بسمه‌تعالی

گزارش و تحلیل مقاله

Application of SDN for secure communication in IoT environment

تعریف مسئله و هدف اصلی مقاله

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 و عملیات مبتنی بر باتری آسیب‌پذیری زیادی در مقابل حملات دارند. حملاتی که فقط به DDOS و Man-in-Middle محدود نمی‌شوند. 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.

نام این روش مخفف عبارت Advanced Encryption Standard Constrained Queuing Telemetry Transport Protocol است. همانطور که مشخص است این روش از چند قسمت مانند روش رمزنگاری AES و Queuing شکل گرفته است که در ادامه در مورد هرکدام توضیح می‌دهیم.

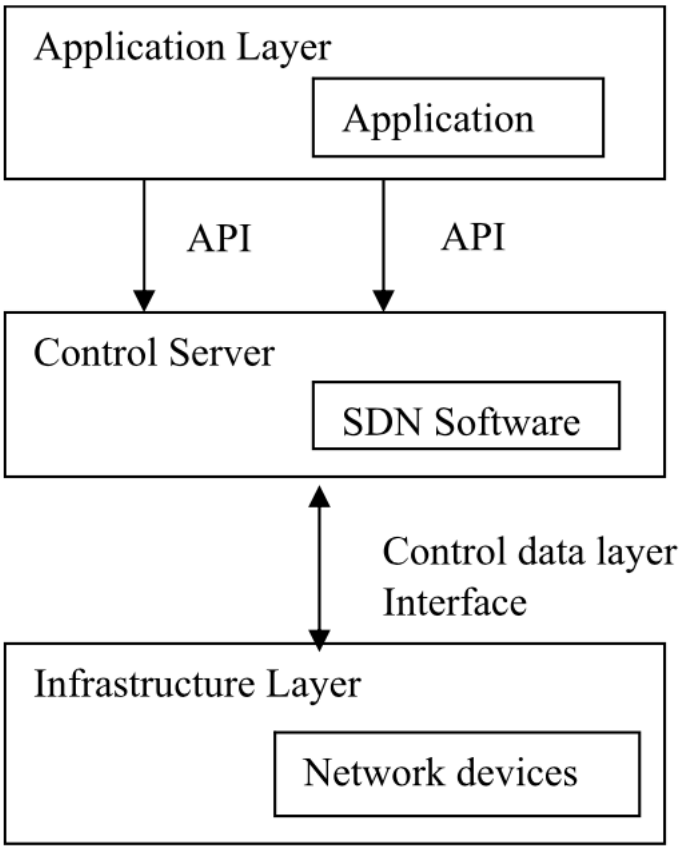
روش رمزنگاری متقارن (AES) از کلیدی یکسان در فرآیند رمزگذاری و رمزگشایی استفاده می‌کند. استاندارد این الگوریتم رمزنگاری به صورت AES-128 و AES-256 تغییر یافته و بر اساس مدل مورد نظر استفاده می‌شود.

در این مقاله، تاکید بر افزایش امنیت در لایه Application کاربرد اینترنت اشیا با استفاده از تکنیک AESCQTT به عنوان نوآوری اصلی یاد شده است.

تحقیقات و روش‌های زیادی در زمینه ایمن‌سازی اینترنت اشیا ارائه شده است که به برخی از آن‌ها اشاره می‌کنیم:

- در مقاله [۱] 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 [۲] سال ۲۰۱۵، ضمن بررسی مشکلات پروتکل‌های موجود IP در WSN پایه مطالعاتی را بر روش توزیع کلید رمز متمرکز ساخته است.
- در مقاله [۳] 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 و 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.

یکی از پایه‌های روش پیشنهادی این مقاله SDN است. مهم‌ترین ویژگی SDN تفکیک Forwarding و لایه Control است (تصویر- ۱). اهمیت لایه Forwarding جایی مشخص می‌شود که بر اساس جداول و منطق برای بسته‌ها تصمیم گرفته می‌شود. بر این اساس بسته‌های ورودی، مصرف، ارسال، حذف و تکرار می‌شوند. اگر بسته‌ای در ارسال به سرور کنترل با مشکل برخورد کند، مجدد ارسال شده و از مفقود شدن بسته جلوگیری می‌شود.

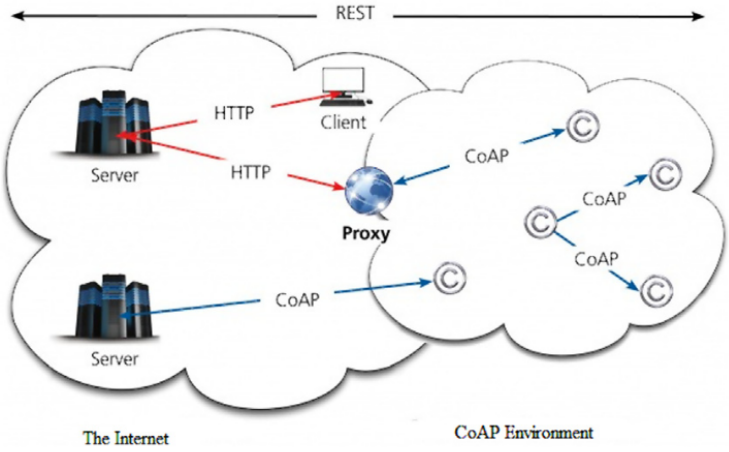


تصویر- ۱

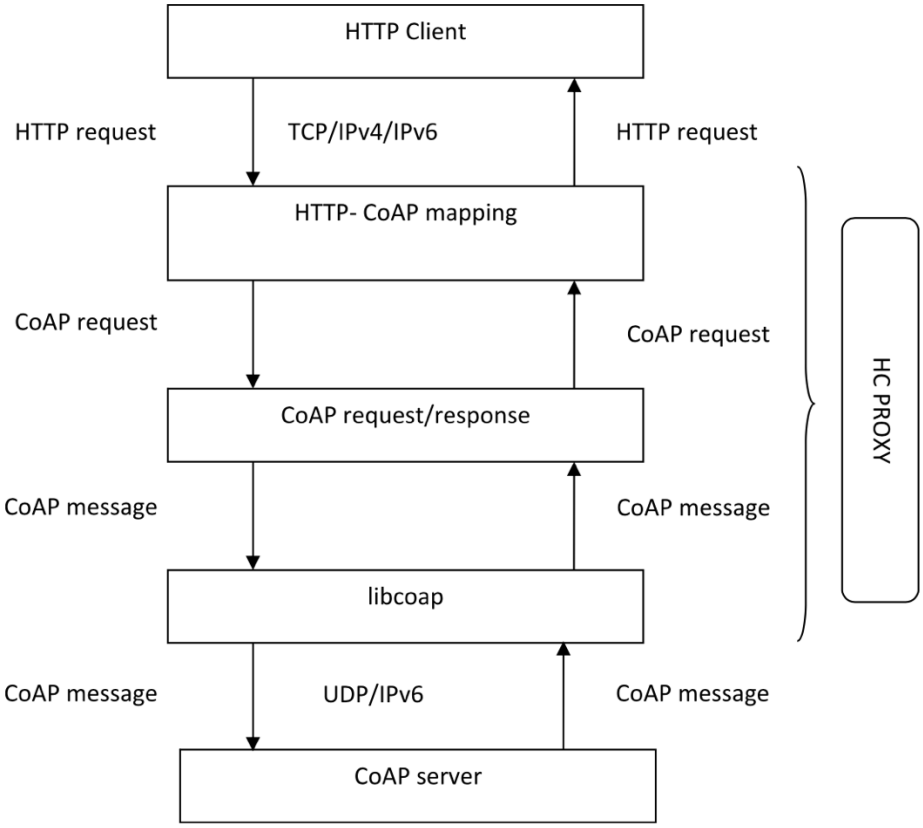
پروتکل CoAP برپایه UDP پیاده‌سازی شده است. این پروتکل در کنار پروتکل HTTP به واسطه proxy می‌تواند بر منابع دسترسی و کنترل داشته باشد (تصویر- ۲). CoAP Proxy گپ بین شبکه استاندارد مبتنی بر HTTP و شبکه محدود شده برپایه CoAP را پر می‌کند. در تصویر- ۳ مدل ارتباطی بین کلاینت HTTP و سرور CoAP نشان داده شده است. بدین صورت سرور CoAP همانگونه که به درخواست‌های کلاینت CoAP پاسخ می‌دهد به کلاینت HTTP هم پاسخ می‌دهد.

پروتکل CoAP برای دستگاه‌های محدود شده طراحی شده است. بسته‌ها در پروتکل CoAP نسبت به HTTP کوچک‌تر هستند. در این پروتکل نگاشت‌ها و فیلدهای بیتی جهت اعداد صحیح استفاده می‌شوند که تحلیل آن‌ها در دستگاه‌های محدود میزان حافظه کمتری نیاز دارد. پروتکل CoAP برپایه TLS عمل می‌کند. در نهایت

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



تصویر- ۲

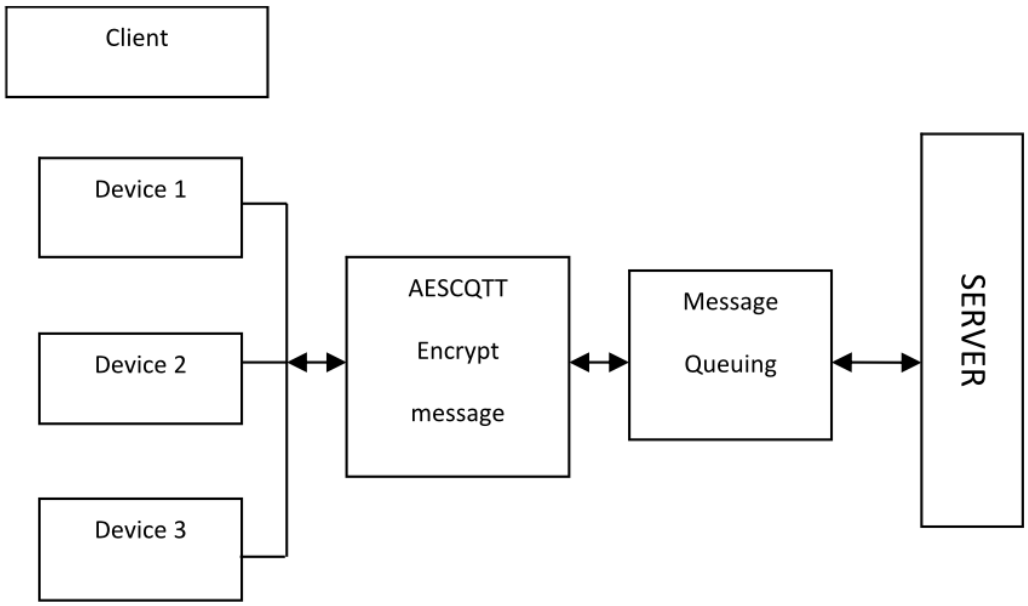


تصویر- ۳

راه‌حل پیشنهادی مقاله برای مسئله

روش پیشنهادی AESCQTT با تایید و مبادله کلید رمز از داده‌های برنامه محافظت می‌کند. در این روش تمام ارتباط با استفاده از TLS بر خلاف TCP رمز شده و مخاطراتی مانند دستورات XSS جلوگیری می‌شود (تصویر-

۴). 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.



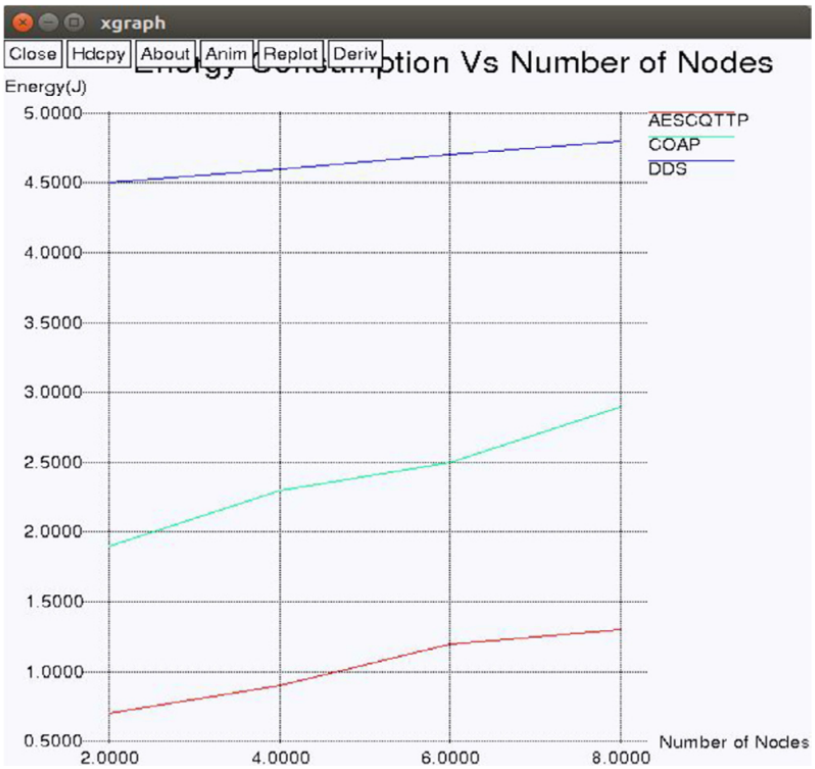
تصویر- ۴

مراحل روش پیشنهادی به این ترتیب هستند:

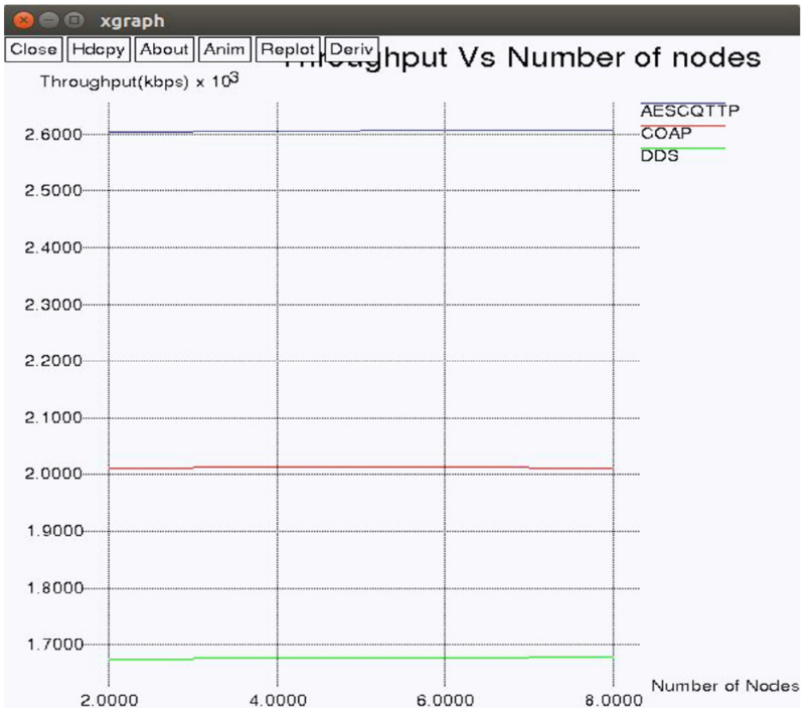
- بسته داده جهت ارسال مقداردهی اولیه می‌شود.
- مقادیر مرزی برای ارسال هر بسته تعریف می‌شوند.
- بررسی می‌شود که آیا بسته دریافت شده است یا خیر.
- سرآیند پیام بررسی می‌شود.
- اگر درست بود ادامه پیام دریافت شده و اگر نه کنار گذاشته می‌شود.
- وضعیت بروزرسانی بسته بررسی می‌شود.
- اگر پیام کامل دریافت شد، برنامه اجرا می‌شود.

رمزنگاری AES استفاده شده در این روش به دلیل کلید یکسان برای رمزگذاری و رمزگشایی در برابر افشای کلید خیلی حساس است. بنابراین به تنهایی استفاده نمی‌شود و در زنجیره‌ای از رمزها قرار می‌گیرد.
تکنیک پیشنهادی ارتباط امنی بین کلاینت و سرور ایجاد می‌کند. اگر تصادم یا ریزش بسته رخ دهد، روش پیشنهادی راه‌کاری برای ارسال مجدد آن ندارد.

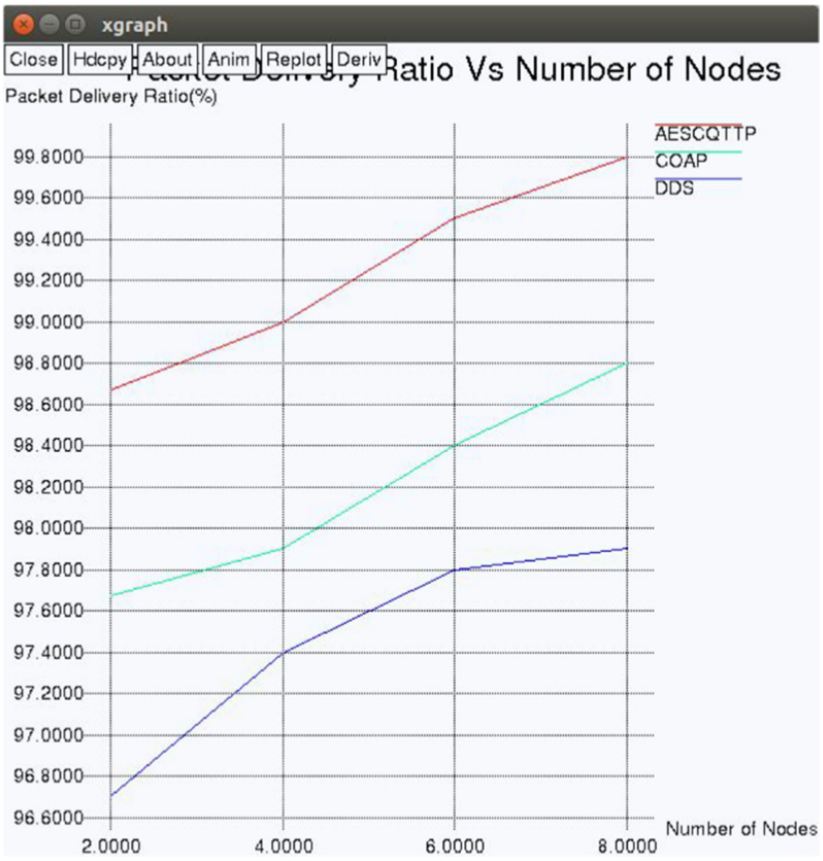
روش پیشنهادی با استفاده از ابزار شبیه‌سازی NS2 از نظر Packet Delivery Ratio، End-to-End delay، Energy efficiency، Security و Throughput با تکنیک‌های CoAP، MQTT و DDS مقایسه شده است.



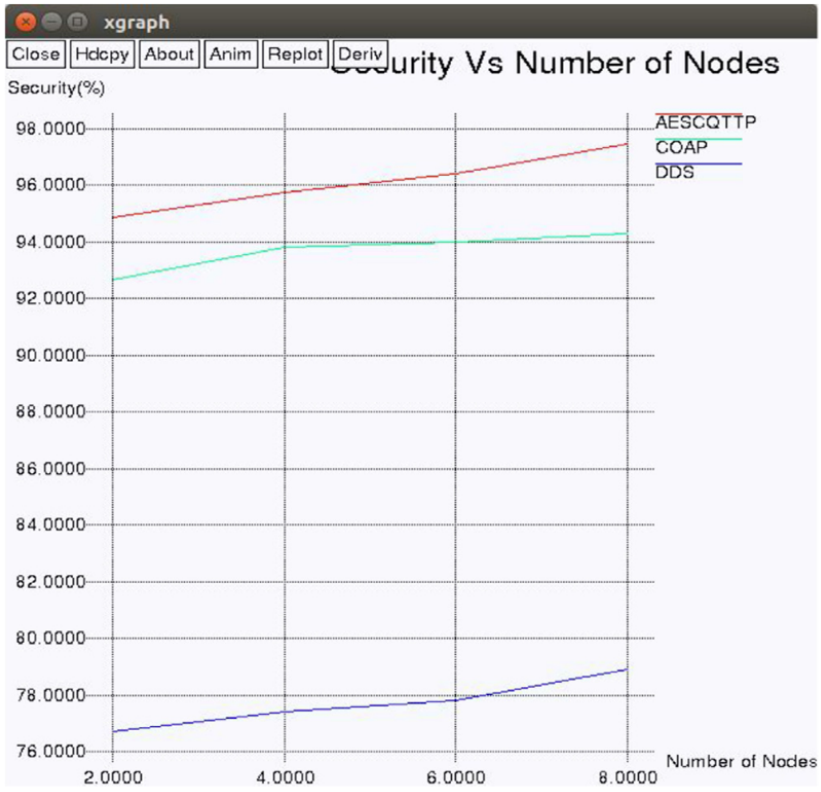
تصویر- ۵- مقایسه *Energy concumption*



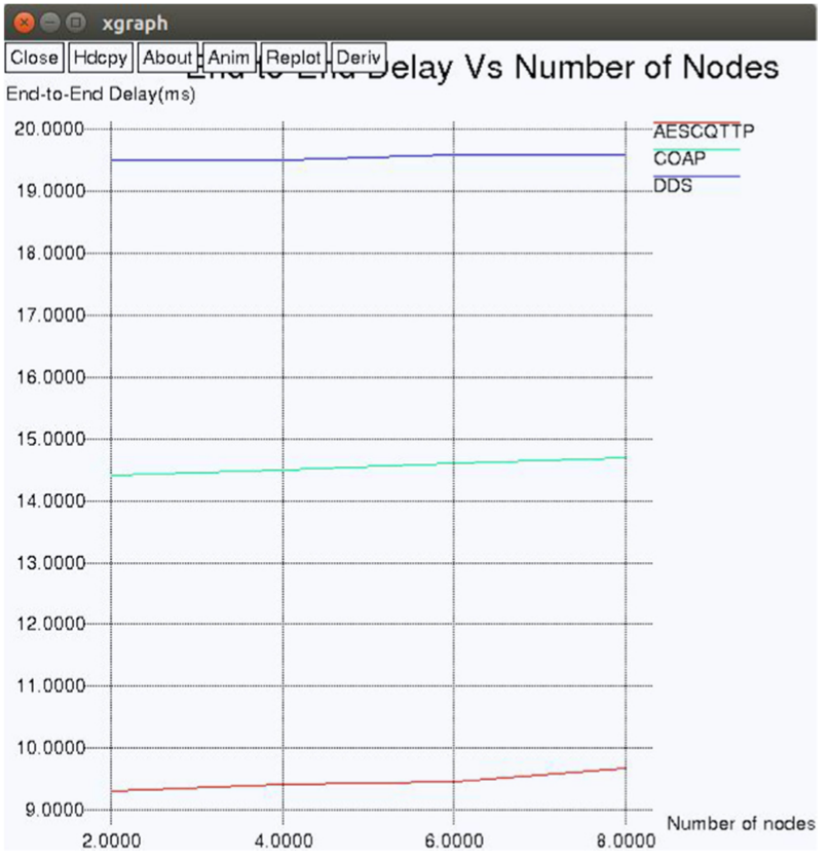
تصویر- ۶- مقایسه *Throughput*



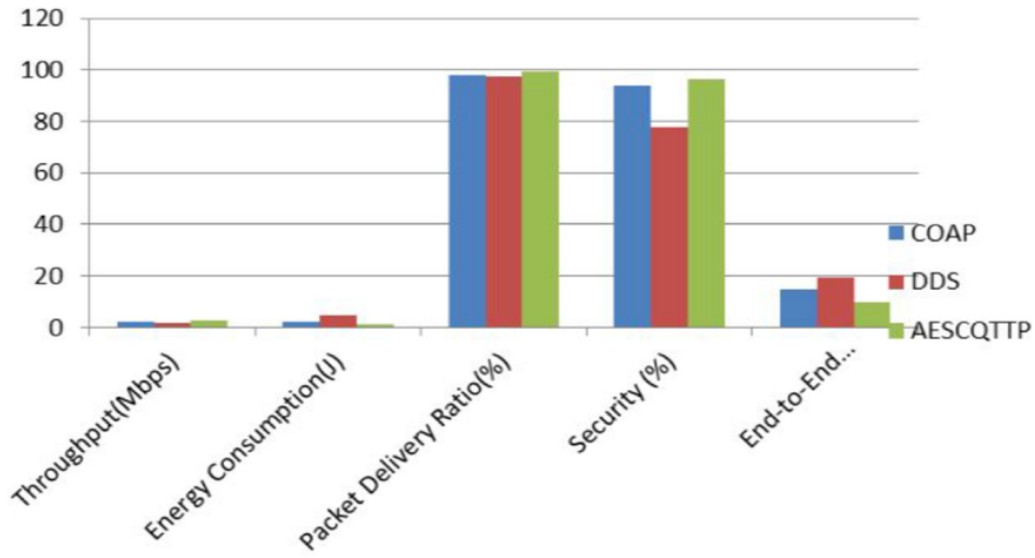
تصویر- ۷- مقایسه *Packet Delivery Ratio*



تصویر- ۸- مقایسه *Security*



تصویر- ۹- مقایسه End-to-End delay



تصویر- ۱۰- مقایسه کارایی

بر اساس نتایج شبیه‌سازی این مقاله، روش پیشنهادی علاوه بر اینکه امنیت را افزایش داده، کیفیت پارامترهایی مانند Throughput را که کاهش نداده، افزایش هم داده است و در مقابل دیگر روش‌ها، برتری نشان می‌دهد.

نقاط قوت و ضعف مقاله

نقاط قوت این مقاله:

- 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 این مقاله:

- عدم ارایه دقیق شیوه شبیه‌سازی
- معیارهای مقایسه شبیه‌سازی دقیق تعریف نشده‌اند

جمع‌بندی و پیشنهادات برای کارهای آتی

در این مقاله روشی برای محافظت از اطلاعات الکترونیکی و جلوگیری از آسیب‌پذیری‌های سطح شبکه و Application به نام AESCQTT ارائه شده که آن را بررسی کردیم. در این روش کل ارتباط با استفاده از TLS امن شده است. این روش 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. علاوه بر این در شاخص‌های دیگر نیز در مقایسه بهبود قابل مشاهده است.

این روش امنیت که یکی از نیازهای اصلی اینترنت اشیا است را درک و بهبود می‌بخشد.

در این راه‌کار مواردی در نظر گرفته نشده است و به صورت کار آتی می‌توان در نظر گرفت:

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

شبیه‌سازی

شبیه‌سازی این مقاله در NS2 انجام شده است. در مورد جزییات شبیه‌سازی و شیوه مقایسه و معیارهای آن صحبتی نشده است و در این شرایط امکان شبیه‌سازی و اعتبارسنجی خروجی‌های مقاله امکان‌پذیر نیست.

مشخصات دقیق مقاله

Kumar, Rajeesh NV, and Mohan P. Kumar, "Application of SDN for secure communication in IoT environment", COMPUTER COMMUNICATIONS, vol. 151, pp. 60-65, 2020

مراجع

[١] Salameh, Haythem A. Bany, Sufyan Almajali, Moussa Ayyash, and Hany Elgala, "Spectrum assignment in cognitive radio networks for internet-of-things delay-sensitive applications under jamming attacks", IEEE Internet of Things Journal 5, No. 3, pp. 1904-1913, 2018

[٢] Nguyen, Kim Thuat, Maryline Laurent, and Nouha Oualha, "Survey on secure communication protocols for the Internet of Things", Ad Hoc Networks 32, pp. 17-31, 2015

[٣] Li, Fagen, and Pan Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things", IEEE Sensors Journal 13, No. 10, pp. 3677-3684, 2013