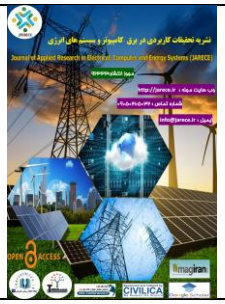
Vol. 1, No. 2, Jul-Sep 2023, (30-40)

Journal of Applied Research in Electrical, Computer and Energy Systems (JARECE)

نشریه تحقیقات کاربردی در برق ، کامپیوتر و سیستم های انرژی

دوره ۱، شماره ۲، تابستان ۱۴۰۲ (۴۰-۳۰)

journal homepage: https://jarece.ir/



# بهبود امنیت اینترنت اشیاء در شبکه های ارتباطی نرم افزار مبتنی بر SDN

**احمد عباس فحامه[۱]، بهناز نحوی[۲]***

۱دانشگاه آزاد اسلامی واحد تهران جنوب، دانشکده فنی و مهندسی، گروه کامپیوتر و نرم افزار، ihsanihsan.k80@gmail.com

۲استادیار، دانشگاه آزاد اسلامی واحد کرج، دانشکده مهندسی داده و هوش مصنوعی، گروه کامپیوتر، behnaz.Nahvi@gmail.com

**چکیده**

امروزه شبکه های نرم افزار محور (SDN) جایگزین شبکه های داده سنتی شده اند. به علت سرعت عمل این شبکه ها در ارسال یا دریافت پیامها و همچنین استفاده از کنترلگرها به منظور کنترل منابع شبکه و ترافیک ارسال دستورالعملها، این شبکه ها برای ارسال بسته های داده مورد استفاده قرار می گیرند. قوانین در جدول جریان ذخیره می شوند. از این رو هر تصمیم و محاسبه توسط کنترل کننده انجام می شود. معماری متمرکز می تواند جمع آوری اطلاعات شبکه و اجرای سیاستها را برای مدیر شبکه آسانتر می کند. مشکلات امنیتی در SDN بسیار متداول می باشند. عمدتا هدف از این حملات ممکنست خراب کردن شبکه یا کاستن از کارایی شبکه باشد. در این تحقیق، یک روش احراز هویت سریع و مقاوم در برابر انواع حملات جهت بهبود امنیت کاربران در اینترنت اشیاء ارائه شده است. در این تحقیق از دو پروتکل DTLS و CoAP برای کنترل دسترسی به داده ها استفاده نموده ایم. روش پیشنهادی، برای کنترل دسترسی به دستگاهها و داده های جمع آوری شده آماده انتقال به مراکز کنترلی یا به دستگاههای دیگر طراحی شده است. روش پیشنهادی با استفاده از متلب پیاده سازی شده و کارایی آن از لحاظ مدت زمان لازم برای احراز هویت کاربران و PSKهای نامعتبر در ۵۰۰۰ کاربر مورد ارزیابی قرار گرفته شده است. در مقایسه با کارهای پیشین، کارایی روش پیشنهادی از لحاظ مدت زمان برای احراز هویت کاربران بسیار بهتر از کارهای دیگر می باشد.

**کلمات کلیدی:** بهبود امنیت، اینترنت اشیاء، شبکه های ارتباطی، شبکه های مبتنی بر نرم افزار (SDN)

## ۱. مقدمه

مفهوم اینترنت اشیاء (IoT) برای اولین بار توسط کوین اشتون در سال ۱۹۹۹ مطرح شد و جهانی را توصیف کرد که در آن هر چیزی از جمله اشیای بی جان از طریق امواج رادیویی برای خود هویت دیجیتال منحصربفرد داشته باشند و به کامپیوترها اجازه دهند تا آنها را سازماندهی و مدیریت کنند. به طور کلی اینترنت اشیاء یک زیرساخت پویا از شبکه جهانی با قابلیت خود-پیکربندی بر اساس استانداردها و پروتکل های ارتباطی سازگار است. همه اشیاء دارای هویتی منحصربفرد و ویژگیهای خاص خود بوده و از توانایی

بکارگیری رابط های هوشمند برخوردارند و در یک شبکه اطلاعاتی یکپارچه می شوند. بستر اینترنت اشیاء بر امواج رادیویی بی سیم قرار داده شده و به دستگاههای مختلف این امکان را می دهد تا از طریق اینترنت با یکدیگر به برقراری ارتباط بپردازند [1].
با گسترش این فناوری، با مسائلی از قبیل تامین امنیت شبکه در کنار بهینه سازی کارایی آن برای مبادله پیامها مواجه خواهیم شد. زیرا اغلب تچهیزات IoT در محیطهایی به کار گرفته می شوند که مستعد حملات سایبری هستند. با توجه به محدودیت منابع در اینترنت اشیاء، رفع چالش های امنیتی یکی از اصلی ترین ضروریات می باشد. این مساله باعث شده تا در سالهای اخیر محققان زیادی در زمینه احراز هویت در تجهیزات اینترنت اشیاء تحقیق کنند. با این وجود اغلب راهکارهای ارائه شده پیشین با دو مساله اساسی مواجه هستند: [2]

- اغلب تحقیقات انجام شده احراز هویت اشیا را به واسطه یک سرویس دهنده تصدیق انجام می دهند. این خصوصیت باعث می شود که معماری امنیتی شبکه وابسته به یک گره واحد بوده و در صورت بروز خرابی در این سرویس دهنده کل پروتکل امنیتی با شکست مواجه شود. در نتیجه به نظر می رسد که استفاده از راهکارهای توزیع شده برای کنترل احراز هویت اشیاء بتواند موجب برطرف کردن این مشکل گردد.
- پیچیدگی الگوریتم های رمزنگاری مورد استفاده در این روشها چالش مهمی محسوب می شود که موجب می شود نتوان از آن برای تمامی تجهیزات اینترنت اشیاء استفاده نمود. زیرا بخش بزرگی از اشیاء، تجهیزاتی با توان پردازشی کم و منابع محدود می باشند.

به منظور رفع دو مشکل مطرح شده، در این تحقیق قصد داریم تا یک طرح احراز هویت سریع و مقاوم در برابر انواع حملات جهت بهبود امنیت کاربران در اینترنت اشیاء ارائه کنیم. در روش پیشنهادی، این عمل با استفاده از شبکه نرم افزار محور (SDN ) و تئوری آشوب وابسته به فضا و زمان صورت خواهد گرفت. شبکه نرم افزار محور یک معماری جدید در شبکه است که دارای ویژگیهایی از قبیل پویایی، مدیریت پذیری و انطباق پذیری می باشد. در این معماری لایه کنترل از لایه داده جدا شده است.
در این تحقیق روش نوینی پیشنهاد می کنیم که از معماری مبتنی بر SDN برای تصدیق احراز هویت کاربران و شناسایی حملات در شبکه استفاده می کند. این تحقیق در پنج بخش تنظیم شده است. در بخش دوم پیشینه تحقیقات انجام شده مرتبط با این تحقیق را مرور خواهیم کرد. در بخش سوم، روش پیشنهادی را به طور کامل توضیح می دهیم. در بخش چهارم نحوه پیاده سازی و ارزیابی کارایی روش پیشنهادی را به طور کامل بررسی خواهیم کرد و در نهایت بخش پنجم نتیجه گیری و پیشنهادات را شامل می باشد.

## ۲. پیشینه تحقیق

Adeel و همکارانش [۱] یک طرح احراز هویت سبک و مقاوم در برابر چندین حمله جهت بکارگیری در اینترنت اشیاء ارائه دادند. در این روش، پس از مرحله احراز هویت، برای برقراری ارتباط امن یک کلید جلسه نیز تولید می شود. نتایج پیاده سازی این طرح نشان داد که، این طرح در برابر حملاتی مانند استراق سمع، حملات جعل هویت و مرد میانی مقاوم می باشد. Nesa و همکارانش [۲] یک پروتکل امنیتی سبک وزن و سریع برای کاربرد در اینترنت اشیاء ارائه نمودند. تکنیک مورد استفاده در این تحقیق، ترکیب درخت درهم سازی مرکل و مدل آشوب می باشد. در این تحقیق، خروجی مدل آشوب با استفاده از درخت درهم سازی پردازش شده، تا پیچیدگی لازم برای داده های رمزنگاری حاصل گردد. Zhao و همکارانش [۳] یک مدل احراز هویت جدید مبتنی بر تئوری آشوب ارائه نموده اند. به عبارت دیگر در این تحقیق، یک الگوریتم سریع و سبک وزن به منظور احراز هویت کاربران ارائه شده است که در آن فرایند احراز هویت با استفاده از ارتباطات آشوبناک ایمن میگردد. بدین منظور، از تئوری آشوب به منظور مدلسازی یک تابع یکتا و غیرقابل کپی برداری استفاده شده که این تابع بر اساس خصوصیات یکتای سخت افزاری اشیاء ایجاد می گردد. Chze و همکارانش [۴] یک پروتکل امنیتی برای ارتباطات در اینترنت اشیاء ارائه دادند. تکنیک به کار رفته در این تحقیق، تصدیق کاربران بر اساس معماری امنیتی چندلایه است. الگوریتم ارائه شده در این تحقیق، توانایی مقاومت در برابر حملاتی از قبیل سیاه چاله،

GreyHole، Sink Hole, Spoofing را دارد. اما یکی از مشکلات آن، عدم کارایی الگوریتم مسیریابی در کنترل شبکه های سریع می باشد. از اینرو معماری امنیتی این سیستم کارایی مناسبی داشته در صورتی که الگوریتم مسیریابی ارائه شده در آن، برای استفاده در اینترنت اشیاء مناسب نمی باشد. Duan و همکارانش [۵] یک چارچوب جدید برای مسیریابی ایمن داده ها در شبکه های حسگر بی سیم ارائه دادند که قابلیت استفاده در کاربردهای اینترنت اشیاء را دارد. این روش در برابر حملات روشن/خاموش کردن، برخورد های خودخواهانه و ... به خوبی عمل میکند اما دارای پیچیدگی محاسباتی بسیار بالایی می باشد . Anitaو همکارانش [۶] از معیار قابلیت اعتماد مستقیم بین هر دو گره برای اعتبارسنجی در شبکه های حسگر بی سیم استفاده کرده اند. این راهکار بر اساس یک سیستم شناسایی دو مرحله ای می باشد. این روش در مقابل حملاتی از قبیل GreyHole ایمن نیست و تصدیق هر کاربر با همسایگان برای شبکه های وسیع و تراکم بالا موجب پیچیدگی و تاخیر بالا در الگوریتم مسیریابی خواهد شد. Krentz و همکارانش [۷] یک راهکار مدیریت اعتبار مبتنی بر گروه برای اینترنت اشیاء ارائه کرده اند. این راهکار، یک مدل تعیین اعتبار مبتنی بر خوشه بوده که برای تامین امنیت الگوریتم های مسیریابی مبتنی بر خوشه بندی مناسب خواهد بود. با استفاده از این ساختار می توان حملات سیاه چاله را شناسایی نمود. اما مشکل اصلی این روش، نیاز سرخوشه به انرژی بسیار زیاد جهت برقرار ارتباط با مرکز داده می باشد که این امر موجب تخلیه سریع انرژی گرههای سرخوشه خواهد شد. Kharkongorو همکارانش [۸] یک پروتکل امنیتی مبتنی بر SDN برای تلفیق با الگوریتم های مسیریابی در اینترنت اشیاء ارائه کرده اند. الگوریتم مسیریابی پیشنهادی دارای ۶ گام است که عبارتند از: ثبت گرهها توسط کنترلگر، مانیتورکردن کل شبکه توسط کنترلگر، دریافت اطلاعات همسایگان توسط هر گره در شبکه، محاسبه انرژی باقیمانده در همسایگان، انتخاب و ارسال داده ها بر اساس انرژی باقیمانده گرهها به سمت همسایه، مسدود کردن گرههای مخرب و جلوگیری از دسترسی مجدد آنها به شبکه با استفاده از کنترلگر. Olivierو همکارانش [۹] یک معماری با هدف تامین امنیت اینترنت اشیاء ارائه کرده اند که مبتنی بر شبکه تعریف شده در SDN طراحی شده است. در این مدل، معماری مبتنی بر SDN در کاربردهای دارای زیرساخت و بدون زیرساخت عمل می کند. روش پیشنهادی در این تحقیق، اولین راهکار ارائه شده برای تامین امنیت در اینترنت اشیا با استفاده از SDN می باشد. این معماری شامل بخشهای (واسط یا لایه فیزیک، لایه قابل برنامه ریزی که یک سوئیچ مجازی سازگار با SDN و یک کنترلگر SDN است، لایه سیستم عامل ) می باشد. Dhakaو همکارانش [۱۰] سعی کرده اند تا با استفاده از بسته های کنترلی حملات سیاه چاله و خاکستری را تشخیص بدهند. در این روش به منظور تشخیص کاربران نفوذی، بسته های کنترلی به کاربران ارسال می شود و پاسخ کاربران با پاسخ مورد انتظار مقایسه می شود. در صورت مغایرت پاسخ بسته کنترلی کاربر به عنوان نفوذگر شناخته می شود . Tanو همکارانش [۱۱] یک الگوریتم مبتنی بر تصدیق پیام برای رفع کمبودهای امنیتی پروتکل OSLR ارائه شده است. در این الگوریتم از یک شبکه پتری فازی به منظور تصدیق کاربران شبکه استفاده شده است. همچنین این روش از یک الگوریتم مسیریابی ایمن برای ارسال داده از طریق گرههای تصدیق شده بهره می گیرد. Yingو همکارانش [۱۲] از کدگذاری زنجیره ای برای برقراری ارتباط ایمن در شبکه های موردی بین خودرویی استفاده نموده اند. این الگوریتم از کد تصدیق پیام و توابع درهم سازی برای تصدیق پیامهای کاربران استفاده می کند. همچنین این محققان به منظور جلوگیری از اتلاف محتوای بسته های ایمن از یک زنجیره دوسطحی کد استفاده نمودند.

Aman و همکارانش [۱۳] یک پروتکل کارآمد برای احراز هویت متقابل در سیستم‌های IoT ارائه می‌کند. پروتکل پیشنهادی از یک تابع غیرقابل کلون فیزیکی برای ارائه ویژگی های امنیتی مورد نظر استفاده می کند. تجزیه و تحلیل پروتکل نشان می دهد که نه تنها در برابر انواع مختلف حملات قوی است، بلکه از نظر حافظه، محاسبات، انرژی و سربار ارتباط نیز بسیار کارآمد است. Rao و همکارانش [۱۴] یک الگوریتم هش سفارشی با طرح امضای دیجیتال منحنی بیضوی اصلاح شده پیشنهاد کردند. روش پیشنهادی در برابر حملهMan-in-the-Middle ، حمله DoS توزیع شده(DDoS) و مقاومت در برابر برخورد مقاوم است. Suganthi و همکارانش [۱۵] برای اطمینان از امنیت و حریم خصوصی بیمار که امنیت و عملکرد را متعادل می کند، طرح احراز هویت دوجانبه پایان به پایان را پیشنهاد کرده اند. این طرح شامل مراحل پروتکل برای یک سناریوی اضطراری است که به وسیله آن کیفیت

مراقبت از بیمار در شرایط بحرانی حفظ می شود. تجزیه و تحلیل امنیتی نشان می دهد که طرح پیشنهادی در مقایسه با سایر طرح های مرتبط کارآمدتر است. Chen و همکارانش [۱۶] یک پروتکل احراز هویت سبک وزن و حفظ حریم خصوصی را برای پرداخت تلفن همراه در زمینه اینترنت اشیا ارائه کردند. از طریق تجزیه و تحلیل امنیتی رسمی ارائه شده در این مقاله، پروتکل پیشنهادی تحت مشکل توسعه یافته CDH ایمن است. علاوه بر این، ارزیابی عملکرد نشان می‌دهد که پروتکل پیشنهادی برای دستگاه‌های هوشمند با منابع محدود در اینترنت اشیا امکان‌پذیر و کارآمد است.

## ۳.روش پیشنهادی

در این تحقیق یک روش احراز هویت سریع و مقاوم در برابر انواع حملات جهت بهبود امنیت کاربران در محیطهای اینترنت اشیاء پیشنهاد می شود. در روش پیشنهادی، از شبکه نرم افزار محور (SDN) و تئوری آشوب وابسته به فضا و زمان استفاده خواهیم کرد. شبکه نرم افزار محور یک معماری جدید در شبکه است که دارای ویژگیهای خاصی همانند پویایی، مدیریت پذیری و انطباق پذیری می باشد. در این معماری، لایه کنترل از لایه داده جدا شده است. در یک معماریSDN ، دو مولفه اصلی وجود دارد که عبارتند از:

- تجهیزات ارسال: سخت افزار یا نرم افزاری است که به طور اختصاصی وظیفه ارسال بسته ها را بر عمده دارد.
- کنترل کننده های SDN : نرم افزاری است که بر روی یک پلتفرم سخت افزاری اجرا می شود.

در روش پیشنهادی از معماری مبتنی بر SDN برای تصدیق احراز هویت کاربران و شناسایی حملات استفاده می شود. بدین صورت که، محدوده دامنه شبکه را به زیردامنه های SDN تقسیم بندی کرده و هر زیردامنه با استفاده از یک کنترلگر SDN، وظیفه تصدیق کاربران مربوط به حوزه خود را برعهده دارد. در این مدل، کنترلگرها هر زیردامنه به مبادله پیامهای تصدیق با سایر کنترلگرها به منظور شناسایی حملات مهاجمین می پردازند. در کنار معماری امنیتی ذکر شده، از تئوری آشوب وابسته به فضا و زمان جهت تولید کلیدهای تصدیق استفاده می شود. نظریه آشوب وابسته به فضا و زمان، یک مدل جدید آشوب پویا در سیستم های توسعه یافته فضایی است که در برخی تحقیقات برای رمزنگاری یا درهم سازی داده ها به کار رفته است و می تواند در افزایش عمومیت مدل تصدیق پیشنهادی موثر باشد.

در روش پیشنهادی از پروتکلهای CoAP و DTLS سعی داریم امنیت داده ها را با کنترل دسترسی تامین کنیم .

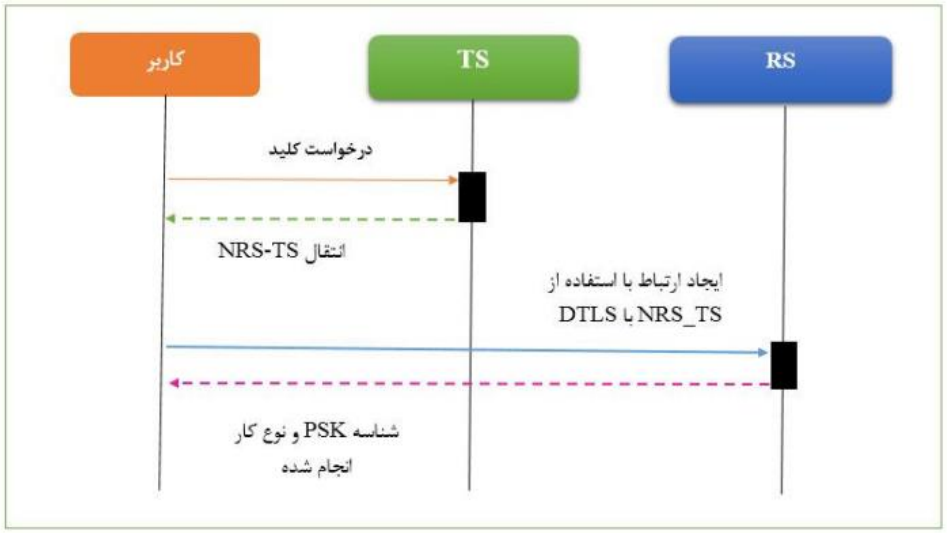
- ابتدا روش کلیدی مشتق شده مبتنی بر روش PKS هم برای کنترل دسترسی مبتنی بر محاسبات رمزنگاری متقارن انجام می شود.
- روش کلیدی عمومی با مجوز که مبتنی بر RPK بوده و کنترل دسترسی مبتنی بر محاسبات رمزنگاری نامتقارن است.

هر دو روش پیشنهادی، برای کنترل دسترسی به دستگاهها و داده های جمع آوری شده آماده انتقال به مراکز کنترلی یا به دستگاههای دیگر طراحی شده است. بدین صورت یک کاربر که بتواند به دستگاه دسترسی داشته باشد، می تواند به هر منبع یا داده ای در دستگاه دسترسی داشته باشد .

در روش پیشنهادی از سه نوع عامل استفاده می کنیم که عبارتند از:

- سرور منبع : یک شیئی یا دستگاه محدود شده است که میزبان منابع CoAP می باشد.
- کاربر : شیئی است که به سرور منبع وصل می شود و می تواند به منابع و داده های موجود در این سرور دسترسی داشته باشد .
- یک منبع محکم و قابل اعتماد : (TS) سروری است که دارای روابط قابل اعتمادی با سرورهای منبع بوده و همزمان از سیاست کنترل دسترسی خاصی استفاده می کنند که دسترسی کاربر به منابع و داده های موجود در سرورها و دستگاهها را کنترل می نماید.

حالت کلید مشتق شده شبیه حالت PSK است با این تفاوت که کلیدها به صورت صریح به سرور منبع (RS) ارائه نمی شوند. در عوض، RSو TS دارای کلید رمز عمومی با نام (NRS-TS) هستند که برای اشخاص دیگر غیرقابل دسترسی و ناشناخته می باشد. جریان (گردش) کار در روش پیشنهادی در شکل ۱ نشان داده شده است .




**شکل ۱-جریان کار برای حالت ایجاد ارتباط**

با توجه به شکل ۱ می توان گفت:

در مرحله آغازین، کاربر بایستی تقاضای توکنی را به TS بفرستد. دسترسی از دو طریق می تواند ایجاد شود:

- یک کلید که بین مشتری و RS(NRS-C) ایجاد می شود که مقدار ۱۲۸ یا ۲۵۶ بیت دارد.
- فعل یا عمل انجام شده که نشانه دسترسی به یک کانال امن است .

پس از دریافت یک توکن دسترسی، مشتری می تواند یک اتصال DTLS با RS را راه اندازی کند. اتصال در حالت PSK آغاز می شود. کلید NRS-C مخفی نگه داشته شده و به عنوان PSK در حالی که نوع عملیات در RS در فیلد شناسه PSK که پیام "تبادل کلید کاربری" ارسال می شود، استفاده می شود.

پس از دریافت پیام نوع کار یا عملیات، RS می تواند NRS-C را از نوع کار با عملیات و NRS-TS تولید کند و با موفقیت دستیابی به داده ها یا منابع را انجام دهد.

روش پیشنهادی با توسعه پروتکل ارتباطی ایجاد می شود این پروتکل به راحتی قادر به احراز هویت DTLS در راستای کنترل دستیابی به ابزارها و داده های تمام منابع میزبان است. این طرح پیشنهادی برای تمام کاربران قابل دسترسی بوده و آنها می توانند به راحتی به این طرح ملحق می شوند و برای انتقال داده های خود از آن استفاده نمایند. بنابراین، می توان با استفاده از روش پیشنهادی بدون نیاز به ارتباط برقرار کردن مجدد یا ذخیره کردن اطلاعات اضافی جلسات، از داده های موجود بر روی آنها محافظت نمود.

شایان ذکر است که این پروتکل هیچ تغییری در استاندارد DTLS و یا پیش نویس استاندارد CoAP انجام نمی دهد. در عمل این بدان معنی است که هیچ تغییری در کتابخانه پیاده سازی DTLS یا CoAP مورد نیاز نیست و پروتکل ممکنست در بالای کد موجود اجرا شود.

در همین حال، پروتکل پیشنهاد شده دارای چند اشکال است.

- اولا: این پروتکل هیچ راه حلی برای کنترل دسترسی به سطح منابع ارائه نمی دهد. اما این مورد می تواند به عنوان معایب جزئی در نظر گرفته شود. زیرا این روش می تواند جداگانه یا بالای پروتکل موجود ساخته شود.

- هدف از شناسه RS حفاظت بیشتر است در صورتیکه سرورهای منبع همان کلید KRS-TA دارند. در این وضعیت اگر شناسه RS در NONCE وجود نداشته باشد، یک کاربر می تواند یک NONCE و KEY برای یک دستگاه تولید کند و سپس از آن برای دسترسی به یک دستگاه دیگر استفاده کند. متاسفانه امکان ارسال یک ساختار دو تایی در فیلد-PSK identityپیام ClientKeyExchange ممکنست حاوی یک نام رشته کلایت در psk-Identity باشد و ساختار باینری تعریف شده در بالا را می توان با استفاده از Field-data field of ClientHello ارسال کرد. ناسازگاری اصلی این روش آنست که نیاز به تعریف فرمت اضافی TLS دارد که موجب تغییر در پیاده سازی DTLS در هر مشتری و در تمام RSمی شود. رویکردی که با استفاده از کدگذاریBASE ۶۴ به نظر می رسد بسیار امیدوارکننده تر از آن است که توسعه دهنده DTLS اضافی را تعریف می کند. به طور کلی، نمی توان پیش بینی کرد که چگونه کلید می تواند به دست آید. بنابراین طراحان کتابخانه DTLS باید راهی برای گسترش بازیابی کلید بدون اصلاح کد داخلی تعریف کنند و از این رو، می توان تاکید کرد که حالت DK مناسب حتی برای کتابخانه های اختصاصی است که دسترسی به کدمنبع را فراهم نمی کند.

پروتکل فقط شامل توضیحات کلی مکانیسم لغو کلیدی است. ما می توانیم پروتکل را با تعریف این بخش در جزئیات بیشتر بهبود بخشیم. درخواست لغو کلید باید حاوی شناسه TA و شناسه RS همراه با شماره توالی کلید است که باید لغو شود. این پیام را می توان با استفاده از جلسه DTLS در حالت خالص PSK ارسال کرد اما دستکاری برای DTLS دارای سربار زیاد است. علاوه بر این، دستگاه محدود دارای اسلات محدود برای جلسات DTLS است بنابراین دستیابی همیشه امکان پذیر نخواهد بود .
از آنجاییکه اطلاعاتی که در درخواست لغو کلید وجود دارد محرمانه نیست اما باید تایید شود، ما پیشنهاد می کنیم از ایجاد اتصال ایمن جلوگیری وشد و پیام را با کد هویت پیام (MAC) بر اساس الگوریتم HMAC محافظت کنیم .MAC را می توان با کلید KRS-TA محاسبه کرد تا بتواند به راحتی بر روی یک دستگاه محدود شده تایید شود.
ساختار درخواست لغو کلید در جدول ۱ نشان داده شده است. این درخواست با ۱ بایت شناسه TA شروع می شود و به دنبال آن ۱۲ بایت شناسه RS و ۸ بایت شماره توالی است. ۳۲ بایت اخیرا یک کد احراز هویت پیام است که براساس اطلاعات موجود در ساختار با کلید KRS-TA محاسبه می شود.

**جدول ۱-داده های مورد نیاز برای ایجاد ارتباطات**

| نام فیلد | اندازه (بایتها) | توضیح عملکرد |
|---|---|---|
| **Ta_id** | 1 | TA را به عنوان عدد مشخص می کند. |
| **Rs_id** | 12 | سرور منبع را مشخص می کند. |
| **Sequence_num** | 8 | تعداد بیتهای رشته برابر با ۶۴ بیت می باشد. |
| **MAC** | 31 | کداحراز هویت را پیام می دهد. |

درخواست لغو کلیدی می تواند بر روی هر پروتکل استاندارد یا برنامه سفارشی ارسال شود. اگر قرار است پروتکل CoAP بر روی دستگاه استفاده شود، سپس باید نقطه انتهایی خاصی را برای لغو کلید تعریف کرده و پیام را به عنوان یک بار استفاده از درخواست ACK ارسال کنیم. راه حلی که ارائه شد شامل پالایش برای لغو NONCE و لغو کلیدی خواهد بود و بیشتر مورد ارزیابی قرار می گیرد.

## ۴.پیاده سازی و ارزیابی روش پیشنهادی

به منظور پیاده سازی روش پیشنهادی در این تحقیق، یک سناریو تعریف می کنیم که با ورود هر کاربر برای انتقال اطلاعات در شبکه، یک شناسه RK تولید شده و به RS ارسال می شود. با اضافه شدن کاربران دیگر، کلیدهای دیگری نیز به RS ارسال می

شود. این کلیدها به ترتیب توالی آنها در لیست قرار می گیرد. چنانچه ترتیب توالی ارسال کلید PSK به هم بخورد و یا کلید PSK تولید شده از حداقل کلید موجود در لیست کمتر باشد، به عنوان یک حمله تشخیص داده شده و هشداری به سیستم بازگردانده می شود. نرم افزار به کار رفته برای پیاده سازی، متلب بوده است.

بدین منظور در این تحقیق، از یک روش رمزنگاری متقارن استفاده شده است تا علاوه بر این که لایه امنیتی به سیستم اضافه می شود، سرعت عملکرد انتقال اطلاعات در روش پیشنهادی را بهبود بخشیم. این روش رمزنگاری شامل مکانیسمی است که کاربر در حین ورود به سیستم برای انتقال از اطلاعات نیاز به یک کلمه عبور دارد. با دریافت PSK به عنوان کلمه عبور مطابق با روش پیشنهادی سعی در ارسال امن داده ها با احراز هوین مناسب داریم. بر اساس روش رمزنگاری متقارن PSK که نشاندهنده کاربر منحصربفردی است در سمت فرستنده رمزنگاری می شود و در رمزنگاری متقارن تمام عملیاتی که در سمت فرستنده بر روی PSK انجام می شود در سمت گیرنده به صورت برعکس بر روی PSK تغییر یافته اعمال می شود تا کلمه عبور اصلی بازیابی شود. در بیشتر روشهای رمزنگاری PSK اصلی در هنگام ارسال طی عملیاتی به یک ماتریس تبدیل می شود و به منظور احراز هویت امن به سمت گیرنده ارسال می شود. در سمت گیرنده همان عملیات بر روی ماتریس معکوس اجرا می شود و در نتیجه نهایی به صورت PSK اصلی بازگردانده می شود. یکی از معروفترین روشهای رمزنگاری الگوریتم blowfish است که در این پیاده سازی از آن استفاده می کنیم.

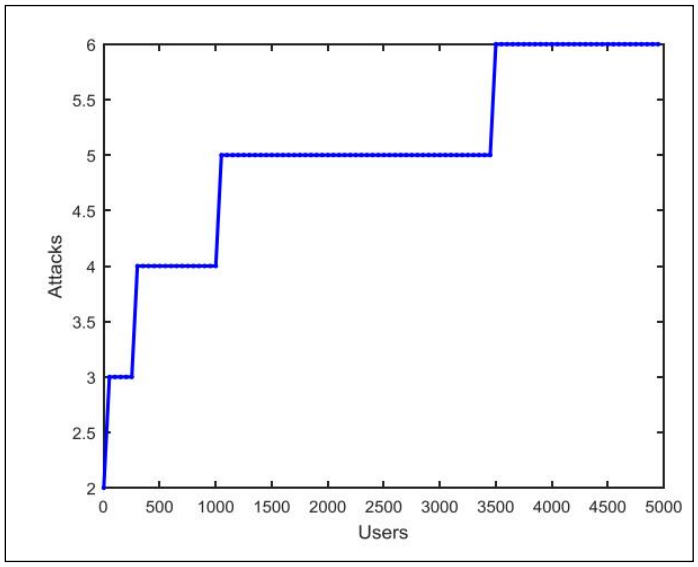
علاوه بر رمزنگاری در روش پیشنهادی راهکاری برای شناسایی حمله های DoS ارائه شده است که در آن ترتیب توالی و تاریخ انقضای PSK در نظر گرفته شده است. چنانچه یک PSK خارج از روال توالی ارسال شود یک مورد غیرعادی تشخیص داده می شود. همچنین اگر PSK از کمترین مقدار موجود در لیست کمتر باشد نشاندهنده انقضای تاریخ کلید عبور بوده و احراز هویت را با مشکب روبرو می کند و از این رو یک حمله برای سیستم در نظر گرفته خواهد شد. از این رو سناریوی پیشنهادی را با افزایش تعداد کاربران ادامه می دهیم و از بین کاربران موجود آنهایی که غیرعادی هستند، نشان می دهیم. جدول ۲ کاربران غیرعادی را در سناریویی با ۱۰۰ کاربر که به صورت حمله در نظر گرفته شده اند، نشان می دهیم.

**جدول ۲-نمایش کاربران غیرعادی در سناریوی پیشنهادی**

| |
|---|
| The PSK no. is 2 and invalid and it’s a DoS attack. |
| The PSK no. is 49 and invalid and it’s a DoS attack. |
| The PSK no. is 60 and invalid and it’s a DoS attack. |

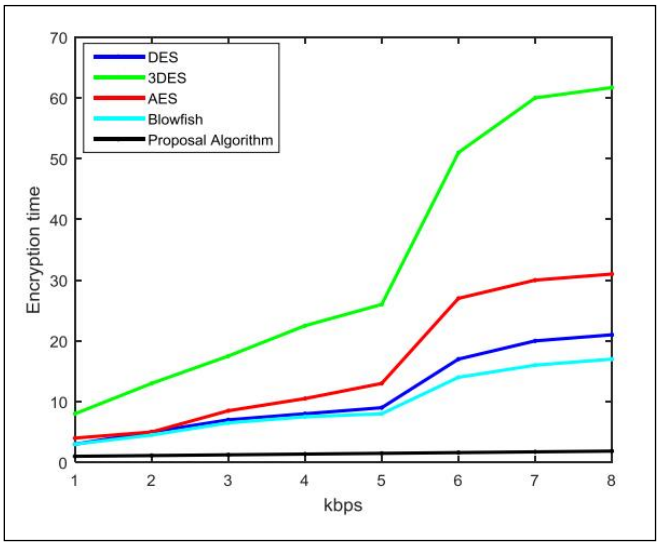
همانطور که در جدول ۲ نشان داده شده است، کاربرانی که با PSK نامعتبر اقدام به ارسال اطلاعات نموده اند، شناسایی شده اند. در ادامه به ارزیابی روش پیشنهادی خواهیم پرداخت.

به منظور ارزیابی کارایی روش پیشنهادی در این تحقیق، از تعداد حملات کشف شده در طی انتقال اطلاعات در لایه شبکه استفاده خواهیم کرد. بدین منظور با ادامه سناریوی یادشده در بخش قبل و افزایش تعداد کاربران به ۵۰۰۰ کاربر، به بررسی تعداد حملات رخ داده شده خواهیم پرداخت. از این رو کاربرانی که با PSK نامعتبر اقدام به انتقال اطلاعات می نمایند، کشف و از انتقال اطلاعات توسط این کاربران در لایه شبکه جلوگیری به عمل آمده است. شکل ۲ نشاندهنده تعداد PSK های نامعتبری است که به عنوان حملات تشخیص داده شده در طی انتقال اطلاعات توسط ۵۰۰۰ کاربر را نشان می دهد.




**شکل ۲-تعداد PSK های نامعتبر در طی انتقال اطلاعات مربوط به ۵۰۰۰ کاربر**

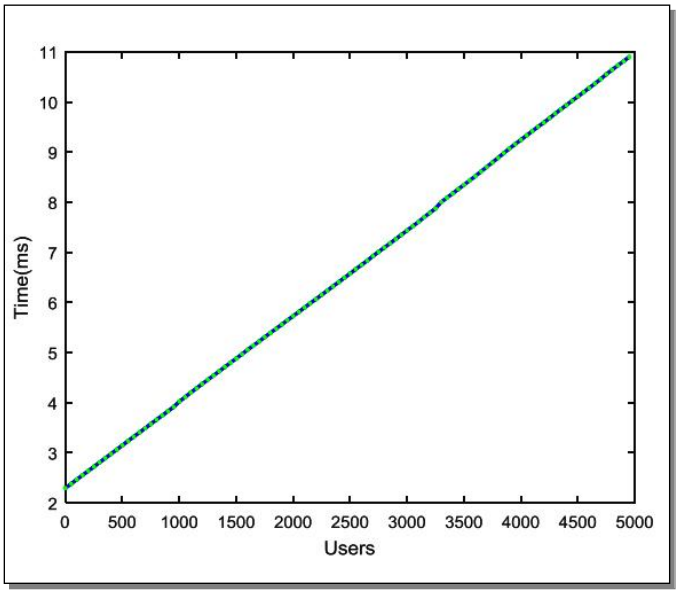
همانطور که در شکل ۲ نشان داده شده است، روش پیشنهادی حملات موجود در بین ۵۰۰۰ کاربر را کشف و شناسایی می نماید. معیار دیگری که به منظور ارزیابی کارایی روش پیشنهادی در نظر گرفته شده است، سرعت رمزنگاری و کشف حملات در هنگام انتقال اطلاعات است. هر چه سرعت رمزنگاری و احراز هویت کاربران در یک سیستم شبکه ای کم باشد، حداکثر تاخیر شبکه در انتقال اطلاعات کم خواهد بود. از این رو سرعت احراز هویت در روش پیشنهادی برای یک کاربر با این معیار در سایر روشهای رمزنگاری مقایسه شده است. شکل ۳ مقایسه سرعت رمزنگاری و احراز هویت روش پیشنهادی را با سایر روشهای رمزنگاری موجود نشان می دهد.




**شکل ۳-مقایسه سرعت رمزنگاری و احراز هویت روش پیشنهادی با روشهای دیگر**

همانطور که در شکل ۳ مشاهده می کنیم، سرعت رمزنگاری روش پیشنهادی برای یک کاربر در مقایسه با سایر روشهای رمزنگاری موجود به صورت چشمگیری کاهش یافته است. از این رو در ادامه به بررسی زمان مورد نیاز برای احراز هویت روش پیشنهادی با توجه به افزایش تعداد کاربران می پردازیم.

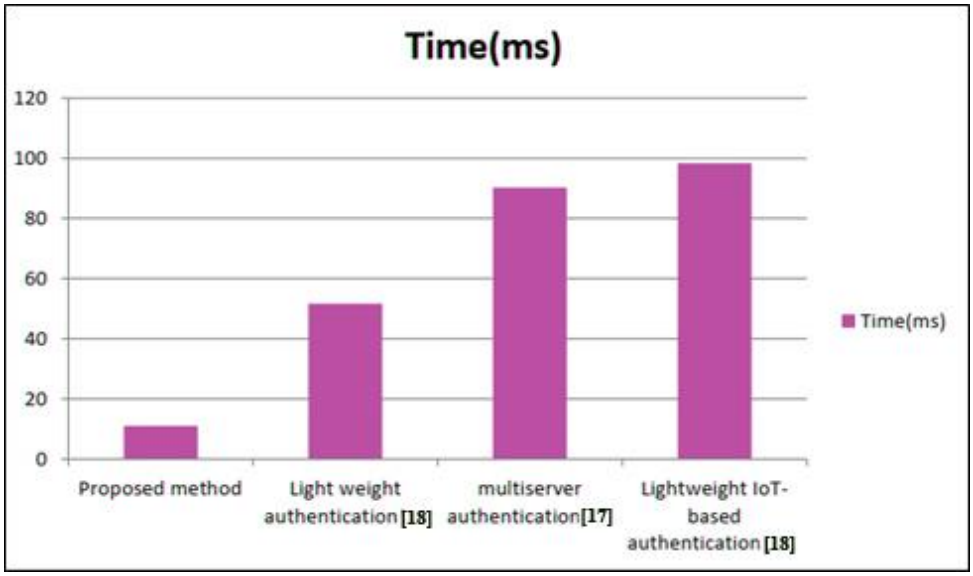
شکل ۴ نشاندهنده زمان مورد نیاز برای احراز هویت روش پیشنهادی با توجه به افزایش کاربران است.




**شکل ٤-زمان مورد نیاز برای احراز هویت در روش پیشنهادی**

همانطور که در این شکل ۴ مشاهده می کنیم، زمان مورد نیاز برای احراز هویت روش پیشنهادی با توجه به افزایش تعداد کاربران با آهنگ ملایمی افزایش می یابد. چنانچه زمان مورد نیاز برای احراز هویت ۵۰۰۰ کاربر در حدود ۱۱ میلی ثانیه است.

با توجه به محبوبیت شبکه های اینترنت اشیاء، کاربردهای بسیاری از این تکنولوژی وجود دارد. از این روز برقراری امنیت در ارتباط مربوط به این نوع شبکه از اهمیت بیشتری برخوردار است. به همین دلیل جنبه های مختلفی از امنیت در شبکه های اینترنت اشیا مورد توجه محققان قرار گرفته می شود. تمرکز اصلی این تحقیق بر روی رمزنگاری در شبکه های اینترنت اشیا برای احراز هویت کاربران است. بدین منظور برای اعتبارسنجی روش پیشنهادی با روشهای پیشین از نظر سرعت انجام احراز هویت کاربران و کشف کاربران غیرمجاز در مراجعه به کاربردهای شبکه اینترنت اشیا پرداخته ایم. شکل ۵ مقایسه روش پیشنهادی با روشهای پیشین را نشان می دهد .




**شکل ۵-مقایسه روش پیشنهادی با روشهای دیگر**

همانطور که در شکل ۵ مشاهده می کنیم روش پیشنهادی از نظر زمان لازم برای احراز هویت و کشف کاربران غیرمجاز از سایر روشهای پیشین عملکرد بهتری دارد.

## ۵.نتیجه گیری و پیشنهادات

یکی از مهمترین چالشهای موجود در شبکه های اینترنت اشیاء تامین امنیت داده ها و اطلاعات مبادله شده می باشد. روشهای مختلفی برای این امر پیشنهاد شده است ولی همچنان تامین امنیت داده های مبادله شده یک چالش اساسی برای مهیاکنندگان شبکه و همچنین برای کاربران محسوب می شود. در این تحقیق، روش نوینی برای این امر پیشنهاد شد که در آن از پروتکلهای DTLS, PSK استفاده شده و همچنین از کنترلگرهای SDN برای کمک به کنترل دقیق بسته های ارسالی در شبکه استفاده می شود. روش پیشنهادی برای کنترل دسترسی و تایید هویت می باشد. تکنیکهای احراز هویت به طور عمده مبتنی بر تکنولوژی احراز هویت کلید عمومی سبک وزن، کلید پیش اشتراکی PSK ، کلید تصادفی تکنولوژی احراز هویت پیش-توزیع شده، استفاده از تکنولوژی احراز هویت یکپارچه مبتنی بر تکنولوژی احراز هویت توابع Hash یکطرفه و غیره می باشند. کنترل دسترسی به طور عمده مبتنی بر رمزنگاری نامتقاون و متقارن است. در این تحقیق برای پیاده سازی روش پیشنهادی از نرم افزار متلب استفاده شد و کارایی روش پیشنهادی از نظر سرعت تشخیص و احراز هویت و تعداد PSK های نامعتبر مورد ارزیابی و مقایسه با کارهای دیگر قرار گرفت و کارایی آن اثبات گردید.

## مراجع

[1]- Adeel, A., Ali, M., Khan, A. N., Khalid, T., Rehman, F., Jararweh, Y., & Shuja, J. (2019). A multi-attack resilient lightweight IoT authentication scheme. Transactions on Emerging Telecommunications Technologies.
[2]- Nesa, N., & Banerjee, I. (2020). A Lightweight Security Protocol for IoT Using Merkle Hash Tree and Chaotic Cryptography. In Advanced Computing and Systems for Security (pp. 3-16). Springer, Singapore.
[3]- Zhao, H., & Njilla, L. (2019, May). Hardware Assisted Chaos Based IoT Authentication. In 2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC) (pp. 169-174). IEEE.
[4]- Chze, P. L. R., & Leong, K. S. (2014, March). A secure multi-hop routing for IoT communication. In 2014 IEEE World Forum on Internet of Things (WF-IoT) (pp. 428-432). IEEE.
[5]- Duan, J., Yang, D., Zhu, H., Zhang, S., & Zhao, J. (2014). TSRF: A trust-aware secure routing framework in wireless sensor networks. International Journal of Distributed Sensor Networks.
[6]- Anita, X., Martin Leo Manickam, J., & Bhagyaveni, M. A. (2013). Two-way acknowledgment-based trust framework for wireless sensor networks. international journal of Distributed Sensor Networks, 9(5), 952905.
[7]- Krentz, K. F., Rafiee, H., & Meinel, C. (2013, September). 6LoWPAN security: adding compromise resilience to the 802.15. 4 security sublayer. In Proceedings of the International Workshop on Adaptive Security (p. 1). ACM.
[8]- Kharkongor, C., Chithralekha, T., & Varghese, R. (2016). A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT). Procedia Computer Science, 89, 218-227.
[9]- Olivier, F., Carlos, G., & Florent, N. (2015). New security architecture for IoT network. Procedia Computer Science, 52, 1028-1033.
[10] Dhaka, A., Nandal, A., & Dhaka, R. S. (2015). Gray and black hole attack identification using control packets in MANETs. Procedia Computer Science, 54, 83-91.
[11] Tan, S., Li, X., & Dong, Q. (2015). Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Networks, 30, 84-98.
[12] Ying, B., Makrakis, D., & Mouftah, H. T. (2013). Privacy preserving broadcast message authentication protocol for VANETs. Journal of Network and Computer Applications, 36(5), 1352-1364.
[13] Aman, Muhammad Naveed, Kee Chaing Chua, and Biplab Sikdar. "A light-weight mutual authentication protocol for IoT systems." GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017.
[14] Rao, Vidya, and K. V. Prema. "Light-weight hashing method for user authentication in Internet-of-Things." Ad Hoc Networks 89 (2019): 97-106.
[15] Suganthi, S. D., et al. "End to end light weight mutual authentication scheme in IoT-based healthcare environment." Journal of Reliable Intelligent Environments 6 (2020): 3-13.
[16] Chen, Yanan, et al. "Light-weight and privacy-preserving authentication protocol for mobile payments in the context of IoT." IEEE Access 7 (2019): 15210-15221
[17] Wazid, Mohammad, et al. "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment." Journal of Network and Computer Applications 150 (2020): 102496.
[18] Zhang, Yan, et al. "A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain." IEEE Internet of Things Journal 8.18 (2021): 13958-13974.