سومین کنفرانس بین المللی اینترنت اشیاء و کاربردها
فروردین ۱۳۹۸ - دانشگاه اصفهان

خصوصیات امنیتی در شبکه LoRaWAN

مجید عبدلی[۱*]، حسن شاکری[۲] و طاهره امید[۳]
[۱] دانشجوی دکتری مهندسی فناوری اطلاعات، گروه کامپیوتر، واحد سبزوار، دانشگاه آزاد اسلامی، سبزوار، ایران
majid.abdoli@iaus.ac.ir
[۲]عضو هیأت علمی دانشگاه آزاد اسلامی واحد مشهد، گروه کامپیوتر، مشهد، ایران
shakeri@mshdiau.ac.ir
[۳]مدیرعامل شرکت قالب اینترنت اشیاء آریان، پارک علم و فناوری استان گیلان، واحدهای فناور ICT، رشت، ایران،
setareh.omid97@gmail.com

چکیده : شبکه ***LoRaWAN*** نوعی از شبکه گسترده با توان مصرفی پایین (***LPWAN***) است که ارتباطات کم‌هزینه، متحرک و دوجهته را برای اینترنت اشیا، ارتباط ماشین-ماشین (***M2M***)، شهر هوشمند و کاربردهای صنعتی فراهم می‌کند. پروتکل ***LoRaWAN*** برای مصرف توان پایین بهینه شده است و طوری طراحی شده است که شبکه‌های بزرگ با میلیون‌ها ابزار را پشتیبانی کند. از آن‌جا که امنیت یک نیاز اساسی در تمامی کاربردهای اشاره شده است، از همان ابتدا به عنوان ویژگی‌های اولیه شبکه ***LoRaWAN*** در آن پیاده‌سازی شده است. با این حال، موضوع امنیت شامل نکات متعددی است و به ویژه، مکانیزم‌های رمزنگاری استفاده‌شده برای اجرای امنیت در ***LoRaWAN*** مستلزم توضیح دقیق است. هدف این مقاله بررسی و ارائه ویژگی‌های امنیتی در شبکه فعلی ***LoRaWAN*** است و همچنین به بررسی چند حمله به این شبکه و راهکارهای جلوگیری از آنها می‌پردازیم.

کلید واژه‌ها: اینترنت اشیاء، امنیت، LPWAN، LoRa، LoRaWAN.

۱- مقدمه

با تبدیل اینترنت اشیا به عنوان یک مفهوم اساسی در جوامع مدرن، ادوات مختلفی به یکدیگر متصل شده‌اند. از میکرو سنسورها گرفته تا وسایل خانه و اتومبیل ها، می‌توانیم به همه آنها از راه دور دسترسی داشته باشیم. تعامل بین این تجهیزات و انسان، هسته اصلی اینترنت اشیاء را تشکیل می‌دهد و تکنولوژی‌های ارتباطی، این امر را ممکن می سازد. به بیان دیگر تکنولوژی‌های ارتباطی نقش اساسی در محیط اینترنت اشیاء بازی می‌کنند[۱].

شبکه‌های LPWAN (شبکه گسترده با توان مصرفی پایین) تکنولوژی‌های ارتباطی نوظهوری در دنیای IoT (اینترنت اشیاء) هستند تا ارتباطات بی‌سیم در فواصل طولانی با توان مصرفی پایین را ارائه دهند. شبکه‌های LPWAN به این دلیل مورد توجه ویژه واقع شده‌اند که ارتباطات بی‌سیم راه دور با توان مصرفی پایین توسط شبکه‌های سنتی معمول به درستی ارائه نمی‌شدند. LoRa (برد بلند) یک راه حل لایه فیزیکی است که توسط شرکت SemTech ارائه شده است. این تکنولوژی نیازمندی‌های LPWAN را با مدولاسیون طیف گسترده Chrip بر آورده می‌کند [۲]. LoRa به کمک پروتکل‌های شبکه LoRaWAN (شبکه گسترده برد بلند) که یک پروتکل استاندارد شبکه برای کمینه‌کردن تبادل پیام‌ها است[۳] می‌تواند ناحیه‌ای به وسعت ۱۵ کیلومتر و ۱۰ سال عمر باتری را پوشش دهد[۴]. بنابراین LoRa و LoRaWAN یکی از مناسبترین محیطهای شبکه‌ای برای ادوات با محدودیت مصرف توان است و همین امر آنها را به یکی از پرکاربردترین تکنولوژیهای LPWAN تبدیل کرده است.

امنیت در شبکه LoRaWAN بر اساس همخوانی با معیارهای اصلی طراحی این شبکه طراحی شده است. این معیارها شامل توان مصرفی پایین، پیچیدگی پیاده سازی کم، هزینه پایین و مقیاس‌پذیری بالا است. همواره مصالحه‌ای بین امنیت و هزینه وجود دارد به علاوه به دلیل آنکه این تجهیزات برای مدت زمان طولانی (حتی سالها) در محل مورد نظر خود قرار می‌گیرند، این امنیت باید آینده نگر باشد. در طراحی امنیت LoRaWAN سعی شده است که پایبندی به آخرین قوانین در این حوزه همچون استانداردها و الگوریتمهای تاییدشده رعایت شود و امنیت انتها به انتها به عنوان ایمن‌ترین روش ارتباط راه دور ارائه شده است[5].

در این مقاله، ویژگیهای امنیتی موجود در مشخصات LoRaWAN بیان می‌شود، سپس جزئیات اجرای آن و برخی از توضیحات مربوط به طراحی امنیتی LoRaWan را ارائه خواهیم داد که شامل خصوصیات اصلی است که LoRaWAN برای تامین امنیت استفاده می‌کند. همچون احراز هویت دوطرفه،

حفاظت از صحت اطلاعات و محرمانگی شرح داده می شود. در نهایت حملات مختلف به شبکه LoRaWAN و راهکارهای مقابله با آنها را مورد بررسی قرار خواهیم داد.

۲- ساختار شبکه LoRaWAN

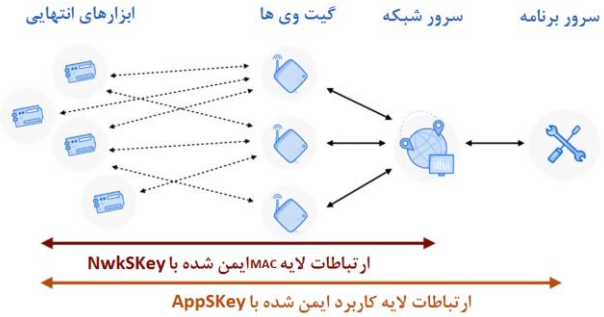
معماری شبکه LoRaWAN به صورت شبکه ستاره‌ای است. این ساختار پروتکلهای ارتباطی را تعریف می‌کند و لایه فیزیکی LoRa امکان ارتباط راه دور را میسر می‌سازد. این پروتکل بر تعیین طول عمر باطری ابزار انتهایی، ظرفیت شبکه، QoS، امنیت و مقدار برنامه های کاربردی سرویس‌دهی‌شده توسط شبکه تاثیر می‌گذارد. مطابق شکل ۱ اجزای مختلفی در شبکه LoRaWAN وجود دارد:

۱- ابزارهای انتهایی: اطلاعات محیطی را جمع آوری می‌کنند و ممکن است فرمانهای ارسال شده برای آنها را اجرا کنند و برای ارتباط از لایه فیزیکی LoRa استفاده می‌کنند.

۲- گیت وی(دروازه): فریمها را از ابزار انتهایی تحویل می‌گیرد و به سرور شبکه ارسال می‌کند. برای ارتباط گیت وی و سرور از کانال با گذردهی بالاتر همچون اترنت، 3G/4G و wifi استفاده می‌شود.

۳- سرور شبکه: بسته‌های ارسال‌شده توسط ابزار انتهایی در سرور شبکه مورد بررسی صحت قرار می گیرند. همچنین بسته‌هایی که قرار است به ابزار انتهایی ارسال شود، در سرور شبکه تولید می شود.

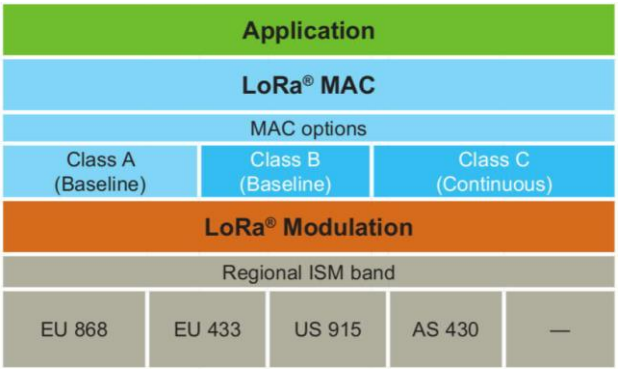
۴- سرور برنامه: در سرور برنامه بسته‌ها رمزگشایی می‌شود و از اطلاعات بدست آمده برای نشان‌دادن عکس‌العمل استفاده می‌شود.[6]



شکل ۱ معماری شبکه LoRaWAN

شبکه LoRaWAN نرخ بیت از ۰.۳ kbps تا ۵۰ kbps را ارائه می‌دهد. این نرخ بیت پایین برای کاربردهایی همچون انتقال بلادرنگ اطلاعات سنسورها در شبکه اینترنت اشیاء، ارتباطات ماشین-به-ماشین(M2M)، شهر هوشمند و کاربردهای صنعتی مناسب است. با این حال، انتقال داده های تصویر بلادرنگ، و یا هر چیزی که نیاز به پهنای باند بالا دارد، ممکن است بر روی شبکه‌های LoRa مناسب نباشد. این پهنای باند پایین، مصرف توان پایین ابزار انتهایی را تضمین می کند و بدین ترتیب استفاده از باتری به عنوان منبع تغذیه را ممکن می‌سازد[7].

ابزارهای انتهایی می‌توانند با ویژگی‌های مختلف پیکربندی شوند. LoRaWAN سه کلاس از دستگاهها را تعریف می کند. با استفاده از این کلاسها می توان زمان تأخیر ارتباط شبکه با ابزار انتهایی (downlink) را در مقایسه با طول عمر باتری انتخاب کرد. این کلاسها به همراه پشته پروتکل شبکه LoRAWAN در شکل ۲ نشان داده شده است. بسته به نیازهای برنامه، کلاس A ، B یا C می تواند انتخاب می شود.



شکل ۲ پشته پروتکل شبکه LoRaWAN [۲]

۳- ویژگیهای امنیتی LoRaWAN

احراز هویت متقابل بین یک دستگاه انتهایی LoRaWAN و شبکه LoRaWAN به عنوان بخشی از فرایند اتصال به شبکه ایجاد می‌شود. این فرایند تضمین می‌کند که فقط دستگاه‌های واقعی و مجاز به شبکه‌های واقعی و مجاز متصل می‌شوند.

لایه MAC و پیامهای لایه کاربرد در پروتکل LoRaWAN، رمز نگاری، تائید هویت، محافظت صحت و محافظت تکرار می-شوند. این محافظتها با احراز هویت دوطرفه ترکیب می‌شود تا اطمینان حاصل شود که ترافیک شبکه تغییر نکرده، از ابزار معتبر می‌آید، برای شخصی که شنود می‌کند قابل درک نیست و عمل ذخیره و بازپخش پیامها روی آنها انجام نمی‌شود.

به علاوه امنیت LoRaWAN رمزنگاری انتها به انتها را برای دنباله‌های لایه کاربردی که بین ادوات انتهایی و سرورهای برنامه

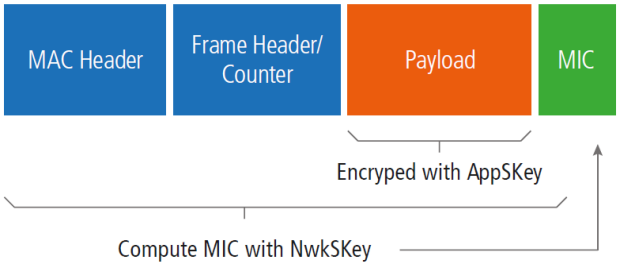
رد و بدل می شود پیاده سازی می‌کند. LoRaWAN از معدود شبکه‌های IoT است که رمزنگاری انتها به انتها را فراهم می‌کند. در شبکه‌های سلولار قدیمی، ترافیک تنها بر روی هوا رمز می‌شود ولی به صورت متن بدون رمز در شبکه هسته اپراتور جابجا می‌شود. در نتیجه کاربران آنها متحمل بار اضافه جهت انتخاب، پیاده‌سازی و مدیریت یک لایه امنیت اضافه می‌شوند (که معمولا با استفاده از نوعی VPN یا امنیت رمزنگاری در لایه کاربرد همچون TLS ایجاد می شود). این روش ها برای شبکه LPWAN مناسب نیست زیرا لایه اضافه امنیتی مصرف توان، پیچیدگی و هزینه بیشتر را همراه دارد.

۳-۱- پیاده سازی امنیت در شبکه LoRaWAN

مکانیزمهای امنیتی که به آنها اشاره شد، بر پایه الگوریتم تست شده و استاندارد شده AES هستند. این الگوریتم ها سالها توسط جوامع رمزنگاری تحلیل شده‌اند و توسط سازمان NIST تایید شده و به صورت گسترده‌ای به عنوان یکی از بهترین روشهای امن‌سازی عملی برای شبکه و نودهای محدود تطابق یافته‌اند. امنیت در LoRaWAN از رمزنگاری اولیه AES به همراه چندین مود عملی استفاده می‌کند: CMAC برای حفاظت از صحت اطلاعات و CTR برای محرمانگی. هر ابزار LoRaWAN به وسیله یک کلید ۱۲۸ بیتی AES به نام APPKey و یک شناسه منحصر به فرد جهانی (EUI-64-based DevEUI) شناسایی می شود. هر دوی این شناسه ها در فرایند احراز هویت استفاده می شوند. تخصیص شناسه EUI-64 مستلزم این امر است که تخصیص‌دهنده از سازمان IEEE شناسه OUI یا همان شناسه سازمانی منحصر به فرد را داشته باشد. به طور مشابه شبکه‌های LoRaWAN با یک شناسه منحصر بفرد جهانی که توسط سازمان LoRa Alliance™ اختصاص داده می شوند شناسایی می شوند [5].

با فرایند فعال‌سازی ابزارها بر روی هوا (Over-the-Air Activation) هم ابزار انتهایی و هم شبکه از AppKey مطلع می‌شوند. این اطمینان با محاسبه یک AES-CMAC (به کمک کلید AppKey) با درخواست اتصالی که توسط ابزار انتهایی ارسال می‌شود و سرور گیرنده شبکه حاصل می‌شود. دو کلید نشست از AppKey مشتق می‌شود یکی برای تامین حفاظت از صحت اطلاعات و رمزنگاری لایه MAC و کاربرد شبکه LoRaWAN به نام NwkSKey و دیگری برای رمزکردن پی لود لایه کاربرد به نام AppSKey (شکل ۱). کلید NwkSKey در شبکه LoRaWAN برای تایید و اثبات اعتبار و صحت بسته ها توزیع می‌شود. کلید AppSKey بر روی سرور کاربرد برای رمزنگاری و رمزگشایی پی لود لایه کاربرد توزیع می شود. دو کلید AppKey و AppSKey می‌تواند از شبکه مخفی شود تا از رمزگشایی پی‌لودهای لایه کاربرد توسط آن جلوگیری شود. شکل ۴ فرایند توزیع کلید و رمز نگاری در شبکه LoRaWAN را نشان می‌دهد.

تمامی ترافیک شبکه LoRaWAN به کمک دو کلید نشست محافظت می شود. هر پی لود با AES-CTR رمز می شود و یک شمارنده فریم را حمل می‌کند (برای جلوگیری از حمله replay) و یک کد صحت پیام (MIC) به وسیله AES-CMAC برای جلوگری از دستکاری بسته محاسبه می شود. شکل ۳ ساختار بسته LoRaWAN به همراه محافظتهای آن را نشان می‌دهد.

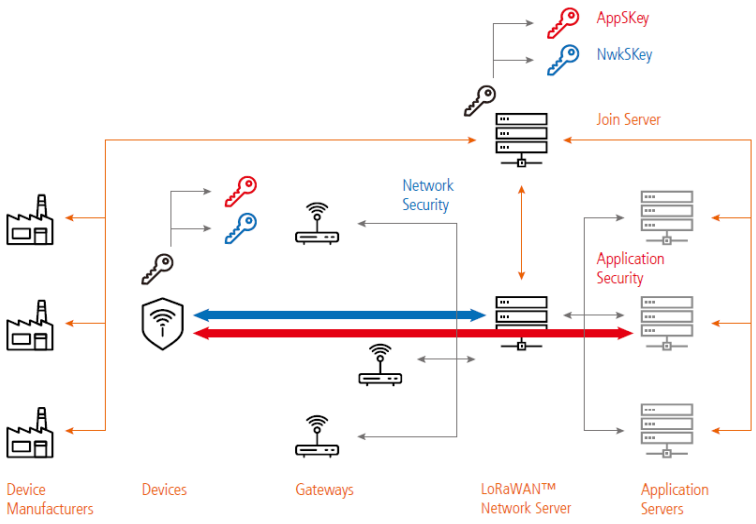


شکل ۳ ساختار بسته LoRaWAN در لایه MAC [5]

همانطوری که اشاره شد، رمزنگاری AES در مود CTR برای ساخت عملگر رمزشده XOR استفاده می شود (همچون سایر مودها چون CBC). اینکار قدرت رمزکنندگی AES را با استفاده از کلید منحصر به فرد برای رمز کردن هر بلاک رمز بالا می برد.

به دلیل آنکه دوکلید AppSKey و NwkSKey هردو از یک APPKey مشتق می شوند، این مشکل پیش می آید که اپراتور شبکه LoRaWAN که APPKey را در اختیار دارد، می تواند از روی آن AppSKey را تولید کند و ترافیک را رمزگشایی کند. برای جلوگیری از این اتفاق، یک سرور مستقل از اپراتور، ذخیره AppKey را مدیریت می‌کند. احراز هویت دوطرفه و تولید کلیدها می تواند توسط یک موجودیت خارج از کنترل اپراتور انجام شود. جهت دادن چنین انعطاف پذیری به اپراتورها، نسخه جدید LoRaWAN دو کلید مستقل یکی برای شبکه (NwkKey) و دیگری برای کاربردها(AppKey) تعریف می‌کند.

رابطهای بین شبکه و سرورهای کاربرد حامل سیگنالهای کنترلی و دیتا هستند. دو تکنولوژی HTTPS و VPN برای ایمن



شکل ۴ فرایند توزیع کلید و رمز نگاری در شبکه LoRaWAN [5]

سازی ارتباط بین این عناصر زیرساخت حیاتی استفاده می‌شوند همانطوری که در سایر سیستمهای مخابراتی از این دو تکنولوژی استفاده می‌شود.

۴- حملات در شبکه LoRaWAN

در این بخش به بررسی برخی از حملات احتمالی در شبکه LoRaWAN می پردازیم. بسته به روش پیاده سازی شبکه ممکن است تعدادی از این حملات برای یک شبکه ممکن نباشد و یا حملاتی وجود داشته باشد که تنها برای یک نوع کاربرد خاص از شبکه LoRaWAN انجام پذیر باشد و در این مقاله به آنها اشاره ای نشده باشد.

- **حمله فیزیکی**

این حمله با غیرفعال کردن، خراب کردن، جابجا کردن، تاثیر گذاردن بر سنسور و خواندن کلیدهای امنیتی ذخیره شده بر روی ابزار انتهایی انجام می شود. هدف حمله کننده در این روش ایجاد خلل در جمع آوری دیتا، جعل هویت ابزار انتهایی و تغییر اطلاعات ارسال شده به سرور شبکه است. برای جلوگیری از این حمله می توان از جعبه های ایمن برای ابزار استفاده کرد، از سنسور حرکت در ابزار انتهایی استفاده شود و برای حفاظت از کلیدهای رمزنگاری از اجزای امنیتی (Security Element) استفاده نمود.

- **جمع آوری فراداده‌ها**

این حمله با راه اندازی یک گیت وی جهت جمع آوری اطلاعات بسته های ارسالی انجام می شود، این اطلاعات می تواند شامل طول پی لود، آدرس ها و شمارنده باشد. از این اطلاعات می توان برای حدس زدن محتویات بسته رمز شده استفاده کرد، به عنوان مثال با یک رخداد خاص در یک سنسور بسته ای با طول مشخص به سرور ارسال می شود. جهت جلوگیری از این حمله می توان طول پی لود را برای تمام بسته ها یکسان در نظر گرفت. راه حل دیگر این است که برای گمراه‌کردن فرد شنود کننده بسته‌هایی به صورت تصادفی برای پوشش دادن به رخدادهای واقعی ارسال کرد.

- **حمله مکان یابی از روش مثلث**

در این روش به کمک تکنیک های مکان یابی از چندین گیت وی غیر مجاز برای تخمین مکان ابزار انتهایی استفاده می‌شود. با مقایسه زمانهای دریافت یک سیگنال توسط گیت‌وی‌های مختلف و استفاده از همپوشانی مکان تقریبی ابزار انتهایی قابل تخمین است. مکان ابزار انتهایی زمانی برای حمله‌کننده اهمیت دارد که به یک شئ متحرک مثل اتومبیل متصل شده باشد. جهت جلوگیری از حمله باید برچسب های زمانی را رمز کرد در صورت لو رفتن کلید AppKey می توان با فرایند اتصال مجدد کلید جدید به ابزار انتهایی اختصاص داد.

- **حمله گیت وی مخرب (۱)**

در این روش حمله‌کننده، گیت وی خود را در شبکه LoRaWAN قرار می دهد و اقدام به تغییر یا فیلتر کردن بسته ها به سمت سرور شبکه یا از سرور شبکه به سمت ابزار انتهایی می‌کند. برای جلوگیری از این حمله باید گیت وی ها در شبکه احراز هویت شوند و یا از بسته تایید دریافت برای اطلاع به فرستنده در مورد دریافت شدن بسته ارسالی در گیرنده استفاده شود.

- **حمله گیت وی مخرب (۲)**

این حمله نیز با قرار دادن یک گیت وی غیرمجاز در شبکه انجام می شود اما در این روش، گیت وی مخرب پیغام تایید دریافت بسته به ابزار انتهایی ارسال می کند تا از ارسال مجدد بسته گم شده برای سرور شبکه جلوگیری کند. روش کار به این صورت است که گیت وی مخرب، بسته تایید دریافت از سمت سرور شبکه را ذخیره می کند و در دفعات بعدی دریافت بسته آن را برای ابزار انتهایی ارسال می کند. برای جلوگیری از این حمله نیز می توان از گیت وی های احراز هویت شده در شبکه استفاده کرد. این مشکل در نسخه جدید شبکه LoRaWAN برطرف شده است زیرا در نسخه های قبلی مشخص نبود که دریافت کدام پیام تایید می شود ولی در نسخه جدید جهت تایید دریافت بسته شماره بسته دریافت شده نیز در تایید دریافت ارسال می گردد.

- **حمله تکرار بسته**

در این حمله پیامهای ارسال شده ذخیره می شود و در زمانی که حمله کننده می خواهد سرور شبکه را گمراه کند دوباره ارسال می شود. برای جلوگیری از این حمله از شمارنده در بسته ها استفاده می شود. بنابراین سرور شبکه در صورت دریافت بسته ای با شماره ای که انتظارش را ندارد آنرا دور می اندازد.

- **سرور برنامه غیر مطمئن**

در صورتی که از یک سرور عمومی به عنوان سرور برنامه استفاده شود احتمال این حمله وجود دارد. در واقع فرایندهای اتصال ابزار انتهایی و رمزنگاری و رمزگشایی پی لود ها در یک سرور عمومی نا ایمن انجام می شود. علت استفاده از سرورهای ناامن به خاطر سادگی پیاده سازی آنهاست. همچنین در هنگام تنظیم نمودن این سرورها ممکن است مسائل امنیتی رعایت نشود. جهت جلوگیری از حمله به سرور برنامه دستیابی به کلید رمز گشایی برنامه AppSKey یا باید سرور خصوصی خود را داشته باشیم و یا الگوریتم رمز خود را پیاده سازی کنیم.

۵- نتیجه‌گیری

در این مقاله به خصوصیات امنیتی مناسب شبکه LoRaWAN اشاره شد. تکنولوژی LoRa و پروتکل شبکه LoRaWAN امکان توسعه و ارائه راه حل های ایمن برای محافظت از شرکت و کاربر نهایی در برابر حملات سایبری را فراهم می کند. اما این موضوع برای توسعه دهندگان و برنامه نویسانی که بر اساس LoRa راه حل های اینترنت اشیاء ارائه می‌دهند باید روشن باشد که صرفاً استفاده از LoRa به معنی داشتن ایمنی نیست. در عوض باید در هنگام طراحی، به حملات احتمالی در شبکه نیز فکر کرد. ذخیره کلیدهای رمز نگاری به عنوان یکی از چالشهای اصلی در امنیت شبکه است. در هنگام طراحی ممکن است بیشتر بر روی تست ایمنی ابزارهای انتهایی و رابطهای کاربر تمرکز شود و به موضوع ایمن سازی ذخیره کلیدها توجه نشود. با شکست در نگهداری کلیدها تمامی شبکه در اختیار حمله‌کننده قرار خواهد گرفت. در نهایت با وجود آن که در تدوین و پیاده‌سازی استانداردهای شبکه LoRaWAN از روشهای ایمن‌سازی شبکه کارآمد و به‌روز استفاده شده است، استفاده از اینترنت اشیاء و پیاده‌سازی این شبکه از راه‌حل‌های پیچیده فناوری اطلاعات است و آسیب‌پذیری‌های امنیتی در هنگام توسعه این امکانات بسیار محتمل است.

مراجع

[1] J. Kim and J. Song, "A Secure Device-to-Device Link Establishment Scheme for LoRaWAN," in IEEE Sensors Journal, vol. 18, no. 5, pp. 2153-2160, 1 March , 2018.

[2] "A technical overview of LoRa and LoRaWAN," LoRa Alliance, San Ramon, CA, USA, Tech. Rep., Nov. 2015. [Online]. Available: https://docs.wixstatic.com/ugd/eccc1a_ed71ea1cd969417493c74e4a13c55685.pdf

[3] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "LoRaWAN specification," LoRa Alliance, San Ramon, CA, USA,Tech. Rep. Version 1.0.2, Jul. 2016.

[4] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 9, no. 2, pp. 855–873, 2nd Quart., 2017.

[5] "A full end-to-end encryption for IoT application provider" by Gemalto, Actility and Semtech February 2017, Tech. Rep., [Online]. Available: https://lora-alliance.org/sites/default/files/2018-04/lora_alliance_security_whitepaper.pdf

[6] J. de Carvalho Silva, J. J. P. C. Rodrigues, A. M. Alberti, P. Solic and A. L. L. Aquino, "LoRaWAN — A low power WAN protocol for Internet of Things: A review and opportunities," 2017 2nd International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, 2017, pp. 1-6.

[7] M. Saari, A. M. bin Baharudin, P. Sillberg, S. Hyrynsalmi and W. Yan, "LoRa — A survey of recent research trends," 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2018, pp. 0872-0877.