در برخی از روش‌ها فرستنده شمارنده و یا اطلاعاتی را که برای ساخت شماره پیام لازم است، نیز همراه پیام ارسال می‌کند. CTR بدون وضعیت[6] و پروتکل DTLS[7] [28] و بسیاری از پروتکل‌های ثبت‌شده از چنین رویکردی بهره می‌برد. برای نمونه در ماژول رمزنگاری ثبت‌شده توسط ویلسون[8] [29] خود شمارنده به همراه پیام ارسال می‌شود. مشکل اصلی این روش‌ها این است که حتی اگر مقدار شمارنده پیام یک رقم صحیح هم باشد، حجم دو الی چهار بایت از فضای پیام را اشغال می‌کند. این حجم برای فضای بسیار محدود پیام‌ها در شبکه LPWAN به‌طورمعمول در دسترس نیست (برای نمونه در شکل (۳))، ازاین‌رو امکان استفاده از آن‌ها در بستر اینترنت اشیای توان پایین که دارای پهنای باند محدود هستند، مناسب نیست.

در دیگر کارهای انجام‌شده از یک عدد تصادفی برای تولید کلید هر پیام ارسال که این عدد نیز به همراه پیام ارسال می‌شود [30, 31]. در برخی دیگر از روش‌ها، نشانه‌ای همراه پیام ارسال می‌شود که گیرنده با کمک آن می‌تواند تشخیص دهد با کلید درست در حال باز کردن پیام است. برای نمونه در ماژول ارائه‌شده [32]، به‌همراه پیام یک برچسب (چکیده) از اطلاعات پیام ارسال می‌شود، گیرنده با کلید خود پیام را باز می‌کند و اگر چکیده پیام بازشده با برچسب دریافت شده مطابقت داشت، آن را می‌پذیرد؛ در غیر این صورت شمارنده خود را افزایش داده و همین روند را با کلید بعدی تکرار می‌کند. با این روش گیرنده می‌تواند ترتیب کلیدهای خود را با فرستنده حتی در صورت ازدست‌رفتن پیام حفظ کند. در [33] این ماژول‌ها در حالت کلی شرح داده شده‌اند. رویکردهای ارائه‌شده، همگی نیاز به افزودن سربار به پیام داشته و استفاده از آن‌ها در بستر پهنای محدود اشیای توان پایین مقدور نیست. به‌اختصار، هیچ یک از رمزنگارهای زنجیره‌ای حال حاضر قادر نیستند بدون افزودن به طول پیام در یک بستر بدون اتصال عمل کنند؛ ازاین‌رو طراحی یک پروتکل جدید و نوآورانه از چنین رمزنگاری مورد نیاز است.

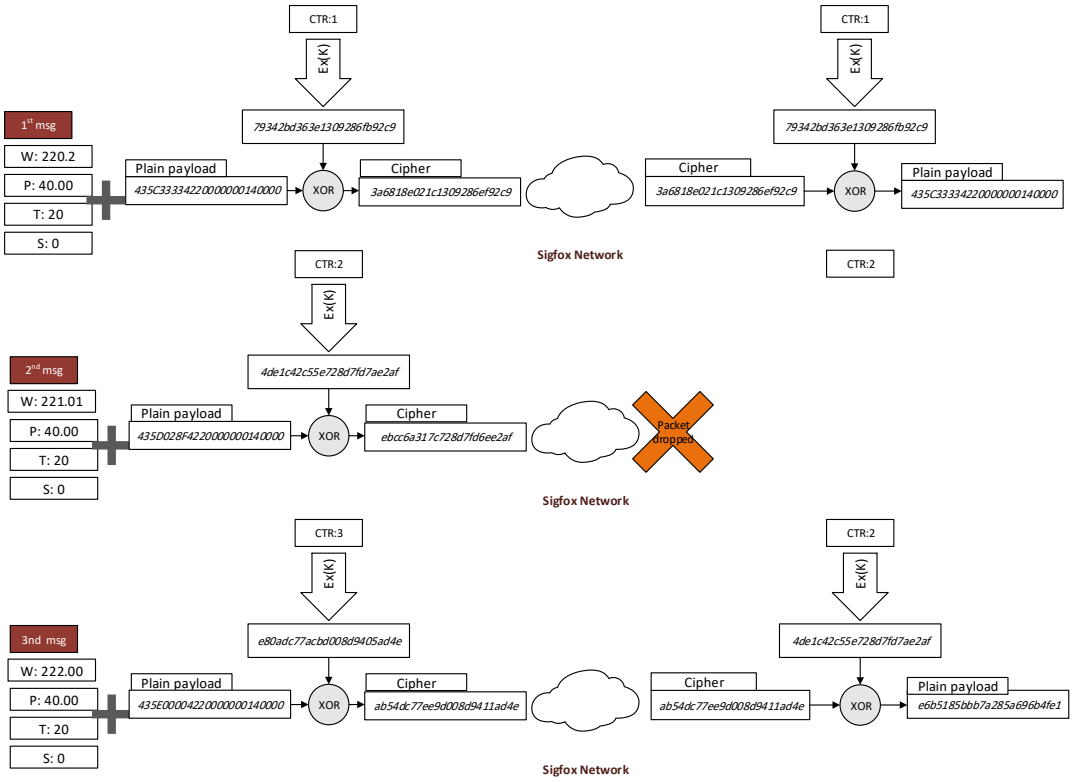
[1] Counter mode encryption
[2] Unsynchronized
[3] Time and frequency diversity

[4] Cipher Block Chaining
[5] Cipher Feedback
[6] Stateless CTR
[7] Datagram Transport Layer Security
[8] Wilson



(شکل-۲): نمونه ارسال پیام در شبکه Sigfox در حالت رمزنگاری بلوکی

(Figure-2): Example of sending a message in Sigfox network in block cipher mode.



(شکل-۳): نمونه ارسال پیام در شبکه Sigfox در حالت رمزنگاری CTR

(Figure-3): Example of sending a message in Sigfox network in CTR encryption mode

۳- روش پیشنهادی

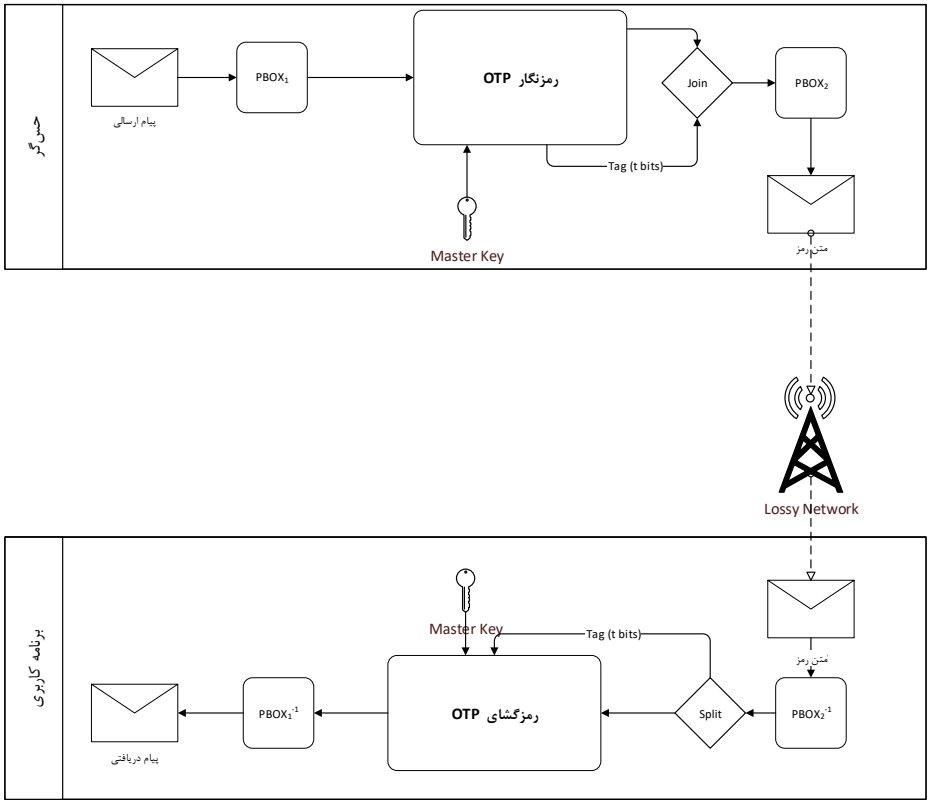
زنجیره‌سازی رمز در روش پیشنهادی این مقاله، بر پایه تولید کلیدهای یک‌بارمصرف[1] با استفاده از مولد اعداد تصادفی LFSR[2] است. رمزنگار دارای دو حالت کاری[3] است که با عنوان حالت کاری صفر و یک شناخته می‌شوند. در حالت کاری یک، فرض بر این است که رمزنگار می‌تواند بخشی بسیار کوچکی از فضای پیام (در حد چند بیت) مصرف کند. این بخش از پیام با چکیده‌ای[4] از وضعیت مولد LFSR به نام برچسب کلید[5] پر می‌شود که رمزنگار به واسطه آن می‌تواند در صورت ازدست‌رفتن ارتباط مجدد، شاخص کلیدهای خود را با گیرنده همگام کند. در این حالت کاری، طول پیام قابل استفاده توسط کاربر به واسطه استفاده بخشی از فضا توسط برچسب کلید کاهش می‌یابد. هرچند این فضا به کمینه ممکن می‌تواند کاهش یابد، ولی ممکن است در برخی از کاربردها این کار

[1] One Time Pad
[2] Linear Feedback Shift Register
[3] Working Mode
[4] Hash
[5] Key Tag

مقدور نباشد. حالت کاری صفر برای رفع این مشکل طراحی شده است. در این حالت کاری، رمزنگار بدون استفاده از هیچ بخشی از فضای پیام سعی می‌کند تا ارتباط خود را با گیرنده حتی در صورت ازدست‌رفتن ارتباط، همگام نگه دارد. همان‌طورکه در بخش قبل شرح داده شد، هیچ‌یک از رمزنگارهای زنجیره‌ای حال حاضر قادر نیستند بدون افزودن اطلاعات به طول پیام در چنین شرایطی عمل کنند، ازاین‌رو پیاده‌سازی حالت کاری صفر، شامل طراحی یک پروتکل جدید و نوآورانه رمزنگاری است که در نوع خود نخستین نمونه از چنین رمزنگارهایی است. در ادامه به‌ترتیب این دو حالت کاری شرح داده می‌شود. با توجه به ساده‌تر بودن حالت کاری یک، ابتدا این حالت کاری شرح داده می‌شود.

۱-۳- حالت کاری یک

ایده اصلی در حالت کاری یک، افزودن یک برچسب به پیام جهت همگام‌سازی گیرنده و فرستنده است. شمای طراحی این حالت کاری را در شکل (۴) مشاهده می‌کنید.



(شکل-۴): معماری رمزنگار در حالت کاری یک

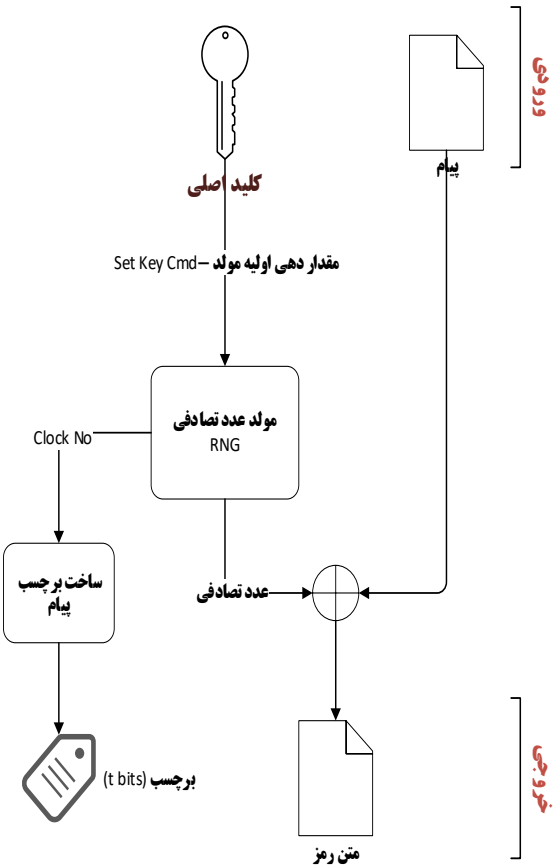
(Figure-4): Cryptographic architecture in working mode one.

فرآیند رمزنگاری شامل استفاده از دو PBOX[1]، یک رمزنگار OTP و یک جعبه ترکیب[2] است. ابتدا پیام توسط PBOX درهم‌ریخته می‌شود و سپس رمزنگار OTP آن را رمز می‌کند. در این فرآیند علاوه بر رمز، برچسبی هم به‌عنوان خروجی تولید می‌شود. رمز و برچسب در مرحله بعد در جعبه ترکیب با هم ادغام و پس از به‌هم‌ریختن مجدد، توسط PBOX2 ارسال می‌شوند.

مهم‌ترین وظیفه در این طراحی را ماژول رمزنگار OTP به عهده دارد. شمای این ماژول را در شکل‌های (۵ و ۶) می‌توان مشاهده کرد. رمزنگاری بر اساس تولید کلید توسط مولد عدد تصادفی RNG انجام می‌شود (RNG استفادشده برپایه LFSR و الگوگرفته از A5/1 [34] است). این مولد لازم است با کلید مقداردهی اولیه شود، این کار تنها یک‌بار در هنگام تنظیم‌کردن کلید انجام می‌شود. رمز با XOR کردن کلید تولیدشده به‌وسیلهٔ RNG و پیام تولید می‌شود؛ علاوه‌بر رمز، این ماژول شمارنده ساعت[3] مولد RNG را هم به‌عنوان برچسب طبق رابطه زیر کد می‌کند:

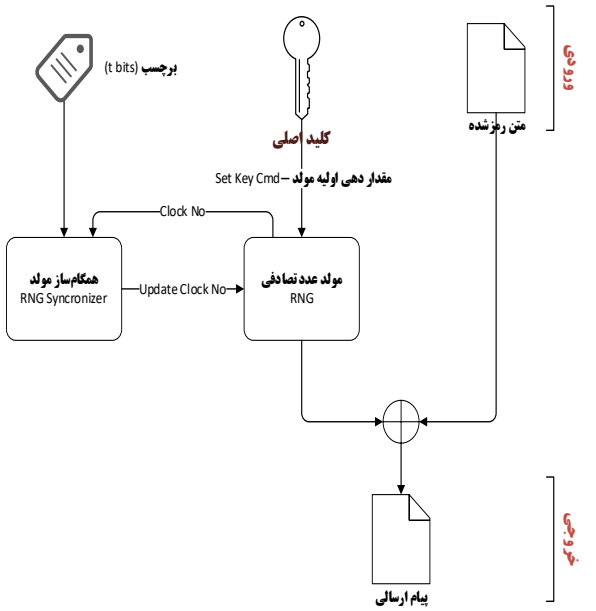
$$Tag = Clock \bmod 2^t \qquad (۱)$$

[1] Permutation Box
[2] Merge
[3] Clock No



(شکل-۵): ماژول رمزنگار OTP در حالت کاری یک

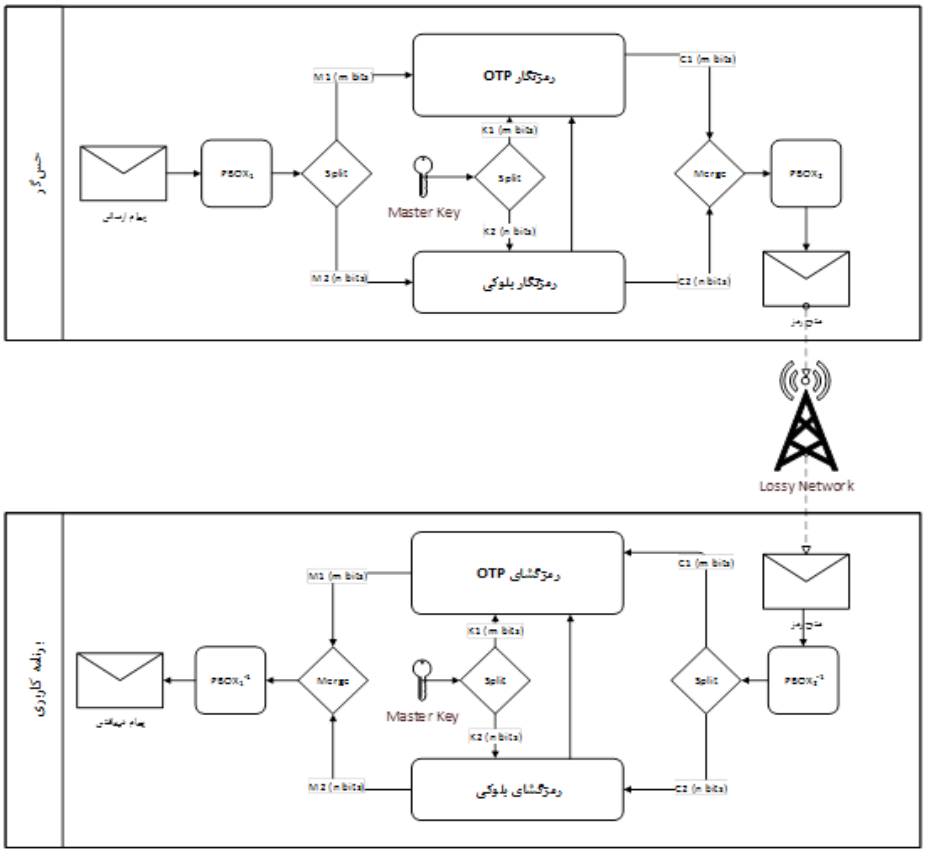
(Figure-5): OTP encryption module in working mode one.



(شکل-۶): ماژول رمزگشای OTP در حالت کاری یک

(Figure-6): OTP decryption module in working mode one.

با توجه به این‌که برچسب لزوماً باید t بیت باشد، برچسب برابر با شمارنده به پیمانه 2^t در نظر گرفته شده است. گفتنی است که از فضای قابل استفاده در پیام t بیت به برچسب اختصاص داده می‌شود؛ بنابراین طول پیام در این حالت کاری t بیت کمتر از بیشینه فضای موجود است.



(شکل-۷): معماری کلی رمزنگار در حالت کاری صفر

(Figure-7): General cryptographic architecture in zero working mode

فرآیند رمزگشایی پیام در رمزنگار در شکل (۶) نمایش داده شده است. ساختار این ماژول مشابه با رمزنگار است و از XOR رمز و کلید تولیدشده به‌وسیلهٔ RNG استفاده می‌کند. برچسب دریافت‌شده در این ماژول جهت همگام‌سازی مولد استفاده می‌شود. شمارنده ساعت مولد درحقیقت شاخص کلید دستگاه است. درصورتی‌که یک پیام از دست برود، طبق توضیحات قبلی شاخص گیرنده یک واحد از شاخص فرستنده عقب می‌افتد. گیرنده می‌تواند با مقایسه شمارنده خود با برچسب از این موضوع آگاه شده و شمارنده خود را به جلو حرکت دهد. با توجه به طول برچسب، ازدست‌رفتن حداکثر 2^t پیام با این روش قابل مدیریت است. به‌عنوان‌مثال اگر t=1 باشد، رمزنگار تنها در برابر ازدست‌رفتن یک پیام مقاوم است. با توجه به احتمال از دست رفتن پیام‌ها می‌توان در صورت نیاز t را افزایش یا کاهش داد. اگر P احتمال ازدست‌رفتن یک پیام باشد، احتمال ازدست‌رفتن k پیام پشت سر هم با استفاده از توزیع هندسی[1] قابل محاسبه است؛ بنابراین پیشنهاد می‌شود t برابر با امید ریاضی این توزیع یعنی $1/P$ در نظر گرفته شود.

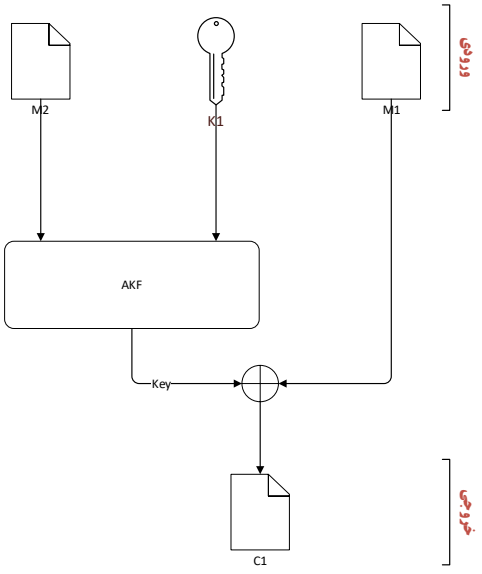
۲-۳- حالت کاری صفر

شمای کلی معماری رمزنگار در شکل (۷) مشاهده می‌شود. ساختار رمزنگاری بر پایه یافتن کلید اختصاصی رمزنگاری/رمزگشایی برای هر پیام و سپس رمزکردن/بازکردن پیام به واسطه آن است. رمزنگار دارای دو PBOX، چند جعبه تقسیم[2] و ترکیب دو ماژول رمزنگار OTP و رمزنگار بلوکی[3] است. ایده اصلی در حالت کاری این است که با تقسیم اطلاعات به دو بخش، یک بخش به‌صورت بلوکی رمز شود تا بتوان سمت گیرندهٔ آن را از رمز خارج و از اطلاعات آن برای همگام‌سازی دو طرف استفاده کرد. گفتنی است در این حالت کاری هیچ بخشی از فضای پیام توسط رمزنگار استفاده نمی‌شود.

همان‌طور که در شکل مشاهده می‌شود، در ابتدا بیت‌های پیام ارسالی به‌وسیلهٔ PBOX نخست به هم ریخته و سپس پیام و کلید به دو بخش n و m بیتی شکسته می‌شود. بخش n بیتی پیام که M2 نام‌گذاری شده به‌وسیلهٔ یک رمزنگار بلوکی متقارن با کلید k2 (بخش nبیتی کلید) رمز و بخش دیگر پیام با کلید k1 توسط رمزنگار OTP رمز می‌شود. فرآیند این رمزنگار به اطلاعات رمزنگار بلوکی وابسته است و از این اطلاعات جهت همگام‌سازی خود استفاده می‌کند، درنهایت خروجی این دو رمزنگار باهم ترکیب و پس از به‌هم‌ریختن مجدد، به‌وسیلهٔ PBOX دوم توسط فرستنده ارسال خواهد شد.

رمزنگاری در ماژول رمزنگار بلوکی توسط یک تابع رمزنگار متقارن انجام می‌شود. این تابع هر رمزنگار متقارن می‌تواند باشد، به‌شرط آن‌که ورودی و خروجی n بیتی داشته باشد و به‌علاوه سریع بوده و قابلیت پیاده‌سازی سخت‌افزاری نیز داشته باشد. لازم به توضیح است در پیاده‌سازی فعلی از XOR برای این منظور استفاده شده است.

فرآیند رمزنگار OTP در شکل (۸) قابل مشاهده است. رمز نهایی مشابه با حالت کاری یک، با XOR پیام و کلید به دست می‌آید، اما فرآیند تولید کلید در این حالت کاری با حالت کاری قبل متفاوت است. چالش اصلی این ماژول این است که به هر پیامی کلید اختصاصی انتساب داده شود تا اگر یک پیام در مسیر ارسال از دست رفت، با دریافت پیام بعدی و یافتن کلید اختصاصی آن بتوان از ناهمگام‌شدن ترتیب دنباله کلیدهای گیرنده و فرستنده جلوگیری کرد. ماژول AKF وظیفه یافتن کلید مناسب برای هر پیام را به عهده دارد.



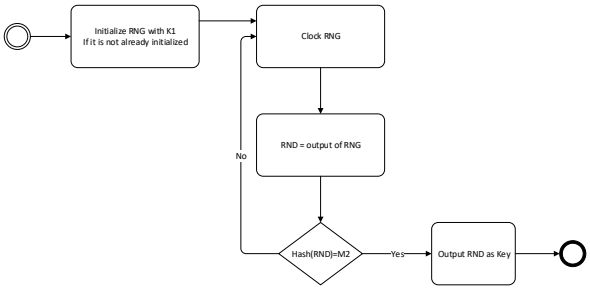
(شکل-۸): ماژول رمزنگار OTP در حالت کاری صفر

(Figure-8): OTP encryption module in zero working mode.

ماژول AKF به هر پیام یک کلید منحصربه‌فرد منتسب و با این کار از خارج‌شدن ترتیب گیرنده و فرستنده جلوگیری می‌کند. الگوریتم ماژول AKF در شکل (۹) قابل مشاهده است. مولد کلید در این ماژول، مولد RNG است. مشابه با حالت قبل این مولد لازم است با کلید مقداردهی اولیه شده باشد. پس از این، ماژول

[1] Geometric distribution
[2] Split
[3] Block Cipher Encryptor

به‌ترتیب خروجی‌های مولد را بررسی می‌کند تا به عددی برسد که چکیده[1] آن با M2 برابر باشد. این عدد به‌عنوان کلید مناسب رمزنگاری به خروجی داده می‌شود. تابع چکیده‌ساز[2] می‌تواند هر تابع دلخواهی باشد به شرط آنکه خروجی آن n بیت باشد.

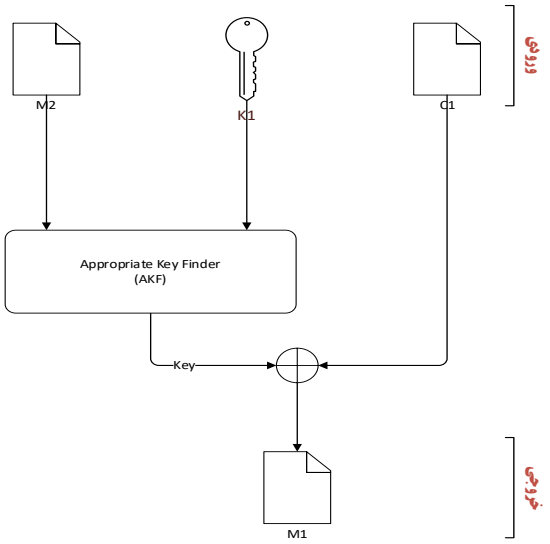


(شکل-۹): الگوریتم یافتن کلید مناسب برای هر پیام در حالت کاری صفر

(Figure-9): Algorithm for finding the key for each message in zero working mode.

فرآیند رمزگشایی ماژول OTP در شکل (۱۰) نمایش داده شده است. این فرآیند به‌طوردقیق مشابه رمزنگار است و از ماژول AKF برای یافتن کلید و با XOR کردن آن با رمز، برای بازتولید پیام استفاده می‌کند. ماژول AKF از M2 برای یافتن کلید مناسب استفاده می‌کند. با توجه به اینکه M2 با رمزنگاری بلوکی رمز شده است، می‌تواند مستقل از زنجیره‌سازی توسط گیرنده رمزگشایی شود.

در این حالت کاری، رمزنگار از سازوکار احتمالاتی برای همگام نگاه داشتن گیرنده و فرستنده استفاده می‌کند. تنها کلیدی برای بازکردن یک پیام مناسب است که $H(key) = M2$ باشد؛ بنابراین حتی درصورتی‌که یک پیام در مسیر از دست برود، سازوکار طراحی‌شده سبب می‌شود که گیرنده با داشتن M2 بتواند کلید مناسب برای پیام بعدی را پیدا کند و دوباره خود را با فرستنده همگام کند. هرچند باید توجه داشت که خروجی تابع چکیده‌ساز ماهیت تصادفی دارد. توزیع احتمالی یافتن کلید در این روش به‌طورکامل منطبق بر توزیع هندسی با احتمال $1/2^n$ است. برای نمونه اگر $n = 4$ باشد، هر عدد خروجی مولد با احتمال $1/16$ ممکن است به‌عنوان کلید تشخیص داده شود؛ بنابراین درصورتی‌که بین شاخص فرستنده و گیرنده فاصله بیافتد، این احتمال وجود دارد که گیرنده در پیام بعدی کلید اشتباهی را انتخاب کند (شاخص دو طرف همگام نشود). هرچند سازوکار احتمالی روش، باعث می‌شود، گیرنده بتواند در درازمدت دوباره خود را با فرستنده همگام کند. درحقیقت احتمال همگام‌نشدن گیرنده و فرستنده در طول زمان با ارسال پیام‌های بیشتر کاهش می‌یابد و ازاین‌رو حتی درصورتی‌که گیرنده نتواند بلافاصله بعد از ازدست‌رفتن یک پیام خود را همگام کند، می‌تواند در طی پیام‌های بعدی شانس خود را جهت همگام‌شدن مجدد با فرستنده افزایش دهد؛ بنابراین در روش پیشنهادی می‌توان اطمینان داشت که گیرنده همواره قادر است بعد از مدتی خود را با فرستنده همگام کند.



(شکل-۱۰): ماژول رمزگشای OTP در حالت کاری صفر

(Figure-10): The mean and median time required to find the key.

۴- شبیه‌سازی و ارزیابی روش پیشنهادی

در این بخش نتایج ارزیابی روش پیشنهادی ارائه شده است. روش رمزنگاری پیشنهادی، در بستر Sigfox پیاده‌سازی شده و سپس در یک کاربرد نمونه شبیه‌سازی شده است. از آنجا که روش پیشنهادی به همگام‌سازی کلید پس از دست رفتن یک بسته پرداخته است، در این شبیه‌سازی فرض می‌شود بسته‌های داده به صورت تصادفی و یا در شرایط تعریف‌شده، در حین ارسال از دست می‌روند و سپس عملکرد سامانه در همگام‌سازی مجدد زنجیره رمز در بسته‌های بعدی ارزیابی شده است.

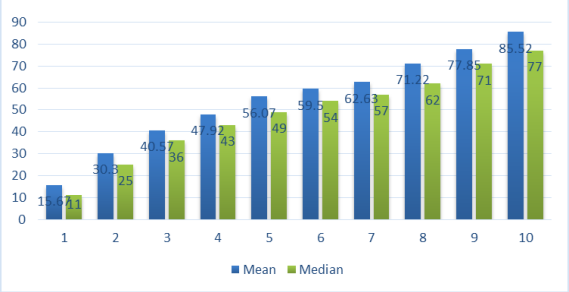
در ادامه، عملکرد روش پیشنهادی در یافتن کلید مناسب، پس از چند رخداد پشت سر هم ازدست‌رفتن بسته بررسی می‌شود. در همه ارزیابی‌ها روش به‌طور

[1] Hash
[2] Hash Function

میانگین برای ده‌هزار بسته شبیه‌سازی شده و همچنین فرض شده است، سامانه در پایان روز (۱۴۰ پیام در بستر Sigfox) به‌صورت دستی همگام می‌شود و داده ارسالی به‌طورکامل تصادفی و بدون هیچ الگوی خاصی است.

۴-۱- هزینه محاسباتی لازم جهت یافتن کلید

فرض کنید مولد LFSR به‌ازای هر واحد زمانی قادر به تولید یک عدد تصادفی است. در این ارزیابی میانگین زمانی لازم جهت یافتن کلید مناسب توسط فرستنده بررسی شده است. این ارزیابی از آن جهت حائز اهمیت است که فرستنده توان پایین و کم‌مصرف بوده و قدرت پردازشی بالایی ندارد؛ ازاین‌رو اگر یافتن کلید به پردازش زیادی در سمت فرستنده نیاز داشته باشد، ممکن است، درعمل قابل استفاده نباشد.



(شکل-۱۱): میانه و میانگین زمان لازم برای یافتن کلید

(Figure-11): The mean and median time required to find the key.

نتایج ارزیابی در شکل (۱۱) نمایش داده است. این شکل میانه[1] و میانگین زمان لازم برای یافتن کلید را نمایش می‌دهد. همان‌طورکه در شکل مشاهده می‌شود؛ برای یافتن یک کلید، میانگین و میانه برابر ۱۵/۶ و ۱۱ است. میانگین به‌شدت به وجود اعداد بزرگ هرچند موردی باشد، حساس است؛ بنابراین نتایج ممکن است، گمراه‌کننده باشد. میانه در این ارزیابی معیار مهم‌تری است چون به‌عنوان نمونه از این آمار می‌توان نتیجه گرفت که در بیش از ۵۰٪ موارد کلید قبل از ۱۱ واحد زمان یافت می‌شود. همان‌طورکه در شکل نمایش داده شده است، برای یافتن دو کلید و بیشتر میانه به‌صورت خطی افزایش نمی‌یابد، به‌عنوان نمونه یافتن ۱۰ کلید در ۵۰٪ موارد در کمتر از ۷۷ واحد زمان انجام می‌شود. همان‌طور که در شرح روش پیشنهادی بیان شد، احتمال یافتن کلید مطابق با توزیع هندسی با احتمال P است که P در اینجا برابر با $1/16$ احتمال تطابق چکیده یک عدد تصادفی با یک رقم ۴ بیتی است. نتایج به‌دست‌آمده نیز به‌طورکامل با توزیع هندسی یادشده تطابق دارد.

[1] Mode

۴-۲- احتمال همگام‌شدن مجدد پس از رخداد ازدست‌رفتن پیام

همان‌طورکه در روش توضیح داده شد، روش پیشنهادی نخستین روش در همگام‌سازی طرفین رمزنگاری است که از سازوکارهای احتمالی استفاده می‌کند. این به این معنی است که این روش ممکن است با احتمالی نتواند بلافاصله پس از رخداد از دست رفتن یک پیام از زنجیره پیام‌ها، خود را مجدد همگام کند. در این ارزیابی احتمال همگام‌شدن فرستنده و گیرنده پس از رخداد ازدست‌رفتن پیام بررسی شده است.

(جدول-۱): احتمال همگام‌شدن پس از ازدست‌رفتن یک پیام از زنجیره پیام

(Table-1): Probability of re-syncing after losing a message from the cipher chain.

شماره پیام	حالت کاری صفر	حالت کاری یک (۴ بیت)	حالت کاری یک (۸ بیت)
۱	0.49	0.87	0.99
۲	0.61	0.97	1.00
۳	0.66	0.99	1.00
۴	0.71	1.00	1.00
۵	0.74	1.00	1.00
۶	0.76	1.00	1.00
۷	0.78	1.00	1.00
۸	0.79	1.00	1.00
۹	0.80	1.00	1.00
۱۰	0.81	1.00	1.00
۱۱	0.82	1.00	1.00
۱۲	0.83	1.00	1.00
۱۳	0.84	1.00	1.00
۱۴	0.84	1.00	1.00
۱۵	0.85	1.00	1.00

نتایج ارزیابی در جدول (۱) نمایش داده شده است. سه حالت کاری صفر، حالت کاری یک با $t = 4$ و حالت کاری یک با $t = 8$ است. همان‌طور که انتظار می‌رود در هیچ یک از روش‌ها بلافاصله پس از ازدست‌رفتن یک پیام زنجیره، طرفین به‌صورت قطعی قادر به همگام‌سازی نیستند، هر چند در حالت کاری یک به‌طورتقریبی این احتمال برابر با یک است، به‌نحوی‌که در حالت $t = 8$ شانس همگام‌سازی برابر با ۹۹/۱٪ است. همچنین در همه حالات این شانس با دریافت پیام‌های بیشتر بالاتر می‌رود. این شواهد بیان‌گر این است که در این روش‌ها فرستنده و

گیرنده قادر خواهند بود پس از دریافت تعداد کافی پیام خود را مجدد همگام سازند. لازم به تأکید است که در شرایط فرض‌شده در این مسأله تنها روش‌های احتمالی قادر به فعالیت هستند، ازاین‌رو هر روش پیشنهادی ممکن است با یک احتمال در همگام‌سازی زنجیره طرفین با شکست مواجه شود.

۳-۴- میانگین تعداد پیام لازم جهت همگام‌سازی

با توجه به نتایج ارزیابی قبلی، این سؤال مطرح می‌شود که به‌طور میانگین چند پیام لازم است تا طرفین بتوانند خود را پس از خارج‌شدن از حالت همگام، مجدد همگام کنند. جهت بررسی این سؤال، روش پیشنهادی در حالت‌های کاری مشابه ارزیابی قبل، جهت به‌دست‌آوردن میانگین تعداد پیام لازم جهت همگام‌سازی مجدد بررسی شده‌اند.

(جدول-۲): میانگین تعداد پیام جهت همگام‌سازی مجدد

(Table-2): Average number of messages to synchronize.

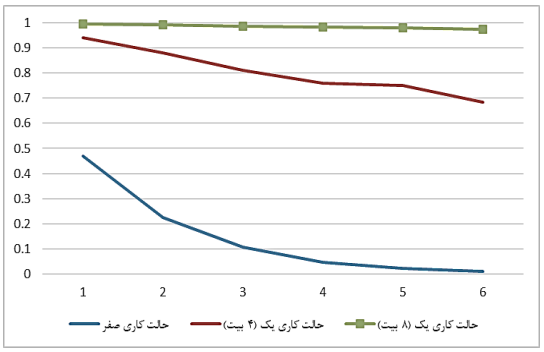
حالت کاری	میانگین تعداد پیام
صفر	6.37
یک ($t = 4$)	0.18
یک ($t = 8$)	0.0097
یک ($t = 12$)	0.0007

جدول (۱) نتایج ارزیابی میانگین پیام لازم جهت همگام‌سازی مجدد را نمایش می‌دهد. همان‌طورکه در جدول نمایش داده شده است، حالت کاری صفر به بیشترین تعداد پیام جهت این امر نیاز دارد، هرچند حتی در این حالت نیز میانگین به‌طورتقریبی تقریباً برابر با شش است. حالت کاری یک نتایج بسیار بهتری را نمایش می‌دهد، به‌نحوی‌که در بهترین حالت در حالت کاری با $t = 12$ طول زنجیره تنها ۰/۰۰۰۷ خواهد بود. این ارزیابی، کارایی روش پیشنهادی را جهت همگام‌سازی درعمل نشان داده است.

۴-۴- همگام‌سازی مجدد پس از رخدادهای ازدست‌رفتن متوالی

در آخرین ارزیابی این بخش، احتمال همگام‌سازی روش پیشنهادی پس ازدست‌رفتن متوالی چند پیام از زنجیره بررسی شده است. با توجه با ماهیت آمار و احتمالی روش پیشنهادی، هدف از این ارزیابی آن است که بررسی کند توالی رخداد تا چه میزان در احتمال همگام‌سازی مؤثر است. نتایج این ارزیابی همچنین نشان می‌دهد هر حالت کاری، حداکثر تا چند رخداد پشت سر هم مقاوم و قابل استفاده است.

نتایج این ارزیابی در شکل (۱۲) نمایش داده شده است. محور افقی تعداد پیام‌های ازدست‌رفته و محور عمودی احتمال همگام‌سازی مجدد با استفاده از روش پیشنهادی و حالات کاری مختلف است. همان‌طورکه انتظار می‌رود احتمال همگام‌سازی با افزایش ازدست‌رفتن زنجیره پیام کاهش می‌یابد. این کاهش در حالت کاری صفر به حدی است که نتایج برای بیش از دو پیام پشت سرهم درعمل قابل‌قبول نیست. این ارزیابی نشان می‌دهد روش پیشنهادی در حالت کاری صفر برای محیط‌هایی که دو رخداد ازدست‌رفتن پشت سر هم وجود دارد، مناسب نیست. نتایج در مورد حالت کاری یک بهتر است. هرچند نتایج در حالت کاری یک و $t = 4$ به‌طورکامل رضایت‌بخش نیست، اما در این حالت کاری و با $t = 8$ احتمال همگام‌سازی با هر تعداد پیام ازدست‌رفته به‌طورتقریبی برابر با یک است.



(شکل-۱۲): احتمال همگام‌سازی مجدد پس از چند رخداد متوالی از دست رفتن پیام

(Figure-12): Probability of re-syncing after several consecutive events of message loss.

۵- جمع‌بندی و کارهای آینده

روش‌های همگام‌سازی زنجیره رمز در شبکه‌های توان پایین و گسترده بلند با چالش‌های جدیدی روبه‌رو هستند. همه روش‌های همگام‌سازی زنجیره رمز نیاز دارند به‌نحوی طرفین از ترتیب بلاک‌ها در زنجیره ارسالی مطلع باشند. این روش‌ها به‌عنوان نمونه فرض می‌کنند در صورت ازدست‌رفتن یک پیام، طرفین مطلع می‌شوند و یا شمارنده پیام به‌همراه آن ارسال می‌شود. در شبکه LPWAN هیچ یک از این فرضیات برقرار نیست. همچنین، هیچ‌یک از رمزنگارهای زنجیره‌ای حال حاضر قادر نیستند بدون

افزودن به طول پیام در یک بستر بدون اتصال عمل کنند. در این مقاله روشی جدید برای همگام‌سازی کلید بین فرستنده و گیرنده در شبکه‌های LPWAN ارائه شده است که قادر است، بدون نیاز به مصرف فضای پیام، در محدودیت‌های این شبکه همگام‌سازی زنجیره رمز را انجام دهد. روش پیشنهادی دارای دو حالت کاری است. در حالت کاری صفر با الگوگرفتن از اثبات کار در زنجیره بلوک، با یافتن کلیدی با چکیده خاص، به هر پیام یک کلید انحصاری اختصاص می‌یابد. در حالت کاری یک، بخش کوچکی از پیام جهت همگام‌سازی طرفین استفاده می‌شود. نتایج نشان می‌دهد روش کاری صفر در محیط‌هایی که احتمال ازدست‌رفتن چند بسته پشت سر هم، پایین است، کارایی قابل قبولی دارد. در مقابل روش کاری یک در همه حالات عملکرد مناسبی از خود نشان داده است، هرچند ناچار به مصرف بخشی از فضای پیام از فضای محدود LPWAN است.

در LPWAN، جهت همگام‌سازی کلید در شرایط مفروض تنها می‌توان از رویکردهای آمار و احتمالی استفاده کرد؛ ازاین‌رو به‌عنوان یکی از کارهای آینده بررسی سایر ایده‌ها و روش‌های آمار و احتمالی مانند امنیت دانش صفر[1] در برنامه قرار دارد؛ همچنین تلاش خواهد شد با ارائه ایده‌های جدید، احتمال همگام‌سازی کلید را در روش پیشنهادی بهبود داد.

6- References ۶- مراجع

[1] S. Barcelona. (Accessed 2015). Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015. Available: http://www.gartner.com/newsroom/id/2905717

[2] C. STAMFORD, "Gartner Says By 2020, More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things," Accessed 2017 2016.

[3] L. ADLER. (2016). How Smart City Barcelona Brought the Internet of Things to Life. Available: http://datasmart.ash.harvard.edu/news/article/how-smart-city-barcelona-brought-the-internet-of-things-to-life-789

[۴] ح. اخوان, م. م. کاشانی, س. ر. احسانی, م. خوشبختیان, and ن. عبدی. (۱۳۹۶). شبکه ارتباطی در اینترنت اشیاء. Available: https://iot.itrc.ac.ir/content/شبکه-ارتباطی-در-اینترنت-اشیاء

[4] H. Akhavan, M Kashani, S. Ehsani, M. Khoshbakhtian, N. Abdi (2017). Communication Networks in Internet of Things. Availabe: https://iot.itrc.ac.ir/content.

[۵] ش. م. گ. ایران, "چارچوب الزامات و انتظارات طرح پایلوت کنتورخوانی هوشمند گاز برای مشترکین خانگی و تجاری جزء," ۱۳۹۵.

[5] Framework of requirements and expectations of the smart gas meter pilot project for home and commercial subscribers, 2016.

[۶] شرکت پارس نت، زیرساخت اینترنت اشیاء. آدرس: www.parsnet.io/خانه/راهکارها-و-خدمات/نحوه-خدمات/،

[6] Parsnet, IoT infrastructure. Available: www.parsnet.io/خانه/راهکارها-و-خدمات/نحوه-خدمات/،

[7] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, C. Vikkelsoe, Present: An ultra-lightweight block cipher, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2007, pp. 450-466.

[8] D. J. Wheeler, R. M. Needham, Tea, a tiny encryption algorithm, in: International Workshop on Fast Software Encryption, Springer, 1994, pp. 363–366.

[9] R. L. Rivest, "The rc5 encryption algorithm", *in: International Workshop on Fast Software Encryption*, Springer, 1994, pp. 86-96.

[10] T. K. Goyal, V. Sahula, "Lightweight security algorithm for low power iot devices", *in: Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on, IEEE*, 2016, pp. 1725-1729.

[11] A. P. J. Guo, T. Peyrin, M. J. B. Robshaw, The led block cipher 6917 ,2011,pp. 326-341.

[12] S. S. M. AlDabbagh, A. Shaikhli, I. F. Taha, M. A. Alahmad, "Hisec: A new lightweight block cipher algorithm", i*n: Proceedings of the 7th International Conference on Security of Information and Networks, ACM*, vol.940, 2014, pp. 151.

[13] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, et al., "Hight: A new block cipher suitable for lowresource device," *in: International*

[1] Zero knowledge security

Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2006, pp. 46-59.

[14] S. S. M. Aldabbagh, I. F. T. Al Shaikhli, "Olbca: A new lightweight block cipher algorithm," *in: 2014 3rd International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, IEEE, 2014, pp. 15-20.

[15] S. S. M. AlDabbagh, Design 32-bit lightweight block cipher algorithm (dlbca), International Journal of Computer Applications 166 (8).

[16] T. Suzaki, K. Minematsu, S. Morioka, E. Kobayashi, Twine: A lightweight, versatile block cipher, in: ECRYPTWorkshop on Lightweight Cryptography, Vol. 2011, 2011.

[17] J. Borgho, A. Canteaut, T. Guneysu, E. B. Kavun, M. Knezevic, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, et al., "Prince-a low-latency block cipher for pervasive computing applications", *in: International Conference on the Theory and Application of Cryptology and Information Security, Springer*, 2012, pp. 208-225.

[18] L. Knudsen, G. Leander, A. Poschmann, M. J. "Robshaw, Printcipher: a block cipher for ic-printing," *in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer*, 2010, pp. 16-32.

[19] W. Wu, L. Zhang, Lblock: "a lightweight block cipher", *International Conference on Applied Cryptography and Network Security, Springer*, 2011, pp. 327-344.

[20] Z. Gong, S. Nikova, Y. W. Law, Klein, "a new family of lightweight block ciphers", *International Workshop on Radio Frequency Identication: Security and Privacy Issues*, Springer, 2011, pp. 1-18.

[21] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "SIMON and SPECK: Block Ciphers for the Internet of Things," *IACR Cryptology ePrint Archive*, vol. 2015, pp. 585, 2015.

[22] T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices," *in Advances in Computing, Communications and Informatics (ICACCI), 2016 International Conference on*, 2016, pp. 1725-1729: IEEE.

[23] J. Kim, J. Song, A dual key-based activation scheme for secure lorawan, Wireless Communications and Mobile Computing 2017.

[24] S. Naoui, M. E. Elhdhili, L. A. Saidane, "Enhancing the security of the iot lorawan architecture, Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)", *International Conference on, IEEE 1020*, 2016, pp. 1-7.

[25] K. Feichtinger, Y. Nakano, K. Fukushima, S. Kiyomoto, "Enhancing the security of over-the-air-activation of lorawan using a hybrid cryptosystem", *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY*, vol. 18 (2), 2018, pp.1-9.

[26] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, C.-H. Tsai, Aes-1030 128 based secure low power communication for lorawan iot environments, IEEE Access 6 (2018) 45325-45334.

[27] A. K. Luhach, "Analysis of lightweight cryptographic solutions for Internet of Things," I*ndian Journal of Science and Technology*, vol. 9, no. 28, 2016.

[28] E. Rescorla and N. Modadugu, "Datagram transport layer security version 1.2," 2012.

[29] A. L. Wilson, "Encryption synchronization combined with encryption key identification," ed: Google Patents, 1993.

[30] P. Epstein, "Key distribution system," ed: Google Patents, 1996.

[31] B .Tehranchi, "Encryption apparatus and method for synchronizing multiple encryption keys with a data stream," ed: Google Patents, 2007.

[32] S. B. Mizikovsky and M. A. Soler, "Automatic resynchronization of crypto-sync information," ed: Google Patents, 20.۰۴

[33] K. Akhavan-Toyserkani and M. Beeler, "Method and system for self synchronizing cryptographic parameters," ed: Google Patents, 2014.

[34] M. Briceno, I. Goldberg, D. Wagner, A pedagogical implementation of A5/1, http://www.scard.org, May 1999.

امیر جلالی بیدگلی مدرک دکترای خود را از دانشگاه اصفهان در سال ۱۳۹۵ رشته مهندسی نرم‌افزار دریافت کرد. وی هم‌اکنون استادیار گروه مهندسی رایانه در دانشگاه قم است. علایق پژوهشی وی، امنیت، یادگیری عمیق و زنجیره بلوکی است.

نشانی رایانامه ایشان عبارت است از:

Jalaly@qom.ac.ir

عباس دهقانی مدرک دکترای خود را از دانشگاه اصفهان در سال ۱۳۹۵ رشته معماری رایانه دریافت کرد. وی هم‌اکنون استادیار گروه مهندسی رایانه در دانشگاه یاسوج است. علایق پژوهشی وی شامل شبکه روی تراشه، اتصالات بی‌سیم روی تراشه، سامانه‌های نهفته و اینترنت اشیا است.
نشانی رایانامه ایشان عبارت است از:
dehghani@yu.ac.ir