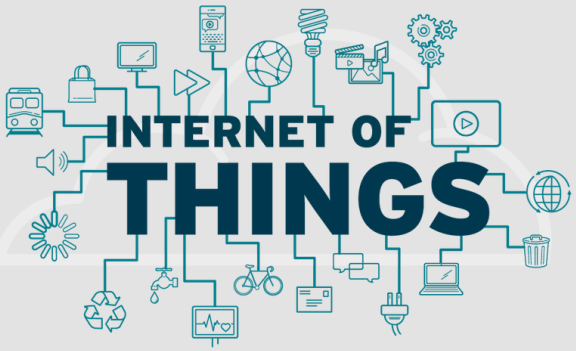
Application of SDN for secure communication in IoT environment



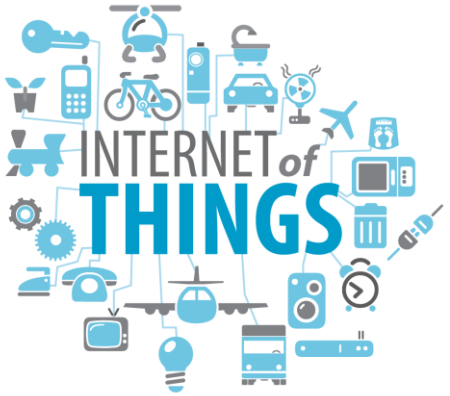
محمد سعید انصاری

دانشجوی دکتری معماری کامپیوتر

استاد گرامی: خانم دکتر جاسبی

تعریف مسئله

- امنیت در اینترنت اشیا متمرکز بر امنیت تجهیزات متصل به هم و شبکه بین آن‌ها است.
- تجهیزات اینترنت اشیا به دلیل
  - محدودیت حافظه
  - توان کم محاسباتی
  - عملیات مبتنی بر باتری



- آسیب‌پذیری زیادی در مقابل حملات دارند.
- در محیط واقعی کاربردهایی از اینترنت اشیا که ایمنی نقش حیاتی در آن‌ها دارد مانند کاربردهای نظامی، سلامت و...، به امنیت نگاه و نیاز ویژه‌ای دارند.
- در این مقاله روشی برای محافظت از اطلاعات الکترونیکی و جلوگیری از آسیب‌پذیری‌های سطح شبکه و Application به نام AESCQTT ارائه شده است.

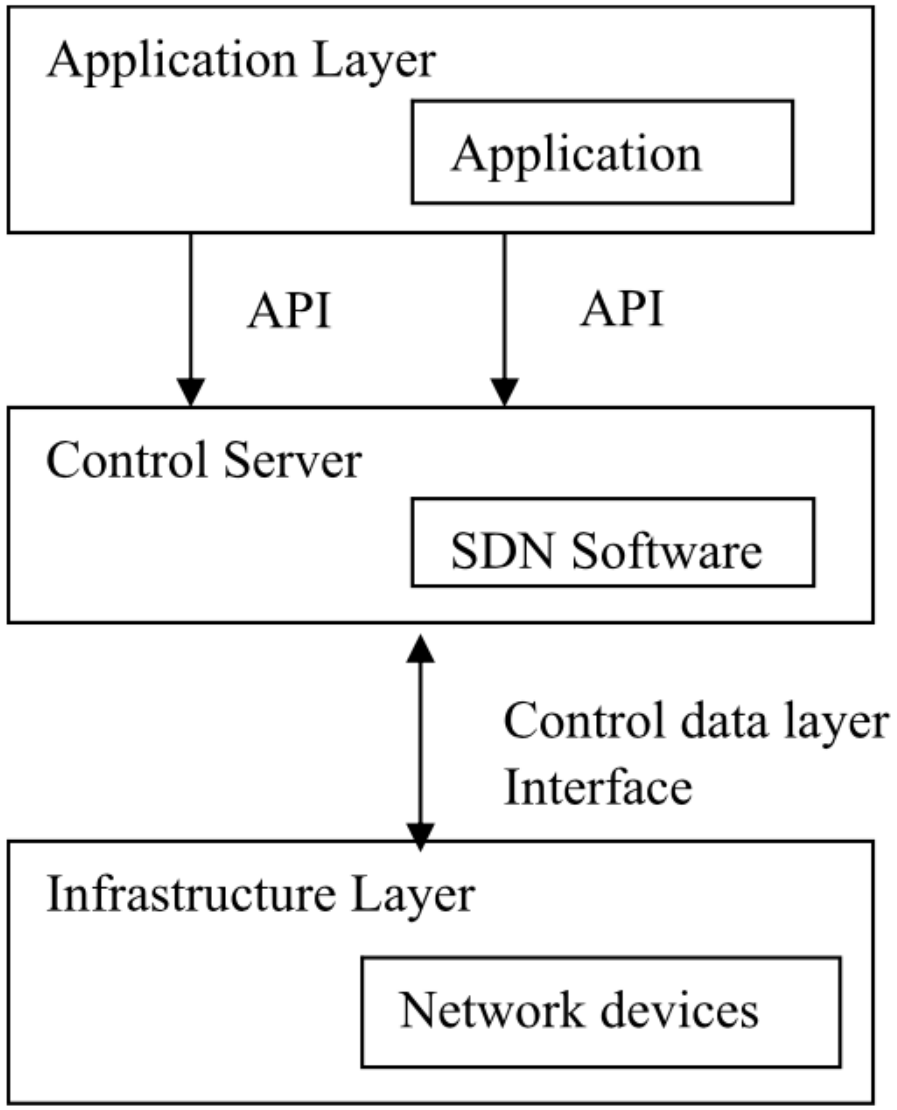
نوآوری

- نوآوری اصلی در این مقاله
  - تاکید بر افزایش امنیت در لایه Application کاربرد اینترنت اشیا با استفاده از تکنیک AESCQTT
- نام این روش مخفف عبارت Advanced Encryption Standard Constrained Queuing Telemetry Transport Protocol است.

رمزنگاری AES

- روش رمزنگاری متقارن (AES) از کلیدی یکسان در فرآیند رمزگذاری و رمزگشایی استفاده می‌کند.
- استاندارد این الگوریتم رمزنگاری به صورت AES-۱۲۸ و AES-۲۵۶ تغییر یافته و بر اساس مدل مورد نظر استفاده می‌شود.

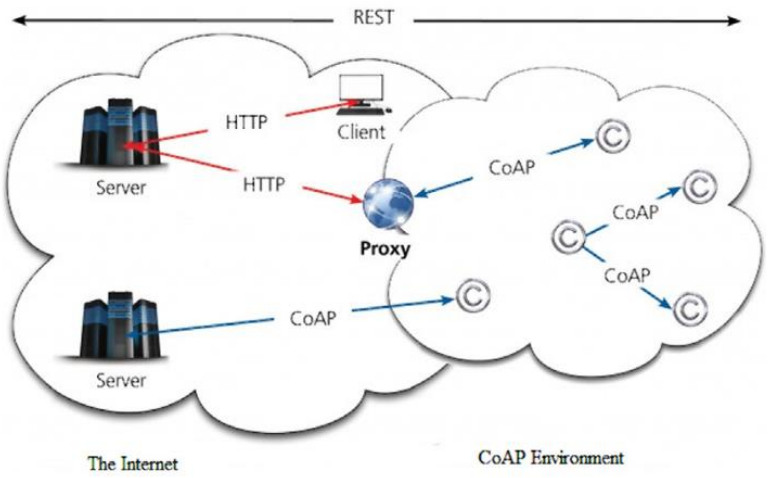
SDN

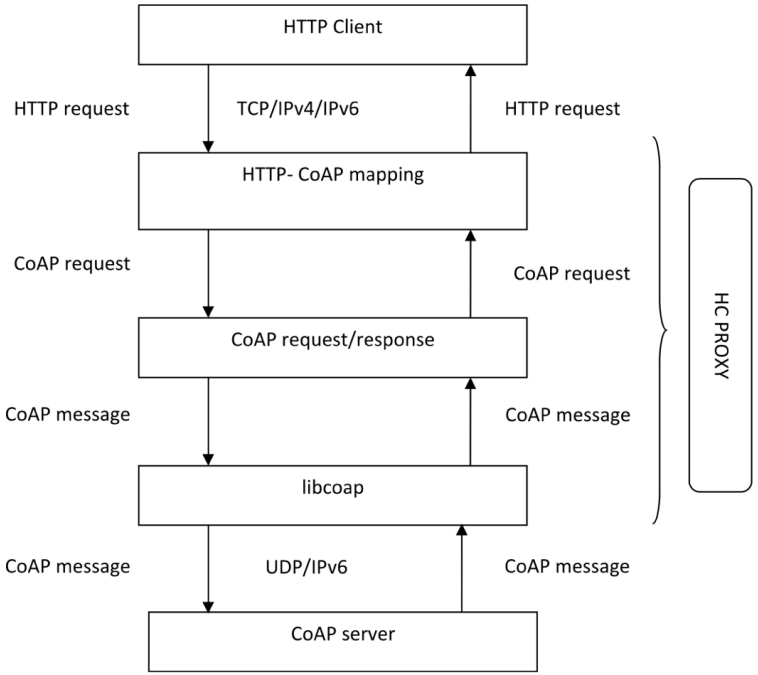


- مهم‌ترین ویژگی SDN تفکیک Forwarding و لایه Control است.
- اهمیت لایه Forwarding جایی مشخص می‌شود که بر اساس جداول و منطق برای بسته‌ها تصمیم گرفته می‌شود.

پروتکل CoAP

- پروتکل CoAP برپایه UDP پیاده‌سازی شده است.
- Proxy CoAP گپ بین شبکه استاندارد مبتنی بر HTTP و شبکه محدود شده برپایه CoAP را پر می‌کند.





این پروتکل از بسته‌های کوچک‌تر، ساده‌تر با اثر کم‌تر استفاده می‌کند و فقط برای تبادل با وب به HTTP مراجعه می‌کند.

مطالعات پیشین

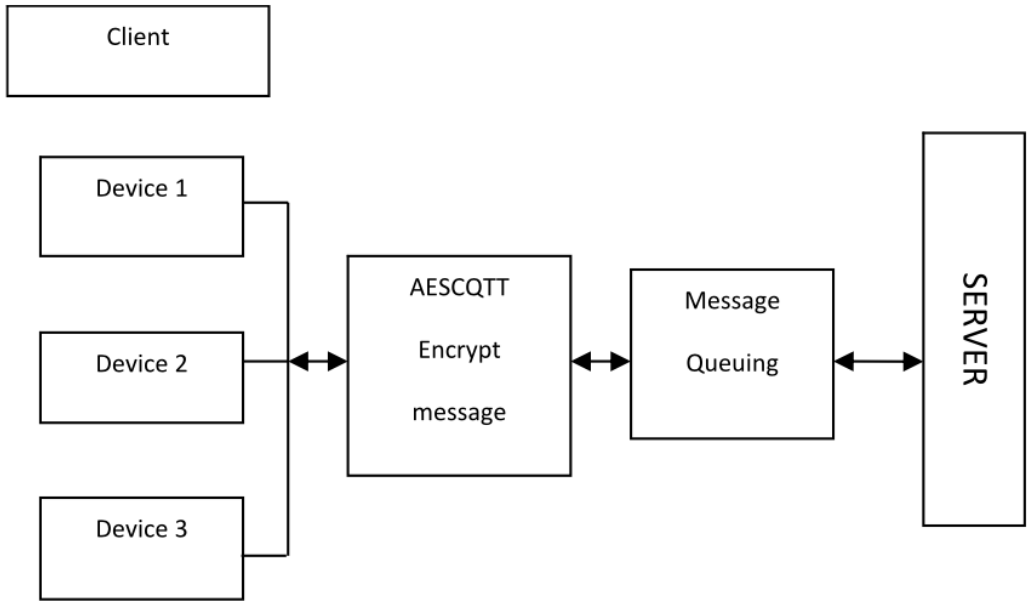
- در مقاله نخست در سال ۲۰۱۸، روشی برای امنیت متصل کننده اینترنت اشیا داده شده است. این روش مبتنی بر جلوگیری از گم‌شدن پیام‌های ارسالی کلاینت به سرور در سیستم ارتباطی است.
- در مقاله دوم در سال ۲۰۱۵، ضمن بررسی مشکلات پروتکل‌های موجود IP در WSN پایه مطالعاتی را بر روش توزیع کلید رمز متمرکز ساخته است.

مطالعات پیشین

- در مقاله سوم در سال ۲۰۱۳، روش رمزگذاری آنلاین و آفلاین را برای محافظت از ارتباطات بین حسگرها در ابر اینترنتی ارائه کرده است.
  - در مرحله آفلاین، محاسبات گسترده و سنگین اجرا می‌شود که کمبود اطلاعات را جبران می‌کند
  - در مرحله آنلاین، فقط محاسبات سبک در صورت وجود پیام انجام می‌شوند.
- بنابراین با این شیوه جلوی حملات جهت دست‌یابی به متن رمز ناکام می‌ماند.

روش پیشنهادی

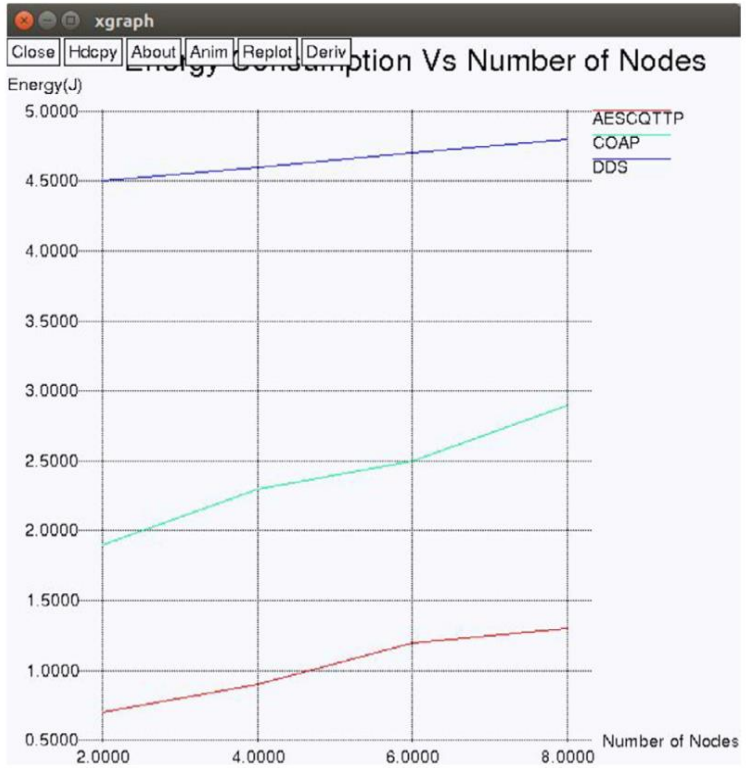
- روش پیشنهادی AESCQTT با تایید و مبادله کلید رمز از داده‌های برنامه محافظت می‌کند.

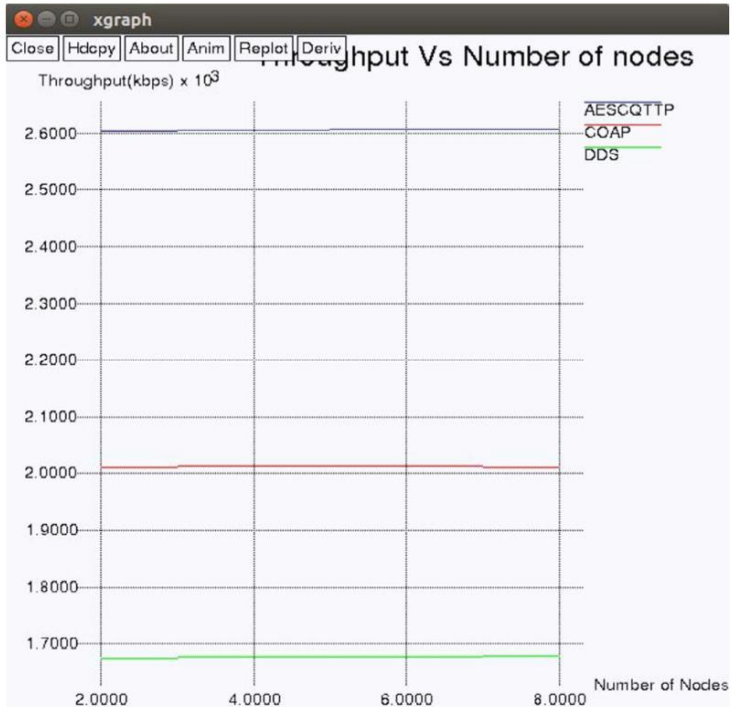


- تمام ارتباط با استفاده از TLS بر خلاف TCP رمز شده و مخاطراتی مانند دستورات XSS جلوگیری می‌شود.
- ساختار این روش از دو بلوک سرور و کلاینت شکل می‌گیرد.
- پیام‌های رمز شده به صورت دوطرفه مبادله می‌شوند. هم‌چنین صف پیام‌ها به صورت FIFO عمل می‌کند.

ارزیابی راه‌حل پیشنهادی

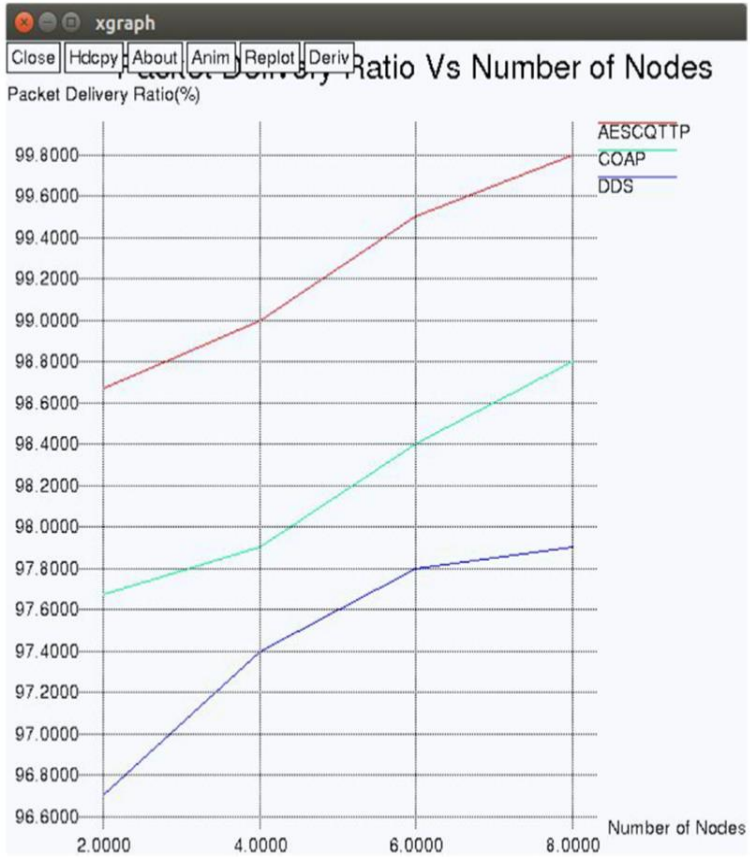
- ابزار شبیه‌سازی NS ۲

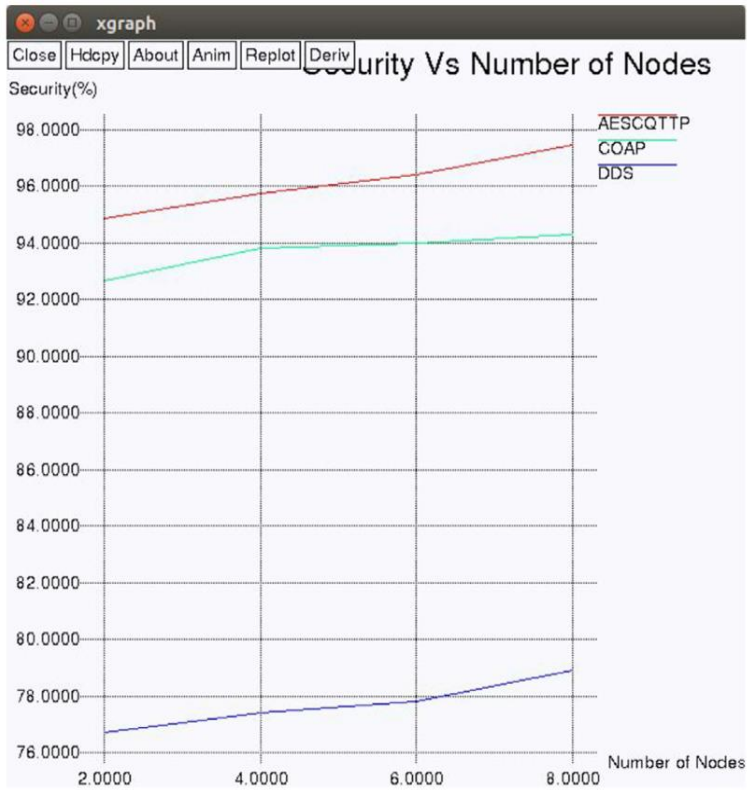




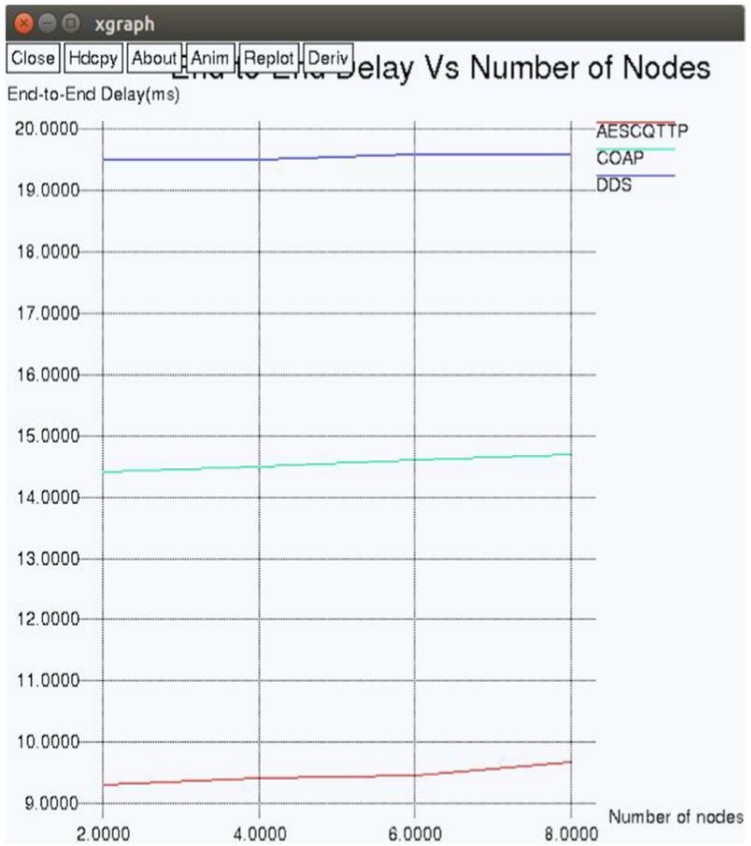
ارزیابی راه‌حل پیشنهادی

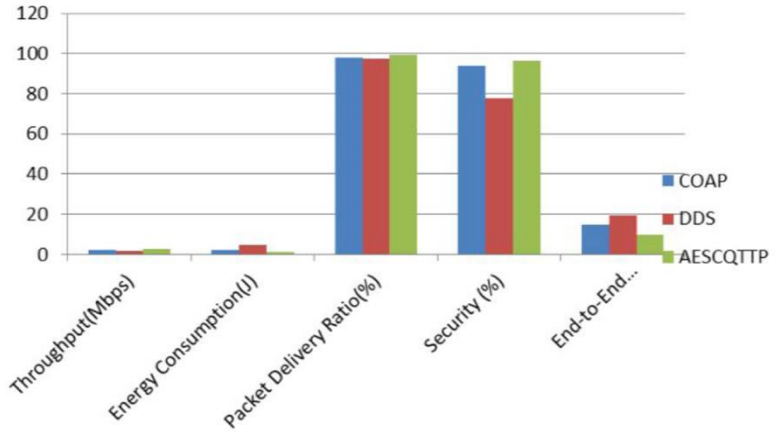
- ابزار شبیه‌سازی NS ۲





ارزیابی راه‌حل پیشنهادی





- در مقایسه با دیگر روش‌ها مانند CoAP (میزان امنیت ۹۳.۷٪) با افزایش امنیت بر اساس معیارهای مقاله به میزان ۹۶.۲٪ بهبودی در شاخص امنیت ایجاد کرده است.

نقاط قوت و ضعف

- نقاط قوت:
  - امکان استفاده همزمان از CoAP و HTTP
  - سرعت روش رمزنگاری به دلیل متقارن بودن
  - امن بودن کل ارتباط که توسط CoAP و TLS امن شده است.
  - استفاده از SDN و تفکیک و کنترل بهتر که امنیت را هم افزایش می‌دهد.
- نقاط ضعف:
  - عدم ارایه دقیق شیوه شبیه‌سازی
  - معیارهای مقایسه شبیه‌سازی دقیق تعریف نشده‌اند

پیشنهادات برای کارهای آتی

- شبیه‌سازی راه‌کار در چند محیط تست متفاوت
- تست انواع حملات و میزان تاثیر آن بر راه‌کار ارایه شده
- تکمیل راه‌کار در زمینه حملاتی که در حال حاضر نمی‌تواند شناسایی کند

مرجع

- Kumar, Rajeesh NV, and Mohan P. Kumar, "Application of SDN for secure communication in IoT environment", COMPUTER COMMUNICATIONS, vol. ۱۵۱, pp. ۶۰–۶۵, ۲۰۲۰

با تشکر از توجه شما

؟