بسمه‌تعالی

گزارش و تحلیل مقاله

A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks

تعریف مسئله و هدف اصلی مقاله

مدل‌های موجود ارتباطات اینترنت اشیا، مانند زیرساخت‌های امنیتی متمرکز بر ابر، به دلیل محدودیت در منابع و انعطاف‌پذیری، توانایی حفظ امنیت و حریم خصوصی در اینترنت اشیا را ندارند. این ضعف باعث قرارگرفتن تجهیزات اینترنت اشیا در معرض حملات جعل[۱] و ارتقا امتیازات[۲] می‌شود. یک جایگزین جذاب، زنجیره بلوکی[۳] است که زیرساختی غیرمتمرکز برای مقابله با حملات DDoS و مقابله با خطر یک نقطه شکست[۴] ارایه می‌کند.

زنجیره بلوکی به عنوان زیرساخت برای بسیاری از کاربردهای اینترنت اشیا دیده شده است:

- فروش انرژی
- تضمین پرداخت عادلانه در شبکه‌های هوشمند
- وسایل نقلیه الکتریکی
- نظارت بر کیفیت محیط در شهر هوشمند
- سیستم‌های مراقب بهداشتی مورد اعتماد

در کنار مزایای مطرح‌شده، زنجیره بلوکی، به دلیل مصرف بالای برق توسط استخراج کننده، از نظر مالی بهینه نیست. هم‌چنین به دلیل طراحی تغییرناپذیر قراردادهای هوشمند، به‌روزرسانی کد نرم‌افزاری آن‌ها یا وصله‌های امنیتی دشوار یا غیرممکن می‌شود.

شبکه‌های نرم‌افزارمحور به دلیل محول کردن محاسبات به ابر و لبه شبکه، در رفع نیازهای اینترنت اشیا، کمک زیادی می‌کنند. هم‌چنین، شبکه‌های نرم‌افزارمحور در زمانی خرابی گره‌ها، به دلیل هدایت و تقسیم بار، جریان‌ها را به مقصد رسانده و نیازمندی‌های QoS[۵] را برطرف می‌کند.

در تحقیقات پیشین از زنجیره بلوکی برای ایجاد بستری امن در ارتباطات اینترنت اشیا، استفاده شده است:

---

[1] Spoofing

[2] Elevation of privileges

[3] Blockchain

[4] Single point of failure

[5] Quality of Service

- استفاده از الگوریتم‌های PoT[1] و PoL[2] که مه[3] را به عنوان لایه میانی مرتبط کننده تجهیزات اینترنت اشیا و ابر به کار می‌برد.
- معرفی چارچوب Devify برای ساخت شبکه‌های اینترنت اشیا مورد اعتماد قابل همکاری به شیوه غیر متمرکز که مدل هستی‌شناسی[4] وب اشیا را برای توسعه برنامه‌های ابری زنجیره بلوکی اینترنت اشیا، پذیرفته است.
- شناسه یکتای رمزشده به نام Trust Bit (TB) جهت ارتباطات غیر متمرکز وسایل نقلیه هوشمند که از طریق یک سیستم پاداش برای حفظ جزییات TB و پخش TB در زمان اتصال موفق و مورد اعتماد، کار می‌کند.

در تحقیقات پیشین به ادغام زنجیره بلوکی و شبکه نرم‌افزارمحور که باعث انعطاف‌پذیری، کارایی، دسترس‌پذیری و امنیت می‌شود، پرداخته شده است:

- استفاده از شبکه‌های نرم‌افزارمحور در اینترنت اشیا مبتنی بر زنجیره بلوکی، باعث افزایش امنیت داده‌های اینترنت اشیا در مقابل تجزیه و تحلیل ترافیک مخرب می‌شود.
- خودکارسازی روند شک کردن، تایید و اعتماد به سرویس‌های وب اینترنت اشیا جهت حفاظت از آن‌ها در مقابل حملات
- مجازی‌سازی منابع اینترنت اشیا با ترکیب زنجیره بلوکی و شبکه نرم‌افزارمحور با اجرای ارتباطات مبتنی بر مجوز هنگام تهیه منابع
- پیشنهاد چارچوب ChainGuard روی کنترل‌کننده Floodlight برای فیلتر کردن و ردگیری بسته‌های نامتعارف و جلوگیری از رفتارهای مخرب منابع آسیب پذیر

در این مقاله یک معماری مبتنی بر زنجیره بلوکی برای اعمال امنیت بر تراکنش‌های اینترنت اشیا با پیاده‌سازی برنامه‌ای غیرمتمرکز آگاه بر شبکه‌های نرم‌افزار محور ارایه شده است که به گوش دادن به گره‌های استخراج‌کننده، گزارش IPهای مشکوک و اعتبارسنجی بسته‌های ناشناخته می‌پردازد. این معماری الگوریتم اجماع PoA[5] را معرفی می‌کند که دستگاه‌های مشکوک هوشمند اینترنت اشیا را نشان داده و آن‌ها را تحت قرارداد هوشمند، گزارش می‌کند.

برخلاف رویکردهای مطالعات پیشین، راه‌حل این مقاله، لیست‌های سیاه و سفید IP را به توابع مجازی شده درون Docker، محول می‌کند.

---

[1] Proof-of-Trust

[2] Proof-of-Luck

[3] Fog

[4] Ontology

[5] Proof-of-Authority

راه‌حل پیشنهادی مقاله برای مسئله

در این بخش به معماری راه‌حل پیشنهادی می‌پردازیم.

طراحی سیستم

معماری راه‌حل پیشنهادی شامل چهار لایه مختلف است. ابتدا، لایه شبکه همتا به همتا زنجیره بلوکی که از IPFS[1] برای ذخیره و به اشتراک گذاری داده‌ها در یک سیستم فایل توزیع‌شده استفاده می‌کند. گره‌های زنجیره بلوکی، یعنی استخراج‌کنندگان و مشتریان، از IPFS برای همکاری با قراردادهای هوشمند و معاملات زنجیره بلوکی استفاده می‌کنند.

بخش دوم، شامل لایه مجازی‌سازی و لایه انتزاعی سرویس کنترل شبکه، است. لایه مجازی‌سازی، زنجیره بلوکی را روی Kubernetes به صورت زیرساخت به عنوان کد[2] فراهم می‌کند، به صورتی که برنامه‌ها در داخل کانتینرهای Docker در چندین میزبان فیزیکی نگهداری می‌شوند. این لایه همچنین بسیاری از ویژگی‌های مدیریتی را برای تسهیل تنظیم VNFها فراهم می‌کند. از یک سمت، این Applianceهای مجازی، گره‌های غیرمتمرکز زنجیره بلوکی مشتری را به صورت کانتینرهای سبک (مثل Pod) میزبانی می‌کنند که با شبکه اصلی زنجیره بلوکی ارتباط برقرار کرده تا تصمیمات قرارداد-محور را بین یکدیگر انجام دهند. از سمت دیگر، آن‌ها با برنامه‌های کاربردی زنجیره بلوکی (مثل DApps) از طریق ABI[3] روی RPC برای تعامل با قراردادهای هوشمند ارتباط برقرار می‌کنند. قراردادهای هوشمند، اشیا قراردادهای خود-اجرایی[4] هستند که تعامل با گره‌های زنجیره بلوکی را برای تبادل داده‌ها به روشی مطمئن و بدون تعارض آسان می‌کنند.

مدیریت جریان

در تصویر- ۱ جزییات مدیریت جریان بین لایه‌های متفاوت به نمایش درآمده است. لایه زنجیره بلوکی در این معماری از چند واحد شکل گرفته است:

- واحد Identification: با استفاده از کلید عمومی و خصوصی دسترسی کاربر/گره را مدیریت می‌کند. گره‌های اینترنت اشیا با استفاده از ۲۰ بایت انتهایی از ۳۲ بایت کلید عمومی، آدرس می‌گیرند که در حساب گره‌ها جهت دریافت و ارسال تراکنش هم استفاده می‌شود.
- واحد AAA: واحدی جهت احراز هویت، اعطای دسترسی و نگهداری حساب‌ها بر پایه زنجیره بلوکی است. گره‌ها با استفاده از حساب کاربری خاصی که به آن‌ها داده شده است، می‌توانند به سرویس‌های زیرساختی طبق سناریوی خاصی دسترسی پیدا کنند و از طریق API زنجیره بلوکی، منابع مورد نیاز را رزرو کرده و تراکنش را اجرا کنند. احراز بر اساس هویت‌ها انجام می‌شود تا از جعل هویت جلوگیری

[1] InterPlanetary File System

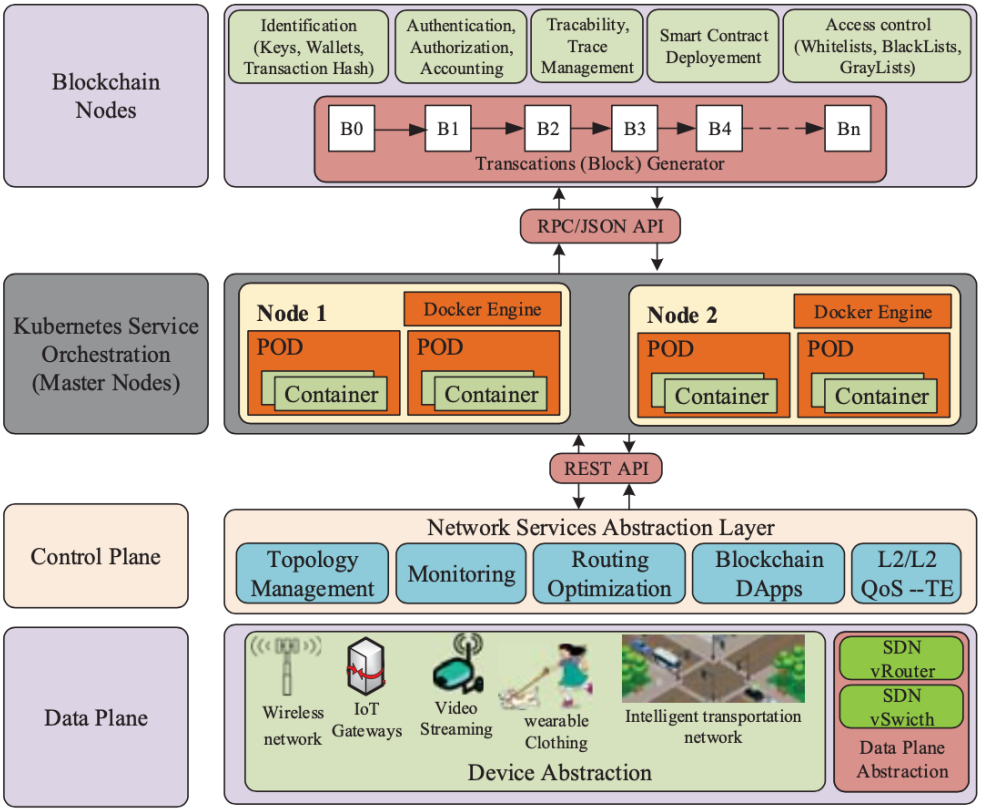
[2] Infrastructure-as-code

[3] Application Binary Interface

[4] Self-executing

شود و از صفحه داده و کنترل در مقابل نفوذ محافظت کند تا از عدم تداخل حملات مخرب با پیکربندی کنترل‌کننده، اطمینان حاصل شود.

- واحد Traceability: این واحد وظیفه دنبال کردن کامل روند تراکنش‌ها از گره مبدا ایجادکننده تا تمامی فرآیندهای روی زیرساخت زنجیره بلوکی را برعهده دارد.
- واحد Smart Contract: وظیفه تعامل بین توابع قرارداد و گره‌های اینترنت اشیا از ایجاد تا پیاده‌سازی را برعهده دارد.



تصویر- ۱

طراحی قرارداد هوشمند

قرارداد هوشمند از ۴۰۰ خط کد ایجاد شده است. گزارش تمامی رفتارهای نادرست علاوه بر MAC و IP، شامل IP گره تحت تاثیر هم هستند. ساختار داده SuspectBehavior جهت کشف و ساختار داده Report جهت گزارش رفتار نادرست به کنترل‌کننده شبکه نرم‌افزارمحور، استفاده می‌شود. یک اعتبارسنج برپایه زنجیره بلوکی، اعتبار تجهزات اینترنت اشیا متصل را بررسی می‌کند. بر اساس پیام‌های OpenFlow، مبدا و مقصد ترافیک ورودی را شناسایی می‌کند. کنترل‌کننده شبکه نرم‌افزارمحور بر اساس اطلاعات موجود در سرآیند بسته‌های OpenFlow، یک دید کلی از شبکه شامل وضعیت ساختار و جزییات تراکنش‌ها، ایجاد می‌کند. بر همین اساس با استفاده بسته‌های رد و بدل شده مابین تجهیزات اینترنت اشیا و شبکه، هرگونه عملیات مخرب را شناسایی می‌کند و لیست سفید و سیاه تجهیزات را ایجاد می‌کند.

الگوریتم اجماع

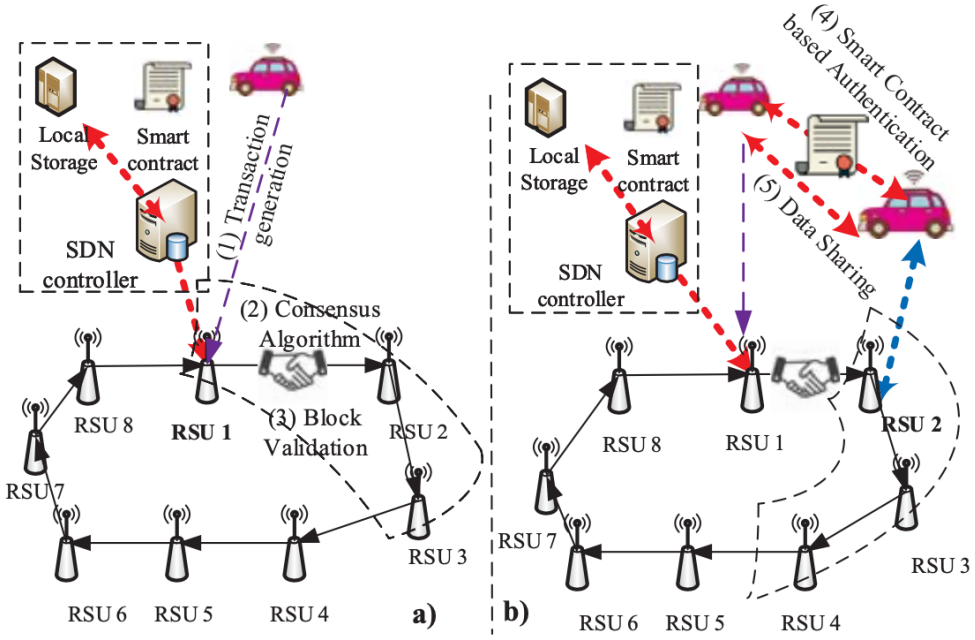
در این مقاله، با استفاده از الگوریتم PoA، تعداد N گره معتمد، انتخاب می‌شود. برای اعمال امنیت شبکه، PoA تعدادی از گره‌های واجد شرایط اینترنت اشیا را از قبل برای اعتبار سنجی تراکنش‌ها، طبق قوانین سخت انتخاب می‌کند. ابتدا گره‌ها بر اساس پارامترهای QoS مثل پهنای باند بیشتر، تاخیر کمتر و منابع سخت‌افزاری بیشتر، انتخاب می‌شوند. این گره‌ها می‌توانند خود تعداد محدودی از سرگروه‌ها که مجموعه‌ای از اختیارات را برای حفظ و کار شبکه دارند را انتخاب کنند.

چارچوب پیشنهادی این مقاله با استفاده از هویت گره‌های از پیش انتخاب شده، در مقایسه با روش الگوریتم PoW[1] بیت‌کوین و PoS[2] اتریوم، به اعتبار یک گره، اهمیت بیشتری می‌دهد. این رویکرد به کارایی بیشتر تمرکززدایی در حالی‌که قدرت محاسباتی کمتری نیاز دارد، به عنوان مزیت دست پیدا می‌کند.

کاربردهای راه‌حل پیشنهادی مقاله

اینترنت وسایل نقلیه[3] مبتنی بر Blockchain-SDN

تصویر- ۲ یک سناریو از اینترنت وسایل نقلیه را نشان می دهد که در آن شبکه‌های توزیع شده، سیستم‌های مختلف اینترنت اشیا مانند اتومبیل‌های متصل، عابر پیاده، جاده‌ها و سیستم‌های پارکینگ را به هم متصل می‌کند.



تصویر- ۲

[1] Proof-of-Work

[2] Proof-of-Stack

[3] Internet of Vehicles (IoV)

همان‌طور که در تصویر- ۲ نشان داده شده است، SDN می‌تواند مسائل مربوط به تغییرات مکرر توپولوژی گره‌ها، تحرک زیاد گره‌ها و تغییرات توپولوژی پویا ناشی از ارتباط گره‌های همکاری را حل کند. به طور خاص، کنترل‌کننده‌های شبکه نرم‌افزارمحور می‌توانند از اطلاعات به دست آمده از واحدهای کنار جاده[1] برای یافتن مسیرهای بهینه به وسایل نقلیه متصل شده و پیام های مسیریابی در کوتاه‌ترین مسیرهای VANET، استفاده کنند. همچنین شبکه نرم‌افزارمحور می‌تواند پوشش RSU را با هماهنگی ارتباط آن‌ها با سایر RSUها و با نقاط دسترسی بی سیم همسایه گسترش دهد. کنترل‌کننده شبکه نرم‌افزارمحور، اطلاعات مسیریابی را از گره‌های VANET جمع می‌کند تا یک نقشه نمای کلی از وسایل نقلیه متصل ایجاد کند و تغییرات توپولوژیکی مختلف را در VANET انجام دهد. به علاوه، در کنار NFV، کنترل‌کننده، کارایی، مقیاس پذیری و QoS را به طور قابل توجهی بهبود می‌بخشد. به طور خاص، شبکه نرم‌افزارمحور/NFV، تولید قوانین جریان را برای پشتیبانی از تخصیص پویا منابع، جداسازی و تنظیم اسلایدهای شبکه و مدیریت تحرک، امکان پذیر می‌کند. RSU بسته‌های دریافت شده از لایه کنترل‌کننده شبکه نرم‌افزارمحور را تجزیه و تحلیل می‌کند تا برای ارسال بسته به وسایل نقلیه متصل شده یا به سمت دیگر RSU، تصمیم بگیرد.

دفترهای[2] توزیع شده زنجیره بلوکی همراه با شیوه‌های اجماع، می‌توانند حفظ داده‌های قابل اعتماد را تضمین کنند. تصویر- ۲ دو مرحله متوالی و چگونگی اجازه سرگروه و مسئولین فعلی را برای تغییر بلوک پیشنهاد می‌کند. ۸ مسئول داریم (RSU1 تا RSU8) که N-(N/2 + 1)=3 آن‌ها اجازه دارند یک بلوک را در هر مرحله پیشنهاد داده و یکی به عنوان سرگروه باشد. در اولین گام (a)، RSU1 سرگروه به همراه RSU2 و RSU3 مجاز به پیشنهاد بلوک هستند. در مرحله بعد (b)، RSU1 دیگر حق پیشنهاد ندارد (باید (N/2)+1 گام صبر کند) و RSU2 به عنوان سرگروه با افزودن RSU4، بلوک‌های جدید را پیشنهاد می‌دهند.

ترکیبی از شبکه نرم‌افزارمحور و زنجیره بلوکی می تواند به طور موثر و کارآمد عملیات سامانه‌های VANET را مدیریت و کنترل کند. زنجیره بلوکی دفترهایی را توزیع می‌کند که تراکنش‌های تولید شده در گره‌های VANET را ثبت کرده و این سوابق را در زیرساخت‌های شفاف، تغییرناپذیر و ایمن حفظ می‌کند. گره‌های RSU می‌توانند برای ایجاد بلوک و انجام استخراج سبک از قبل انتخاب شوند. به عنوان مثال، یک فرایند رای‌گیری می‌تواند برای تایید معاملات و تایید صحت بلوک‌های مبادله شده، بین این گره‌های از پیش واجد شرایط شده، ایجاد شود. پیام های مختلفی که بین RSU رد و بدل می‌شوند می‌توانند به عنوان گواهی بر قابلیت اطمینان داده‌های دریافت شده ثبت شوند. در چنین رویکردی، معاملات جعلی به راحتی توسط خوشه فهرست شده گره‌های VANET قابل تشخیص است و می‌توان تصمیماتی را برای گره‌های فرستنده ارائه داد تا هرگونه نفوذ شناسایی شده را گزارش دهند. در نتیجه، زنجیره بلوکی می‌تواند بلوک ها را همزمان با شبکه نرم‌افزارمحور

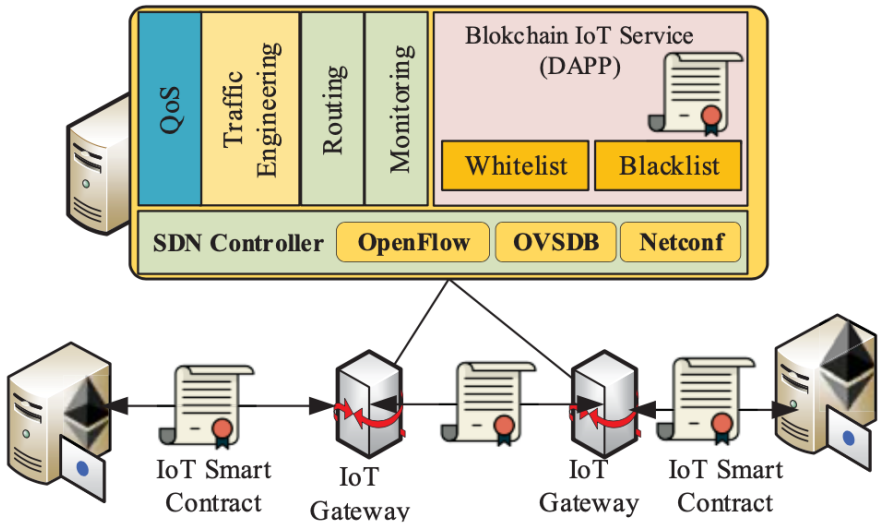
[1] Road Side Units (RSU)

[2] Ladger

کنترل کند تا ضمن جلوگیری از فعالیت‌های مخرب، از یک مدیریت شبکه کارآمد، چابک و انعطاف‌پذیر، اطمینان حاصل کند.

افزایش امنیت بین دروازه[1]های اینترنت اشیا

در تصویر- ۳ شیوه اتصال دروازه‌های اینترنت اشیا به کنترل‌کننده شبکه نرم‌افزارمحور با استفاده از لایه سرویس زنجیره بلوکی توسعه داده شده این مقاله، به نمایش درآمده است.



تصویر- ۳

کنترل کننده شبکه نرم‌افزارمحور یک برنامه غیرمتمرکز مبتنی بر Python را پیاده سازی می کند که با Ethereum Web3 API ادغام شده تا ترافیک را فیلتر کرده و گره‌های مشکوک اینترنت اشیا را شناسایی کند. این یک شیوه همکاری برای ایجاد لیست سفید یا سیاه از آدرس‌های IP دروازه‌های اینترنت اشیا مشکوک را فراهم می‌کند. در این رویکرد، وظیفه ذخیره آدرس‌های IP در لیست سیاه و سفید به VNFها سپرده می‌شود. نمونه‌های VNF می‌توانند به صورت پویا برای تامین شرایط متغیر و مطابقت با تقاضای بیشتر برای ترافیک و یا نیازهای جزیی‌تر خدمات، به کار گرفته شوند.

این رویکرد، مقیاس‌پذیری، انعطاف‌پذیری، چابکی، تاب‌آوری[2] و مدیریت پویای منابع را بهبود داده و اعتماد به شبکه IoT-on-the-blockchain را اعمال می‌کند. در این شرایط، اگرچه تجهیزات اینترنت اشیا برای نیازهای امنیتی به اندازه کافی قدرتمند نیستند ولی با سازماندهی خدمات درخواستی ارائه شده توسط شبکه نرم‌افزارمحور/NFV و قابلیت امنیتی ارائه شده توسط زنجیره بلوکی، می‌توانیم هماهنگی آن‌ها را در تخریب Botnetها در مقیاس بزرگ اعمال کنیم.

[1] Gateway

[2] Resiliency

نقاط قوت و ضعف مقاله

نقاط قوت این مقاله:

- ارائه راه‌کاری که قابلیت پیاده‌سازی در محیط واقعی دارد.
- کنترل دسترسی به صورت جامع بدون نیاز به تعریف قوانین در هر یک از اجزای شبکه به صورت جداگانه و مدیریت مرکزی قوانین بر اساس شبکه‌های نرم‌افزارمحور
- راه‌کار ارائه شده، امکان پیاده‌سازی در محیط‌های موجود بدون نیاز به تغییر در سمت کاربر و در ذات پروتکل OpenFlow را دارد که در مقایسه با دیگر مقاله‌ها امکان استفاده و تست آن را در انواع محیط موجود فراهم می‌آورد.

نقاط ضعف این مقاله:

- میزان تاخیر و سربار احتمالی حاصل از این معماری در مقایسه با دیگر روش‌ها، بررسی نشده است.
- در این مقاله نتایج تست و پیاده‌سازی احتمالی اعلام نشده است و معلوم نیست در شرایط بار زیاد این سامانه و معماری چه واکنشی نشان خواهد داد.
- در این راه‌کار یک کنترلر برای یک شبکه بزرگ داریم که در صورت بروز اختلال در آن، کلیه عملکردهای شبکه مختل خواهد شد. برای مباحث redundancy پیشنهادی در نظر گرفته نشده است.

جمع‌بندی و پیشنهادات برای کارهای آتی

در این مقاله، ما یک معماری جدید اینترنت اشیا به صورت ترکیبی از شبکه نرم‌افزارمحور/NFV و زنجیره بلوکی، ارائه شده است تا شفافیت و امنیت پویای تقاضا را برای تراکنش‌های اینترنت اشیا، فراهم کند. این از کانتینرهای سبک Kubernetes برای تامین نیازهای مختلف مقیاس‌پذیری و کارایی حاکم بر ارتباط اینترنت اشیا، استفاده می‌کند. علاوه بر این، روش اجماع PoA برای انتخاب مسئولین و سرگروه‌ها در اعتبارسنجی معاملات تایید صحت بلوک‌های مبادله شده، معرفی شد. در نتیجه، تراکنش‌های جعلی می‌توانند شناسایی و حذف شوند. برپایه برنامه غیر متمرکز مبتنی بر زنجیره بلوکی که گره‌های مخرب را شناسایی می‌کند، آن‌ها را در لیست سیاه قرار داده و دستورات از راه دور را به کنترل‌کننده شبکه نرم‌افزارمحور داده تا آن‌ها را از شبکه حذف کند.

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

- پیاده‌سازی و مقایسه راه‌کار پیشنهادی این مقاله با روش‌های دیگر در چندین کاربرد واقعی مانند:
  - شبکه VANET
  - شبکه مراقبت‌های بهداشتی
- استفاده از روش‌های یادگیری ماشین در بهبود عملکرد تشخیص گره‌های مخرب
- مقایسه الگوریتم اجماع PoA که در این مقاله پیشنهاد شده با دیگر الگوریتم‌ها و مقایسه نتایج به دست آمده

مشخصات دقیق مقاله

A. Hakiri, B. Sellami, S. Ben Yahia and P. Berthou, "A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks," 2020 Global Information Infrastructure and Networking Symposium (GIIS), 2020, pp. 1-4