# یک چارچوب امنیتی نرم‌افزار-محور برای شبکه اینترنت اشیا

علی قدیمی[۱*]، مهدی امینیان[۲] و محمد صالحی[۳]
[۱] دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران، ali.ghadimi.ir@gmail.ir
[۲] استادیار، گروه مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران، mahdi.aminian@guilan.ac.ir
[۳] استادیار، گروه مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران، mohammad.salehi@guilan.ac.ir

**چکیده :** اینترنت اشیا زندگی روزانه ما را به اندازه زیادی در حوزه‌های گوناگونی تحت تاثیر خود قرار داده است، از دستگاه‌های پوشیدنی کوچک گرفته تا سامانه‌های صنعتی بزرگ؛ در نتیجه، انواع گسترده‌ای از نرم‌افزارهای کاربردی در چارچوب‌های مختلف اینترنت اشیا پیاده‌سازی شده‌اند. در کنار نیازمندی‌های دیگر در اینترنت اشیا، امنیت یکی از کلیدی‌ترین نیازمندی و الزام برای برپایی شبکه اینترنت اشیا برای کاربردهای مختلف است. در این مقاله، جهت رفع محدودیت‌های امنیتی موجود در پیاده‌سازی مناسب شبکه اینترنت اشیا، روش جدیدی بر پایه امنیت نرم‌افزار-محور با نام ویزا برای شناسایی و احراز هویت اشیای متصل به شبکه معرفی می‌گردد. نتایج آزمایش‌ها نشان می‌دهد که راهکار ارائه شده می‌تواند با کنترل دسترسی اشیا، از شبکه در مقابل حملاتی چون جعل هویت، داس، شخص میانی و بازپخش محافظت نموده و در عین حال تاثیر کمی در کاهش توان عملیاتی شبکه داشته باشد.

**کلید واژه‌ها:** احراز هویت، امنیت، اینترنت اشیا، کنترل دسترسی، SDN

## ۱- مقدمه

اینترنت اشیا (IoT[۱])، نشان‌دهنده وضعیت کنونی و همچنین آینده اینترنت می‌باشد که بر اساس آن هر شی می‌تواند با استفاده از ابزارهای ارتباطی و از طریق اتصال به اینترنت با دنیای پیرامون خود تعامل داشته باشد. اینترنت اشیا به معنای وجود شبکه یکپارچه‌ای متشکل از فناوری‌ها و راهکارهای ارتباطی متنوعی است که در آن بسیاری از وسایل می‌توانند نسبت به اشتراک‌گذاری اطلاعات خود با یکدیگر و یا انسان‌ها اقدام نمایند. به سبب تعداد زیاد اشیائی که به اینترنت متصل هستند، حجم انبوهی از داده تولید می‌شود که بهره‌برداری از این داده تولید شده و تبدیل آن به اطلاعات مفید، نیازمند تلاش فراوان و انجام عملیات پردازشی زیادی می‌باشد. به علاوه، سازماندهی و کنترل این حجم انبوه از داده، نیازمند نظریه‌های بدیعی در طراحی و مدیریت اینترنت اشیا است تا عملکرد آن را بهبود بخشد[۱].

محققان زیادی به مطالعه فناوری‌هایی پرداخته‌اند که بتواند حجم انبوه از دستگاه‌های هوشمند، میزان ترافیک و تعداد بسته‌ها را پردازش کند. یکی از فناوری‌های قابل اجرا در این زمینه، سامانه‌های نرم‌افزار-محور (SDSys[۲]) می‌باشد که شامل شبکهٔ نرم‌افزار-محور (SDN[۳])، امنیت نرم‌افزار-محور (SDSec[۴]) و غیره می‌شود. از این فناوری می‌توان در محیط اینترنت اشیا جهت مدیریت مناسب شبکه بهره برد، زیرا می‌تواند همه دستگاه‌های متصل به شبکه را کنترل کند.

یکی از مشکلات اساسی که مانع از مقبولیت عمومی نرم‌افزارهای IoT شده است، نگرانی‌های امنیتی می‌باشد. در حالی‌که برای رفع این مشکل راه حل‌هایی موجود است که از انواع شبکه‌های سنتی استخراج شده‌اند، اما نیاز است تا چارچوبی بر پایه اصول امنیتی نرم‌افزار-محور نیز معرفی گردد. پیروی کردن از راهکارهای امنیتی سنتی جهت استفاده در ایده‌های فناوری نوین مانند شبکه نرم‌افزار-محور، غیر منطقی است. به همین دلیل، امنیت نرم‌افزار-محور که نمونه‌ای از مجازی‌سازی عملکرد شبکه است، در حال ظهور می‌باشد. این فناوری جدید بوسیله جدا کردن قسمت کنترل امنیت از سایر بخش‌ها، روش جدیدی را در طراحی،

[۱] Internet of Things
[۲] Software-Defined System
[۳] Software-Defined Networking
[۴] Software-Defined Security

پیاده‌سازی و مدیریت امنیت مهیا می‌کند. این جداسازی، راه حل توزیع شده امنیتی مقیاس‌پذیری را مهیا می‌کند که هرچند کارکرد امنیتی را مجازی‌سازی کرده، اما به عنوان یک سیستم منطقی واحد، قابل کنترل است. امنیت نرم‌افزار-محور به این دلیل ارائه شده است که به امن‌سازی زیرساخت‌های محیط‌های مجازی، از جمله شبکه مجازی، ذخیره‌سازی مجازی و حتی سرورهای مجازی در مقابل تهدیدهای گوناگون کمک کند. این تهدیدها می‌توانند تهدیدهای سنتی چون تشخیص نفوذ و یا مخصوص محیط‌های مجازی مانند تهدیدهای داخلی باشند[۲].

در ادامه این مقاله، در بخش ۲ پژوهش‌های پیشین در زمینه امنیت شبکه اینترنت اشیا با محوریت شبکه‌های نرم‌افزار-محور مورد بررسی قرار خواهند گرفت. در بخش ۳ راهکار پیشنهادی ما ارائه شده و در بخش پایانی نتایج شبیه‌سازی و نتیجه‌گیری عنوان شده است.

## ۲- پیشینه

یکی از مهمترین چالش‌ها در گسترش و استفاده از اینترنت اشیا، نگرانی‌های امنیتی و حریم خصوصی می‌باشد. از طرفی معماری شبکه نرم‌افزار-محور به عنوان راهکاری در زمینه پیاده‌سازی شبکه اینترنت اشیا مطرح می‌باشد. به همین جهت گروهی از محققان به مطالعه روش‌هایی روی آورده‌اند تا بتوانند با استفاده از فناوری SDN، نسبت به رفع چالش‌های امنیتی پیش‌رو اقدام نمایند. هنگامیکه درباره ایمنی شبکه بحث می‌شود، هدف نهایی جلوگیری از بروز مشکلات امنیتی در بستر شبکه است، اما انجام این کار در سطوح مختلفی قابل پیاده‌سازی می‌باشد.

در [۳]، روشی ارائه شده است که درآن پس از شناسایی هویت مهاجم، اطلاعات آن به کنترل‌کننده[۱] SDN ارسال می‌شود و به این ترتیب هر کنترل‌کننده با ارسال اطلاعات مهاجم به کنترل‌کننده همسایه خود، نسبت به پخش اطلاعات آن در شبکه اقدام می‌نماید. در [۴]، پیشنهاد شده است تا از فناوری زنجیره بلوکی[۲] به منظور احراز هویت در شبکه استفاده گردد. در [۵]، به منظور دفع حملات سیلاب تی‌سی‌پی[۳] و سیلاب آی‌سی‌ام‌پی[۴]، از یک SDN Gateway استفاده شده است که با تحلیل و شمارش هر جریان داده[۵]، حملات را شناسایی کرده و با استفاده از سازوکارهای دفاعی مانند مسدود کردن جریان‌های داده ارسالی از طرف مهاجم، ارسال به قرنطینه و یا اعمال QoS[۶] (برای مثال محدود کردن نرخ ارسال اطلاعات توسط مهاجم) با آن مقابله می‌نماید.

در [۶]، از خوشه‌بندی[۷] در شبکه اینترنت اشیا بر پایه SDN استفاده شده است. با توجه به اینکه در فناوری OpenFlow پس از نصب Flow Entry در سوئیچ‌ها، بسته‌های ارسالی توسط قوانین از پیش تعیین شده موجود در سوئیچ هدایت شده و کنترل‌کننده آنها را بررسی نمی‌کند، بنابراین در این مقاله پیشنهاد شده است به جهت جلوگیری از مشکلات امنیتی ناشی از سوئیچ‌های غیر معتبر یا آلوده به ویروس، سوئیچ یا دستگاه‌های میانی شبکه در هر تبادل اطلاعات با استفاده از پروتکل OpFlex نسبت به ارسال اطلاعات سوئیچ یا دستگاه فرستنده به کنترل‌کننده اقدام کنند. در صورتی که کنترل‌کننده تشخیص یک تهدید بالقوه را بدهد، نسبت به حذف Flow Entry از پیش نصب شده در سوئیچ اقدام می‌نماید.

در چارچوب امنیتی ارائه شده در [۷]، شبکه اینترنت اشیا به چندین شبکه محلی مجزا از یکدیگر تقسیم شده است که هر کدام شامل یک کنترل‌کننده و تعدادی شی می‌باشد. به دلیل وجود محدودیت منابع در بعضی از اشیا، همه آنها امکان استفاده از فناوری SDN را ندارند، اما همه اشیا بوسیله یک IoT Agent به یک کنترل‌کننده IoT متصل می‌باشند و در نتیجه می‌توانند از توان سایر دستگاه‌ها که دارای منابع بیشتری می‌باشند و قابلیت استفاده از SDN را دارند استفاده کنند.

در [۸]، یک پردازنده کم مصرف ECDSA مناسب برای به‌کارگیری در RFID ارائه شده است که می‌تواند عملیات مربوط به رمزنگاری کلید عمومی مانند امضای دیجیتال را بر روی یک تگ[۸] RFID با منابع محدود اجرا نماید. بنابراین می‌توان از آن جهت رمزنگاری کلید عمومی به منظور احراز هویت اشیا در شبکه استفاده نمود.

در [۹]، با الهام گرفتن از تکنیک‌های موجود در زمینه کنترل دسترسی به شبکه، پیشنهاد شده است تا با استفاده از فناوری SDN نسبت به کنترل دسترسی اشیا در لبه شبکه اقدام

---

[۱] Controller
[۲] Blockchain
[۳] TCP Flood
[۴] ICMP Flood
[۵] Flow
[۶] Quality of Service
[۷] Clustring
[۸] Tag

شود. در مقاله‌های دیگری همچون [۱۰] و [۱۱] و [۱۲] نیز با مورد توجه قرار دادن مسئله احراز هویت فرستنده پیام، سعی شده است تا با استفاده از رمزنگاری نسبت به ایجاد مکانیزمی جهت احراز هویت فرستنده پیام در شبکه اینترنت اقدام گردد.

در [۱۳]، از راهکار VAVE به منظور اعتبارسنجی فرستنده پیام در اینترنت استفاده شده است. در این راهکار که بر پایه معماری SDN می‌باشد، پس از محاسبه یک مسیر و ثبت آن در محیط VAVE، در صورتی که بسته‌ای با همان آدرس مقصد و مبدا ثبت شده در VAVE، اما از طریق رابط دیگری وارد کنترل‌کننده شود، مشخص کننده یک فرستنده جعلی می‌باشد و در نتیجه آن بسته فیلتر شده و ارسال نمی‌گردد. در [۱۴]، از SDN جهت مقابله با حملات LAN استفاده شده است که در آن سعی شده است تا به جای احراز هویت فرستنده پیام، تا جای ممکن اطلاعات فرستنده و گیرنده پیام مانند آدرس MAC آنها از دید یکدیگر و سایر اعضای شبکه مخفی بماند؛ بنابراین مهاجم اطلاعات مورد نیاز برای شروع یک حمله را در اختیار نداشته و نمی‌تواند با استفاده از حملات سنتی مانند ARP اسکن نیز به آن دست پیدا کند.

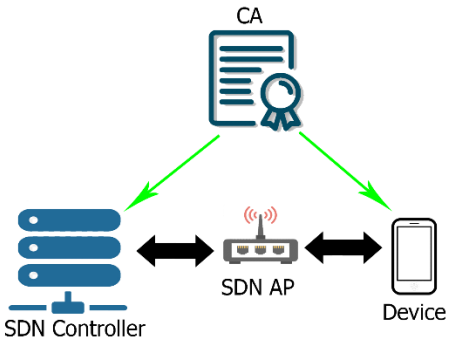
در [۱۵]، نگارنده با مد نظر قرار دادن مخاطرات ناشی از وجود یک کنترل‌کننده متمرکز، پیشنهاد می‌کند تا بعضی از وظایف کنترل‌کننده که در آنها نیازی به داشتن اطلاعات جامع از همه شبکه نیست، به دستگاه‌های لبه شبکه مانند سوئیچ‌ها منتقل گردد. در این مقاله، دو مکانیزم رمز یکبار مصرف و Port Knocking جهت احراز هویت معرفی شده است که هدف آنها افزایش امنیت شبکه و در عین حال کاهش بار بر روی کنترل‌کننده می‌باشد.

## ۳- روش پیشنهادی

در این مقاله، با توجه به اهمیت جوابگویی[۱] در افزایش امنیت شبکه، چارچوبی ارائه می شود که بتوان ا شیا مت صل به شبکه را احراز هویت نمود. جهت رسیدن به این هدف، به روشی نیاز است که به وسیله آن بتوان هر شی موجود در شبکه را به درستی شناسایی کرد. از آن جایی که در دنیای اینترنت نیز همانند دنیای حقیقی، امنیت به قابلیت شناسایی بسیار وابسته است، در شبکه نیز نیاز به یک شناسه یکتا برای شناسایی هر شی است.

در ادامه، راهکار VISA[۲] که شامل یک چارچوب امنیتی برای استفاده در شبکه نرم افزار-محور، یک راه حل احراز هویت اشیا و یک افزونه برای پروتکل IPV4 می‌باشد، معرفی می‌گردد.

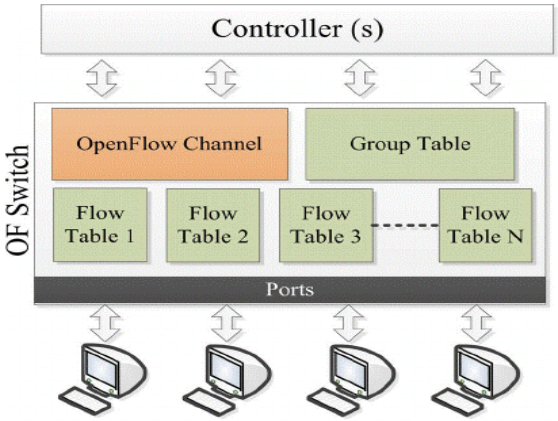
در روش پیشنهادی ما، با استفاده از رمزنگاری کلید عمومی از هویت شی متصل به شبکه اطمینان حاصل می‌شود. روش کار به این صورت است که در مرحله احراز هویت، هر شی اطلاعات ارسالی مورد نظر را با کلید خصوصی خود امضا می‌کند. بنابراین، گیرنده‌ی پیام با داشتن کلید عمومی می‌تواند از صحت اطلاعات دریافتی اطمینان حاصل نماید. این کلید عمومی و خصوصی توسط یک نهاد صادر کننده گواهینامه (CA[۳]) صادر می‌شود، سپس هر کلید عمومی به یک آدرس MAC تخصیص داده شده و کلید خصوصی در اختیار شی قرار می‌گیرد. در هنگام احراز هویت، کلید عمومی به همراه آدرس MAC مربوطه به صورت یک گواهی برای نهاد احراز هویت کننده (کنترل‌کننده) ارسال می‌شود. ارتباط زیرساخت کلید عمومی[۴] در شکل ۱ نشان داده شده است.




شکل ۱: ارتباط زیرساخت کلید عمومی در چارچوب VISA

با توجه به اینکه در راهکار VISA از رویکرد شبکه نرم‌افزار-محور و پروتکل OpenFlow استفاده شده است، هر شی هنگام اتصال به شبکه از طریق سوئیچ‌های OpenFlow با لایه کنترل‌کننده ارتباط برقرار می‌کند. این لایه وظیفه تصمیم‌گیری در خصوص مسیریابی بسته‌های شبکه را بر عهده دارد، اما با توجه به اینکه دارای دید کلی نسبت به شبکه می باشد، بنابراین می‌تواند سیاست[۵]های مربوط به کنترل دسترسی مورد نظر جهت اتصال اشیا به شبکه را نیز اعمال نماید. ساختار سوئیچ OpenFlow در شکل ۲ نشان داده شده است.

[۱] Accountability
[۲] Valid Identity Secure Authentication
[۳] Certificate Authority
[۴] Public Key Infrastructure
[۵] Policy




شکل ۲: ساختار سوئیچ OpenFlow [۱۶]

در مدل TCP/IP، در پروتکل‌های لایه ۲ شبکه مانند Ethernet و IEEE 802.11، هر شی هنگام ارسال بسته‌های اطلاعات در شبکه، آدرس MAC خود را نیز به بسته‌ها اضافه می‌کند. در راهکار VISA، فرستنده هنگام ارسال هر بسته، یک کلید موقت که در واقع یک عدد تصادفی است را تولید کرده و در قسمت Options مربوط به سرآیند IPV4 آن بسته قرار می‌دهد. این کلید موقت، یک عدد تصادفی[۱] است که در هر بسته ارسالی از طرف فرستنده متفاوت می‌باشد. فرستنده از این کلید موقت برای شناسه‌گذاری آدرس MAC گیرنده هر بسته ارسالی استفاده می‌کند.

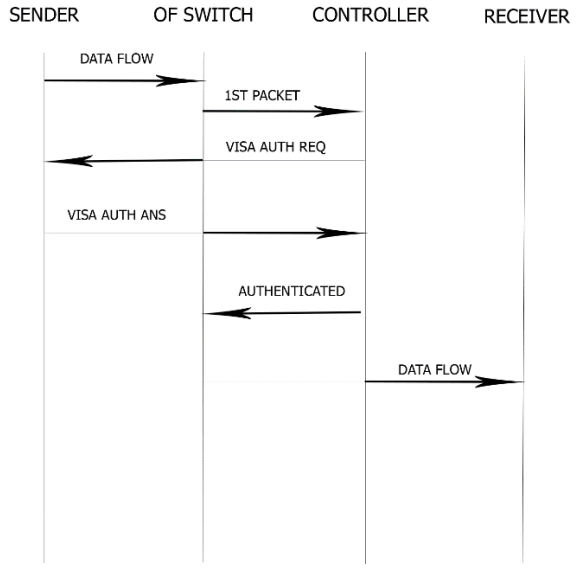
در پروتکل OpenFlow، اولین بسته از هر جریان اطلاعات[۲] توسط سوئیچ به کنترل‌کننده ارسال می‌شود. کنترل‌کننده پس از دریافت این بسته، فرستنده پیام را در وضعیت شناسایی قرار می‌دهد. کنترل‌کننده ابتدا آدرس MAC فرستنده را بررسی نموده و اصالت آن را از CA استعلام می‌کند. در صورتی که آدرس MAC معتبر نباشد، کنترل‌کننده از طریق Firewall آن را برای مدت معینی در لیست سیاه قرار می‌دهد، بنابراین بسته های ارسالی از طرف آن شی در سوئیچ مسدود می‌شوند و امکان اتصال شی به شبکه داده نمی شود.

در صورت معتبر بودن آدرس MAC فرستنده، کنترل‌کننده، کلید عمومی مربوط به آن آدرس MAC را در قالب گواهی از CA دریافت نموده و فرستنده را در وضعیت احراز هویت قرار می‌دهد. در این مرحله، کنترل‌کننده به منظور احراز هویت فرستنده پیام، کلید موقت جدیدی را تولید کرده و به فیلد Options بسته دریافتی اضافه می‌نماید؛ و به این ترتیب یک بسته احراز هویت که شامل کلید موقت دریافتی از فرستنده پیام و کلید موقت تولید شده توسط کنترل‌کننده است را ایجاد نموده، و برای فرستنده پیام ارسال می‌کند.

این کلید موقت، یک عدد تصادفی است که در هر بسته احراز هویت ارسالی از طرف کنترل‌کننده متفاوت می‌باشد. کنترل‌کننده از این کلید موقت برای افزایش امنیت و شناسایی بسته‌های پاسخ احراز هویت جعلی استفاده می‌کند.

فرستنده پیام پس از دریافت بسته احراز هویت، "کلید موقت فرستنده" آن را بررسی نموده و در صورتی که مربوط به خودش باشد، یک بسته پاسخ احراز هویت شامل "کلید موقت کنترل‌کننده"، "کلید موقت فرستنده"، به همراه آدرس MAC فرستنده و گیرنده پیام متناظر با "کلید موقت فرستنده" تولید نموده و آن را با استفاده از کلید خصوصی خود امضا کرده و برای کنترل‌کننده ارسال می‌کند.

کنترل‌کننده، بسته پاسخ احراز هویت را با استفاده از کلید عمومی راستی‌آزمایی نموده و در صورت صحیح بودن امضا و کلید موقت کنترل‌کننده و فرستنده، آدرس‌های MAC دریافتی را با آدرس MAC فرستنده و گیرنده موجود در بسته اولیه مقایسه می‌کند. در صورت یکسان بودن مقادیر فوق، کنترل‌کننده از صحت هویت فرستنده پیام و مقصد مورد درخواست آن اطمینان حاصل نموده و آن را در وضعیت اعطای مجوز[۳] قرار می‌دهد. مراحل فوق در شکل ۳ نشان داده شده است.




شکل ۳: مراحل احراز هویت VISA

[۱] Nonce
[۲] Flow
[۳] Authorizing

در وضعیت اعطای مجوز، کنترل‌کننده با استفاده از ابزار امنیتی خود مانند ACL[۱] و Firewall، در خصوص تخصیص دسترسی‌های مجاز به فرستنده تصمیم‌گیری نموده و آن را در سوئیچ اعمال می‌نماید. همچنین کنترل‌کننده نسبت به ثبت رویدادهای هر شی در Accounting اقدام می نماید.

همان گونه که پیشتر عنوان شد، فرستنده هنگام ارسال هر بسته، یک کلید موقت را تولید کرده و آن را در IP Header بسته قرار می‌دهد. در IP ورژن ۴، یک قسمت به عنوان Options وجود دارد که معمولا بدون استفاده است. در ایده پیشنهادی این مقاله، از این قسمت برای قرار دادن کلید موقت استفاده می‌شود. شکل ۴ ساختار افزونه اضافه شده به قسمت Options مربوط به IP Header ورژن ۴ را نشان می‌دهد که به شرح زیر می‌باشد:

Copied: مقداراین فیلد برابر با ۱ قرار داده می‌شود تا اطلاعات فیلد Options در همه بسته ها کپی شود.

Class: نشان دهنده طبقه‌بندی کلاس‌های مختلف Option می‌باشد. در راهکار VISA از مقدار ۳ استفاده شده است.

Number: یک عدد ۵ بیتی است که مشخص کننده نوع Option می‌باشد. در راهکار VISA مقدار این فیلد برابر با ۳۰ در نظر گرفته شده است.

Option Length: طول قسمت Options را نمایش می‌دهد که با توجه به نوع بسته ارسالی، مقدار آن متغیر است.

Type: یک عدد دو بیتی است که مشخص کننده نوع بسته می‌باشد. در تمامی بسته‌های ارسالی عادی، مقدار آن برابر با ۰ می‌باشد. در صورتیکه بسته ارسالی یک بسته درخواست احراز هویت VISA باشد، مقدار این فیلد برابر با ۱ است. در بسته‌های پاسخ احراز هویت VISA، مقدار این فیلد ۲ می‌باشد.

Nonce-S: یا همان کلید موقت فرستنده، یک عدد تصادفی ۳۹ بیتی است که در هر بسته ارسالی منحصر به فرد می‌باشد.

Nonce-C: کلید موقت کنترل‌کننده، یک عدد تصادفی ۳۹ بیتی است که در هر بسته درخواست احراز هویت منحصر به فرد می‌باشد.

| Copied | Class | Number | Option Length | Type | Nonce-S |
|---|---|---|---|---|---|
| Nonce-C | | | | | |

شکل ۴: ساختار افزونه اضافه شده به IP Header ورژن ۴ در راهکار VISA

## ۴- شبیه‌سازی و نتیجه‌گیری

جهت پیاده سازی مدل پیشنهادی، از شبیه‌ساز Mininet-WiFi در محیط لینوکس استفاده گردید. در ابتدا، با استفاده از این شبیه‌ساز، یک محیط تست شامل یک Host، چهار ایستگاه[۲]، چهار AP[۳]، یک سوئیچ OpenFlow و یک کنترل‌کننده ایجاد شد. درلایه کنترل از کنترل‌کننده Floodlight استفاده شد. همچنین درSBI[۴] از پروتکل OpenFlow استفاده گردید.

در ادامه با استفاده از نرم افزار Eclipse، ماژول مورد نظر خود را به کنترل‌کننده Floodlight اضافه نمودیم. این ماژول شامل کدهایی جهت پیاده سازی ۳ حالت زیر می‌باشد:

- شناسایی
- احراز هویت
- اعطای مجوز

کارایی راهکار VISA از دو منظر قابل بررسی می باشد: میزان تاثیر آن بر عملکرد شبکه و امنیت در مقابل حملات.

### ۴-۱. عملکرد شبکه

نظر به اینکه در راهکار VISA از رمزنگاری کلید عمومی استفاده شده است، ممکن است این نگرانی ایجاد شود که این موضوع سبب بروز تاثیر منفی در عملکرد شبکه گردد. با توجه به اینکه در پروتکل OpenFlow فقط اولین بسته از هر جریان داده به کنترل‌کننده ارسال می‌شود، بنابراین مراحل احراز هویت تنها بر روی اولین بسته اجرا شده و در مجموع سبب کاهش معنادار توان عملیاتی[۵] شبکه نمی‌گردد.

جهت بررسی این موضوع، با استفاده از ابزار Iperf، توان عملیاتی شبکه را به مدت ۱۰ دقیقه در دو حالت عادی و بعد از اجرای راهکار VISA اندازه گیری نمودیم. نتیجه آزمایش در جدول ۱ نمایش داده شده است.

[۱] Access Control List
[۲] Station
[۳] Access Point
[۴] Southbound Interface
[۵] Throughput

جدول ۱: مقایسه توان عملیاتی در حالت استفاده از راهکار VISA و بدون استفاده از آن

| کنترل‌کننده | میانگین توان عملیاتی | اطلاعات منتقل شده | مدت زمان اجرا |
|---|---|---|---|
| Floodlight | 1.96 Gbits/sec | 140 Gigabyte | 600 s |
| Floodlight with VISA | 1.95 Gbits/sec | 140 Gigabyte | 600 s |

## ۴-۲. امنیت در مقابل تهدیدها

جهت بررسی امنیت راهکار ارائه شده در مقابل تهدیدها، تعدادی از حمله‌های رایج در IoT را در نظر گرفته و امنیت VISA را در مقابل این حمله‌ها بررسی نمودیم که خلاصه آن در جدول ۲ نشان داده شده است.

جدول ۲: راهکار VISA جهت مقابله با حمله‌ها

| نوع حمله | راهکار در VISA |
|---|---|
| جعل منبع[۱] | استفاده از امضای دیجیتال جهت احراز هویت |
| آدرس دهی[۲] | احراز هویت با استفاده از امضای دیجیتال و بررسی آدرس MAC در نهاد صادر کننده گواهی. |
| Arp Spoofing | احراز هویت برای همه بسته های ارسالی از جمله بسته‌های ARP و تعریف یک مقدار آستانه در میزان ارسال اطلاعات توسط فرستنده معتبر |
| سیلاب SYN | احراز هویت بسته‌های ارسالی در فواصل کوتاه‌تر و اعمال محدودیت در بسته‌های ارسالی SYN |
| حمله Smurf | ثبت اطلاعات هر شی از جمله مبدا و مقصد پیام در قسمت Accounting و اعمال محدودیت در ارسال بسته‌های پینگ از سوی مبدا به مقصد. |
| حمله بازپخش | استفاده از کلید موقت در هر بسته ارسالی |
| حمله شخص میانی | استفاده از کلید موقت و احراز هویت با استفاده از امضای دیجیتال |

پروژه اینترنت اشیا OWASP که به منظور کمک به تولیدکنندگان، توسعه‌دهندگان و مصرف‌کنندگان در شناخت بهتر مسائل امنیتی مرتبط با اینترنت اشیا ایجاد شده است، لیستی از ۱۰ تهدید امنیتی مهم در دنیای IoT را تعریف کرده است [۱۷]. در جدول ۳، وضعیت ایمنی چارچوب VISA در مقابل این ۱۰ تهدید امنیتی نشان داده شده است.

جدول ۳: امنیت VISA در مقابل ۱۰ تهدید امنیتی OWASP

| تهدید | امنیت در VISA | راهکار در VISA |
|---|---|---|
| رابط وب ناامن | ✓ | رابط وب تنها پس از احراز هویت قابل دسترسی است |
| تأیید هویت/ مجوز ناکافی | ✓ | احراز هویت، اعطای مجوز و Accounting کامل |
| خدمات شبکه ناامن | ✓ | ممانعت از دسترسی به شبکه توسط کنترل دسترسی |
| عدم رمزگذاری لایه انتقال[۳] | × | _ |
| نگرانی های حریم خصوصی | ✓ | با احراز هویت، اعطای مجوز و Accounting کامل و کنترل دسترسی از حریم خصوصی محافظت می‌شود |
| رابط ابر[۴] ناامن | ✓ | عدم دسترسی مستقیم به اشیا |
| رابط سیار[۵] ناامن | ✓ | عدم دسترسی مستقیم به اشیا |
| قابلیت تنظیم امنیت ناکافی | ✓ | امکان اعمال سیاست‌های امنیتی برای شرایط مختلف با توجه به ثبت رویدادها در Accounting |
| نرم افزار / میان افزار ناامن | ✓ | عدم دسترسی مستقیم به اشیا و استفاده از Accounting احتمال بروز خطر را کاهش می‌دهد |
| امنیت فیزیکی ضعیف | × | _ |

## ۵- جمع‌بندی

در این مقاله، راهکار VISA معرفی گردید که شامل یک چارچوب امنیتی نرم‌افزار-محور به همراه مکانیزمی جهت احراز هویت اشیا می‌باشد. در VISA به منظور احراز هویت از آدرس MAC اشیا استفاده نمودیم، زیرا در هر کارت واسط شبکه منحصر به فرد بوده و استفاده از آن نیازمند تغییر ساختار شبکه‌های فعلی نمی‌باشد. علیرغم اینکه محدودیت منابع اشیا و نگرانی از کاهش توان عملیاتی شبکه می‌تواند مانعی بر سر راه استفاده از ابزارهای رمزنگاری جهت احراز هویت باشد، اما در این مقاله نشان دادیم که با بهینه سازی فرآیند استفاده از رمزنگاری کلید عمومی می‌توان از امضای دیجیتال به منظور احراز هویت اشیایی همچون سنسور RFID نیز اقدام نمود. این بهینه سازی شامل استفاده از تکنیک و پردازشگرهای کم مصرف جهت انجام

[۱] Source Spoofing
[۲] Address Minting
[۳] Transport
[۴] Cloud
[۵] Mobile

فرآیند رمزنگاری و تولید امضـــای دیجیتال و همچنین کاهش تعداد دفعات استفاده از آن در فرآیند احراز هویت می‌باشد.

## مراجع

[1] Ammar M, Russello G, Crispo B, “Internet of Things: A survey on the security of IoT frameworks”, Journal of Information Security and Applications, No. 38, pp 8–27, 2018.

[2] Jararweh Y, Al-Ayyoub M, Darabseh A, et al, “SDIoT: a software defined based internet of things framework”, Ambient Intell Human Comput 6, pp 453–461, 2015.

[3] Grigoryan G, Liu Y, Njilla L, Kamhoua C and Kwiat K, "Enabling Cooperative IoT Security via Software Defined Networks (SDN)", 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, pp. 1-6, 2018.

[4] Tselios C, Politis I and Kotsopoulos S, "Enhancing SDN security for IoT-related deployments through blockchain", 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, pp. 303-308, 2017.

[5] Bull P, Austin R, Popov E, Sharma M and Watson R, "Flow Based Security for IoT Devices Using an SDN Gateway", 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, pp. 157-163, 2016.

[6] Gonzalez C, Charfadine S M, Flauzac O and Nolot F, "SDN-based security framework for the IoT in distributed grid", 2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech), Split, pp. 1-5, 2016.

[7] Vandana C, “Security improvement in IoT based on Software Defined Networking (SDN)”, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 5, Issue 1, 2016.

[8] Hutter M, Feldhofer M, Plos T, “An ECDSA Processor for RFID Authentication”, Ors Yalcin S.B. (eds) Radio Frequency Identification: Security and Privacy Issues. RFIDSec 2010. Lecture Notes in Computer Science, vol 6370. Springer, Berlin, Heidelberg, 2010.

[9] Flauzac O, Gonzalez C, Nolot F, “New Security Architecture for IoT Network”, Procedia Computer Science, Volume 52, pp. 1028-1033, 2015.

[10] Xin L, Ang L, Xiaowei Y, and David Wetherall, “Passport: secure and adoptable source authentication”, in Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, USENIX Association, USA, pp. 365–378, 2008.

[11] Perlman R, “Network layer protocols with Byzantine robustness”, Ph.D. Thesis on Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1988.

[12] Kent S, Lynn C, Seo K, "Secure Border Gateway Protocol (S-BGP)", in IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 582-592, 2000.

[13] Yao G, Bi J, Xiao P, "Source address validation solution with OpenFlow/NOX architecture", 2011 19th IEEE International Conference on Network Protocols, Vancouver, BC, pp. 7-12, 2011.

[14] Rietz R, Cwalinski R, König H, Brinner A, Wang T, “ An SDN-Based Approach to Ward Off LAN Attacks”, J. Comput. Netw. Commun, 2018.

[15] Almaini A, Al-Dubai A, Romdhani I, Schramm M, Alsarhan A, “Lightweight edge authentication for software defined networks.”, Computing, pp. 1 – 21, 2020.

[16] Ijaz A, Suneth N, Mika Y, Andrei G, “Security in Software Defined Networks: A Survey”, IEEE Communications Surveys & Tutorials, pp. 17, 2015.

[17] Samociuk D, Adamczyk B, “Secure gateway for Internet of Things with internal AAA mechanism”, Theoretical and Applied Informatics, 28(3), pp. 17–35, 2017.