نشریه علمی «نوآوری های فناوری اطلاعات و ارتباطات کاربردی»
سال اول، شماره ۲، زمستان ۱۳۹۸؛ ص ۱۶- ۱۱

به‌کارگیری شبکه‌های مبتنی بر نرم‌افزار جهت ارتقای امنیت در اینترنت اشیاء

رضا روزبهی[۱]، محمد قاسم‌زاده[۲*]

۱- دانشجوی کارشناسی ارشد و ۲- دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران

(دریافت: ۱۳۹۸/۰۲/۱۱، پذیرش: ۱۳۹۸/۰۵/۰۹)

چکیده

ارتقای امنیت و حفظ سیاست‌های حریم خصوصی یکی از مطالبات مهم در همه عرصه‌ها، از جمله فضا اینترنت و جنبه‌های خاص آن مانند اینترنت اشیاء (IoT) می‌باشد. برای دست‌یابی به این مهم راه‌کارهای چندی ارائه شده‌اند. در این مقاله نشان می‌دهیم که چگونه می‌توان با بهره‌گرفتن از شبکه مبتنی بر نرم‌افزار(SDN) در اینترنت اشیاء به نتایج ارزشمندی دست یافت. در این رابطه ابتدا به بررسی و تشریح مفاهیم IoT و SDN پرداخته می‌شود و در ادامه روشی برای تلفیق IoT و SDN ارائه می‌گردد که با استفاده از آن می‌توان حملات تهدیدآمیز و اتصالات ناامن را به سرعت شناسایی و قطع نمود. ضمناً چنین مهاجمینی را در یک لیست سیاه قرار می‌دهد تا در آینده اجازه هیچ‌گونه اتصالی به آن‌ها داده نشود. برای ارزیابی عملیاتی روش پیشنهادی نیاز به چندین شیء متصل به اینترنت اشیاء و یک شبکه مبتنی بر نرم‌افزار فعال داریم. تحلیل‌های نظری نشان می‌دهند که تأثیر این روش در آمادگی شبکه در مقابل یورش به داده‌های دستگاه‌های متصل به اینترنت اشیاء و غلبه بر حملات DDoS بسیار چشم‌گیر خواهد بود.

کلید واژه‌ها:

اینترنت اشیاء، شبکه مبتنی بر نرم‌افزار، امنیت، IoT، SDN

۱- مقدمه

اینترنت شبکه جهانی است که ارتباط تمامی کاربران با وسایل و تجهیزات مختلف را با هم برقرار می‌کند، اما ساختار این شبکه در حال تغییر است به گونه‌ای که هم‌اکنون می‌توان آن را مجموعه‌ای بزرگ از بازارهای وسیع و توسعه‌یافته نیز دانست. همگرایی داده‌های بسیار عظیم، حسگرهای چند منظوره و شبکه‌های کارا، فرصت‌های بالقوه و جدید بی‌شماری را پیش‌روی بنگاه‌های اقتصادی قرار داده است. در واقع اینترنت اشیاء (IoT) را تقریباً می‌توان بزرگ‌ترین و جدیدترین بازاری دانست که می‌تواند فرصت‌های بسیار زیادی را برای بنگاه‌های اقتصادی در حوزه‌های مختلف ایجاد کند. هدف اینترنت اشیاء به‌ظاهر ساده است و ظرفیت‌های زیادی پیرامون آن دیده می‌شود. قابلیت‌های متعدد این فناوری موجب شده است شرکت‌ها و کمک‌نوآورهای بسیاری روی آن تمرکز کنند و ایده‌های آن‌ها به ساخت محصولاتی مانند یخچال‌های متصل به اینترنت، روشنایی کنترل‌کردنی از طریق اپلیکیشن و بسیاری دیگر از این محصولات منجر شود.

از دید کمیسیون اروپا دو اصل عمومی در سیاست‌گذاری اینترنت اشیاء وجود دارد، یکی این‌که اینترنت اشیاء نباید هویت، یکپارچگی، حریم خصوصی و حقوق بشری یا آزادی‌های فردی یا عمومی را نقض کند. دیگری این‌که افراد باید کنترل داده‌های شخصی خودشان که توسط یا درون اینترنت اشیاء تولید و پردازش می‌شود را در اختیار داشته باشند، به‌جز زمانی که این اصل با اصل اول در تعارض باشد. از زاویه دید حفاظت از داده‌ها نیز مهم‌ترین چالش‌ها یکی این است که میزان اطلاعات بسیار زیاد است و دیگری این‌که بیشتر ارتباطات به‌صورت خودکار صورت می‌گیرند [۱].

اینترنت اشیاء در حال تبدیل شدن به یک عنصر کلیدی از اینترنت آینده و یک زیرساخت حیاتی ملی و بین‌المللی است. با این شرایط، تأمین امنیت کافی برای زیرساخت‌های اینترنت اشیاء، اهمیت روزافزونی پیدا می‌کند. برنامه‌های کاربردی مقیاس بزرگ و خدمات بر اساس اینترنت اشیاء به‌طور فزاینده‌ای در برابر هرگونه اختلال، حملات و یا سرقت اطلاعات، آسیب‌پذیر هستند.

مسئله امنیت در اینترنت اشیاء را می‌توان مهم‌ترین چالش توسعه این فناوری در نظر گرفت [۲]. در این رابطه استانداردهای مختلفی درحال توسعه است ولی همچنان نیازمندی‌های امنیتی اینترنت اشیاء و حتی مخاطرات آن به‌خوبی شناسایی و تحلیل نشده است. شبکه‌های مبتنی بر نرم‌افزار (SDN) با دارا بودن قابلیت مسیریابی هوشمند ترافیک و استفاده از منابع بلااستفاده در شبکه، آمادگی شبکه برای یورش داده‌های دستگاه‌های متصل

* رایانامه نویسنده پاسخگو: m.ghasemzadeh@yazd.ac.ir

به اینترنت اشیاء را بسیار بیشتر می‌کند. شبکه‌های SDN با رفع نقاط ضعف و افزایش بازدهی، امکان پردازش داده‌های تولیدشده توسط IoT را بدون وارد کردن فشار مضاعف به شبکه، ممکن می‌سازند.

۲- اینترنت اشیاء

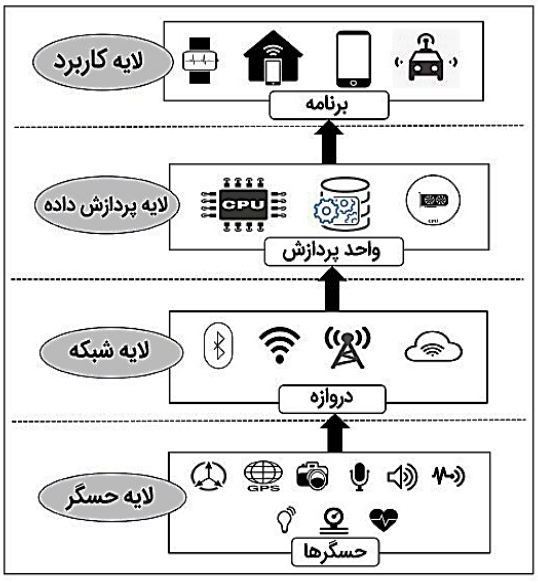
۲-۱- تشریح اینترنت اشیاء

اینترنت اشیاء (IoT) به‌طورکلی به فناوری اطلاق می‌شود که در آن تمام اشیاء و وسایل اطراف ما به شبکه اینترنت و یا اینترانت[۱] باهدف سنجش و کنترل از راه دور متصل شده‌اند و می‌توانند از طریق آن برای هم داده ارسال کرده و با هم در ارتباط باشند.

اتحادیه بین‌المللی مخابرات (ITU) اینترنت اشیاء را زیرساختی جهانی برای جامعه اطلاعاتی که بر اساس فناوری‌های ارتباطی و اطلاعاتی دارای قابلیت تعامل‌پذیری از قبل موجود و رو به رشد از طریق اتصال (فیزیکی و مجازی) اشیاء، خدمات پیشرفته‌ای را ممکن می‌سازد تعریف کرده است [۳].

۲-۲- معماری IoT

در شکل (۱) معماری IoT که شامل ۴ لایه می‌باشد نشان داده شده است.



شکل (۱): لایه‌ها و اجزاء معماری اینترنت اشیاء [۴و۵].

در بحث امنیت لایه‌های شبکه و پردازش داده از اهمیت بالایی برخوردارند. لایه شبکه وظیفه فراهم کردن امکانات شبکه‌ای موردنیاز را دارد. این لایه باید بتواند حجم بالای داده‌ها و اینترنت اشیاء را که توسط حسگرهای بی‌سیم و دستگاه‌های هوشمند تولید می‌شوند، پشتیبانی کند. عملکرد این لایه صرف‌نظر از ماهیت شبکه باید مطمئن و قابل‌اعتماد باشد. همچنین یکپارچه‌سازی پلتفرم‌های اینترنت اشیاء در این لایه از اهمیت بالایی برخوردار است.

لایه پردازش داده نیز مسئولیت تجزیه و تحلیل اطلاعات، کنترل امنیت، مدل‌سازی فرآیندها و مدیریت دستگاه‌ها، مدیریت جریان داده‌ها و اطلاعات و یکپارچه‌سازی سازوکارهای دستیابی به اطلاعات را بر عهده دارد. با توجه به حجم بالای داده، نیاز فیلترینگ نسبت به فرآیند استخراج اطلاعات حس خواهد شد تا بتوان بر اساس پردازش انجام‌شده به یک دید مناسب از داده‌های بزرگ دست‌یافت.

۲-۳- چالش‌های IoT

اینترنت اشیاء باوجود تمام مزایایی که دارد چالش‌هایی را نیز با خود به همراه دارد که از آن جمله می‌توان به مشکلات امنیتی و حریم خصوصی، استانداردها، سازگاری بین تجهیزات مختلف، پهنای باند، سازگاری و طول عمر، برآورده کردن انتظارات مشتریان، به‌روز نگه‌داشتن سخت‌افزاری، غلبه بر مشکلات ارتباطی و انتظار برای مقررات دولتی اشاره کرد.

برقراری امنیت و حفظ حریم خصوصی شاید بزرگ‌ترین چالش در IoT باشد [۲]. از آن‌جا که اشیاء به اینترنت متصل هستند همانند کامپیوتر و موبایل‌های هوشمند آن‌ها نیز در معرض نفوذ غیرمجاز و هک شدن می‌باشند.

به علت گستردگی افرادی که با مجموعه اینترنت اشیاء در ارتباط خواهند بود در صورت هک شدن آن‌ها، اثرات زیان‌بار و گسترده‌ای خواهد داشت. البته امنیت در اینترنت فعلی هم یک چالش بزرگ به شمار می‌آید، اما در اینترنت اشیاء این مسئله ابعاد بزرگ‌تری پیدا می‌کند. توزیع‌شدگی بیش‌تر شبکه و به‌تبع آن نقاط ورود بیش‌تر به سامانه، یکی از دلایل این موضوع است.

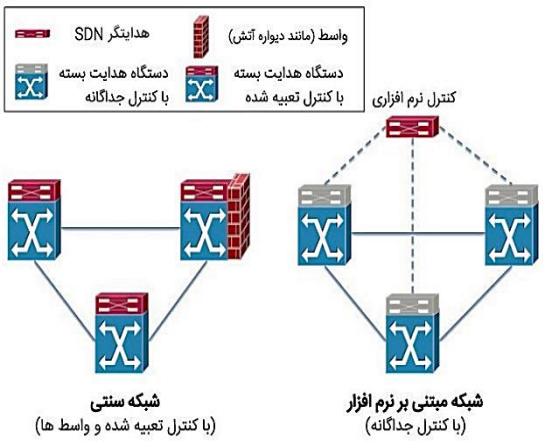
همچنین اشیائی که قرار است به اینترنت متصل شوند، معمولاً ساختار و معماری ساده‌تری نسبت به کامپیوترها دارند و این موضوع پیاده‌سازی ابزارهای امنیتی را در آن‌ها دشوار می‌سازد و سبب می‌شود کار بیشتری را طلب کند. آخرین دلیل برای حیاتی بودن امنیت IOT این است که اینترنت اشیاء خیلی بیش‌تر از اینترنت فعلی به زندگی واقعی نزدیک شده است. درواقع نفوذ به چنین شبکه‌ای معادل بانفوذ به زندگی روزمره‌ی کاربران خواهد بود.

[۱] شبکه محلی

۳- شبکه‌های مبتنی بر نرم‌افزار

اساس مفهوم شبکه مبتنی بر نرم‌افزار (SDN) درواقع جداسازی لایه سخت‌افزاری از لایه کنترلی است. به‌طور سنتی هر روتر و سوییچ در شبکه یک نرم‌افزار از قبل نصب‌شده دارد که فعالیت های آن را مدیریت می‌کند و این موضوع به این معنی است که در صورت نیاز به هرگونه تغییر در شبکه باید هر بخش جداگانه تنظیم مجدد شود. به کمک SDN یک مرکز مدیریت جامع خواهیم داشت که تغییرات شبکه را تقریباً به‌صورت لحظه‌ای اعمال می‌کند بدون اینکه نیازی به تغییر تنظیمات بخش فیزیکی شبکه باشد. این موضوع به مدیران IT کنترل بیشتری بر شبکه خود را می‌دهد و شبکه را بسیار انعطاف‌پذیر می‌کند.

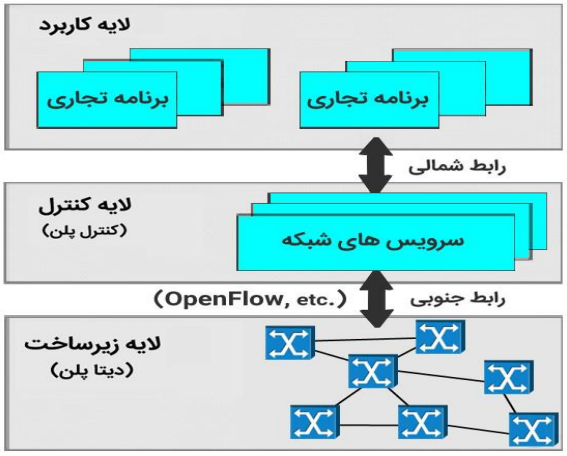
همان‌طور که در شکل (۲) می‌بینیم، برخلاف روش سنتی، در این روش کنترل جریان از سطح سخت‌افزاری در گره‌های شبکه خارج شده و به‌صورت متمرکز و جداگانه توسط یک هدایتگر بر عهده گرفته می‌شود. سوییچ‌های SDN توسط یک سیستم‌عامل شبکه مدیریت می‌شوند که اطلاعات را توسط APIها جمع‌آوری می‌کند و به‌وسیله آن‌ها لایه دیتا را ایجاد می‌کند. سپس یک مدل از توپولوژی شبکه را در اختیار هدایتگر SDN قرار می‌دهد. بنابراین، هدایتگر می‌تواند از تمامی اطلاعات شبکه به‌منظور بهینه‌سازی جریان و تأمین نیازهای کاربر استفاده کند. به‌عنوان مثال می‌توان پهنای باند شبکه را به‌صورت پویا به لایه دیتا تخصیص داد.



شکل (۲): نمای کلی شبکه سنتی و شبکه مبتنی بر نرم‌افزار [۶].

۳-۱- معماری SDN

در معماری شبکه‌های SDN سعی شده است که توانایی و هوشمندی شبکه‌های کامپیوتری بیشتر شود. این کار با جداسازی بخش کنترل داده‌ها از سوییچ و روتر سخت‌افزاری و تمرکز آن‌ها در لایه‌های نرم‌افزاری مجازی شبکه انجام می‌شود. یک هدایتگر نرم‌افزاری متمرکز که دیدی از کل شبکه را در اختیار داشته، بسیار مؤثرتر و هوشمندتر از بخش‌های کنترلی پراکنده روترها و سوییچ‌ها عمل خواهد کرد. با یک هدایتگر متمرکز، قابلیت‌هایی مانند برنامه‌ریزی، مقیاس‌پذیری، انعطاف‌پذیری، خودکارسازی و توسعه نرم‌افزاری به شبکه اضافه می‌شود. شکل (۳) معماری SDN که را نشان می‌دهد.



شکل (۳): لایه‌ها و اجزای معماری شبکه‌های مبتنی بر نرم‌افزار [۷-۸].

بخش‌های مختلف شکل عبارت‌اند از:

لایه زیرساخت: این بخش به‌طور مستقیم مسئول ارسال داده‌ها بر اساس جدول‌های برنامه‌ریزی‌شده توسط هدایتگرها است.

رابط جنوبی: توسط ONF- Open Networking Foundation و با نام OpenFlow استاندارد شده است. OpenFlow امکان دسترسی مستقیم و ایجاد تغییر در برنامه ارسال تجهیزات شبکه نظیر سوئیچ‌ها را، هم به‌صورت فیزیکی و هم مجازی فراهم می‌کند.

لایه کنترل: با همه دستگاه‌های موجود در یک دامنه شبکه ارتباط مستقیم داشته، از توپولوژی شبکه آگاه است و شبکه را از یک نقطه مرکزی برنامه‌ریزی می‌کند.

رابط شمالی: برای برقراری ارتباط میان هدایتگر و سرویس‌ها و برنامه‌های کاربردی در حال اجرای شبکه استفاده می‌شود. این رابط برای تسهیل نوآوری و ارائه سرویس‌های جدید با روشی آسان استفاده می‌شود.

لایه کاربرد: در این لایه برنامه‌ها از طریق رابط شمالی مابین کنش‌ها و منابع موردنیاز هدایتگر ارتباط برقرار می‌کند. علاوه بر این، برنامه‌های کاربردی می‌توانند از طریق جمع‌آوری اطلاعات از هدایتگر یک دید انتزاعی از شبکه ایجاد نمایند که برای تصمیم‌گیری مورد استفاده قرار می‌گیرد [۹-۱۰].

۴- تلفیق IoT و SDN

SDN یک راه‌کار کلیدی برای حل مشکلات IoT است. نمی‌توان گفت که IoT به SDN وابسته است، ولی SDN می‌تواند فواید زیادی برای IoT داشته باشد. بااین‌حال، به‌کارگیری SDN اقدامی ضروری از طرف ارائه‌دهندگان خدمات برای استفاده از فرصت‌های IoT است. استفاده از قابلیت‌های SDN این کار را برای ارائه‌دهندگان زیرساخت شبکه آسان‌تر خواهد نمود، به‌ویژه قابلیت‌هایی شامل؛ بهبود زنجیره خدمات، مدیریت پویای ترافیک شبکه و مدیریت زمانی استفاده از پهنای باند. که در نتیجه قدمی بسیار بزرگ در بحث امنیت و حفظ سیاست‌های حریم خصوصی در IOT خواهد بود.

زنجیره خدمات، امکان اولویت‌بندی فعالیت‌های پردازشی مرتبط با برنامه‌های کاربردی را برای هر یک از کلاینت‌ها فراهم می‌سازد. بهبود زنجیره خدمات به اپراتورها امکانات مختلفی می‌دهد؛ مثل تأمین امنیت مجازی از طریق VPNها، فایروال‌ها و فناوری‌های احراز هویت، یا تعیین حداقل عملکرد قابل‌قبول در سیاست‌های سازمان به‌منظور تأمین حقوق و اختیارات مشترکان.

مدیریت پویای ترافیک نیز امکان نظارت و هماهنگ کردن تغییرات پهنای باند را به صورت خودکار برای اپراتورها فراهم می‌کند. چنین چیزی به‌خصوص برای ارائه‌دهندگان خدمات IoT در سطح جهانی، که خود را برای افزایش تصاعدی تعداد دستگاه‌ها و داده‌های IoT آماده می‌کنند، بسیار ایده‌آل است.

مدیریت زمانی استفاده از پهنای باند نیز به اپراتور اجازه می‌دهد تا زمان و میزان ترافیک موردنیاز مشتریان یا برنامه‌های کاربردی را برای هر بازه زمانی، برنامه‌ریزی کند.

SDN کمک می‌کند که مجموع عملیات بسیار کاهش یابند. امکانات SDN مثل خودکارسازی، تأمین منابع، قابلیت برنامه‌ریزی و هماهنگی، می‌تواند ارزش زیادی را در یک محیط مبتنی بر IoT ایجاد کند. همچنین استانداردهای SDN مانند OpenFlow می‌توانند توزیع سیاست‌های امنیت و همچنین قابلیت همکاری میان دستگاه‌های مختلف IoT را تسهیل کنند [۱۰].

SDN دارای ویژگی‌های متمایزی است که این ویژگی‌ها سبب ارائه مزایای زیادی برای غلبه و شکست حملات DDoS می‌شوند:

۱- تفکیک سطح کنترل از سطح داده‌ها: همان‌طور که در بخش ۳ این مقاله گفتیم SDN سطح کنترل را از سطح داده‌ها جدا می‌سازد، و ازاین‌رو امکان انتشار حمله در مقیاس بزرگ و آزمایش دفاعی را به‌آسانی فراهم می‌سازد. قابلیت پیکربندی عالی SDN سبب تفکیک مشخص میان شبکه‌های مجازی می‌شود، و اجازه آزمایش در محیط واقعی را می‌دهد. پیشرفت در توسعه ایده‌های جدید می‌تواند با استفاده از انتقال یکپارچه از فاز آزمایشی به فاز عملکردی، به اجرا درآید. این ویژگی SDN، تسهیلات زیادی را در مطرح کردن اندیشه‌ها و روش‌های جدید برای کاهش حمله DDoS، ارائه می‌دهد.

۲- هدایتگر مرکزی و نمای شبکه: هدایتگر دارای معلومات و اطلاعاتی از کل سامانه شبکه و نظریه‌های کلی برای ایجاد تدابیر امنیتی پایدار است، همچنین الگوهای ترافیکی را برای تهدیدهای امنیتی بالقوه نظارت، تحلیل و مطالعه می‌کند. کنترل مرکزی SDN، این امکان را فراهم می‌سازد تا به‌طور فعال گروه‌های به خطر افتاده را قرنطینه نموده و به گروه‌های مجاز بر اساس اطلاعات به دست آمده از درخواست گروه‌های نهایی رسمیت بخشد و شاخص تصدیق و شناسایی از راه دور را در سرورهای سرویس کاربر به‌منظور تصدیق و سندیت اطلاعات کاربران و پایش سامانه در طی ثبت، از دور کنترل نماید.

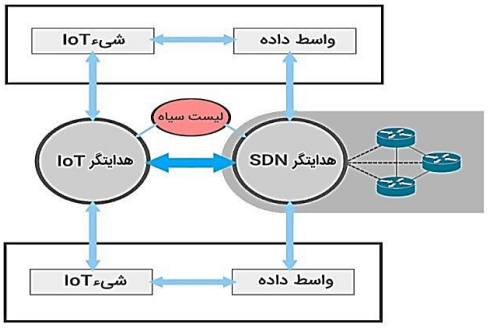
۳- قابلیت برنامه‌ریزی شبکه به‌وسیله برنامه‌های خارجی: قابلیت برنامه‌ریزی SDN، از پروسه بهره‌برداری اطلاعات از سامانه‌های کشف مزاحمت و نفوذ و همچنین سامانه‌های پیشگیری از مزاحمت و نفوذ، پشتیبانی می‌کند. بیشتر الگوریتم‌های هوشمند می‌توانند بر اساس حملات مختلف DDoS، با انعطاف بالایی مورداستفاده قرار گیرند.

۴- تجزیه و تحلیل ترافیک مبتنی بر نرم‌افزار: تجزیه و تحلیل‌های ترافیک بر اساس نرم‌افزار، سبب نوآوری می‌شود طوری که می‌تواند با استفاده از همه انواع الگوریتم‌های هوشمند، پایگاه‌های داده، و هرگونه ابزار نرم‌افزاری دیگری، اجرا شود.

۵- به‌روزرسانی پویای قوانین حمل‌ونقل (ارسال) و انتزاع جریان: تجدید پویای قوانین حمل‌ونقل از واکنش سریع به حملات DDoS حمایت می‌کند. بر اساس تجزیه و تحلیل‌های ترافیک، تدابیر امنیتی جدید به‌روزرسانی شده می‌تواند در سراسر شبکه به شکل قوانین جریان برای بلوکه کردن ترافیک حمله بدون به تأخیر افتادن، توسعه یابد [۱۱].

۴-۱- معماری پیشنهادی (تلفیق IOT و SDN)

شکل (۴) معماری پیشنهادی ما برای تلفیق IOT و SDN را نشان می‌دهد.



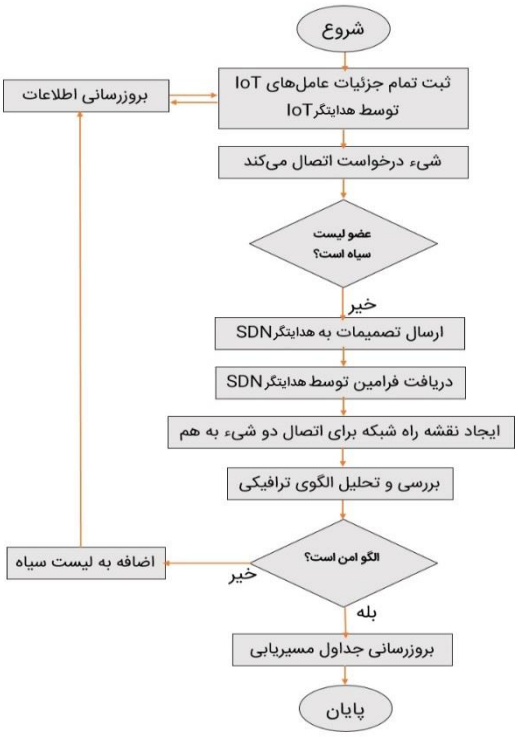
شکل (۴): معماری پیشنهادی برای تلفیق IoT و SDN.

بخش‌های مهم و اصلی این معماری را یکی هدایتگرها یعنی هدایتگر IoT و هدایتگر SDN و دیگری اشیاء و داده‌ها تشکیل داده است. درواقع برای ارتقای امنیت و حفظ حریم خصوصی اینترنت اشیاء مدیریت متمرکزی از هدایتگرها داریم که اشیاء و اتصالات آن‌ها را بررسی و تحلیل می‌کنند و فرامین لازم را صادر می‌کنند و در این بین لیست سیاه را می‌توان کلیدی‌ترین نکته این معماری دانست.

در بخش بعدی فلوچارت و روش کار را به‌صورت کامل توضیح داده‌ایم.

۴-۲- فلوچارت روش پیشنهادی

در شکل (۵) روش کار معماری پیشنهادی را به‌صورت فلوچارت نشان داده‌ایم.



شکل (۵): فلوچارت روش پیشنهادی.

روش کار این‌گونه است که هدایتگر IoT تمام جزئیات عامل‌های IoT مانند شناسه شیء، آدرس، پروتکل شبکه و زیر شبکه را ثبت می‌کند. هر دستگاه IoT یک عامل IoT دارد که با هدایتگر IoT ارتباط برقرار می‌کند. عامل IoT نیز مسئول شناسایی، تجزیه، تحلیل و جمع‌آوری داده‌ها از محیط برای دستیابی به اهداف کاربر است. هر شیء در IoT می‌تواند با هر شیء دیگر از طریق شبکه SDN ارتباط برقرار کند. هدایتگر IoT تصمیمات لازم را بر اساس داده‌های ارائه‌شده توسط عامل‌های IOT انجام خواهد داد، پس ابتدا بررسی می‌کند که این شیء در لیست سیاه نباشد. (فرض این‌است که لیست سیاه در ابتدا خالی است). سپس تصمیم‌گیری می‌شود و فرامین به هدایتگر SDN ارسال می‌شود، حال این تصمیمات از طریق هدایتگر SDN به زیر شبکه فیزیکی منعکس می‌شود. همچنین لازم به ذکر است هدایتگر IoT هنگام دریافت درخواست اتصال از عامل IoT، قوانین پیش‌بری بسته را بر اساس پروتکل‌های شبکه استفاده می‌کند و این قوانین را به هدایتگر SDN تحویل می‌دهد. پس هنگامی‌که هدایتگر IoT آدرس یا شناسه شیء مقصد را دریافت می‌کند، باید آن را در شبکه پیدا کند. هدایتگر SDN نقشه راه شبکه را ایجاد می‌کند یعنی هر دو شیء را با استفاده از الگوریتم مسیریابی با اطلاعات توپولوژی از سطوح IoT و SDN متصل می‌کند. حال همان‌گونه که در ابتدای بخش ۴ گفتیم هدایتگر قابلیت نظارت، تحلیل و تحلیل الگوهای ترافیکی را برای تهدیدهای امنیتی بالقوه دارد، پس با بررسی این موضوع اتصالات ناامن و تهدیدآمیز را به‌سرعت قطع کرده و شیء موردنظر را به لیست سیاه اضافه می‌کند و سپس اطلاعات را به‌روزرسانی می‌کند.

در کل این موضوع را نیز باید در نظر بگیریم که هنگام استفاده از SDN در خدمات و برنامه‌های کاربردی IoT، باید امنیت را در تمام بخش‌ها بهبود بخشید؛ زیرا هر دستگاه یا برنامه کاربردی می‌تواند الزامات امنیتی خاص خود را داشته باشد و سطح متفاوتی از امنیت را طلب کند. بنابراین SDN لزوماً باعث افزایش امنیت نمی‌شود، این بستگی به وضعیت امنیتی هر کاربر نیز دارد. بااین‌حال، با استفاده از قابلیت‌های SDN مشخصاً وضعیت امنیتی IoT می‌تواند بهبود یابد.

۵- نتیجه‌گیری

IoT با وجود تمام مزایایی که دارد، هنوز چالش ها و مشکلاتی نیز دارد که برقراری امنیت و حفظ حریم خصوصی شاید بزرگ‌ترین آن‌ها باشد. SDN با دارا بودن قابلیت مسیریابی هوشمند ترافیک و استفاده از منابع بلااستفاده در شبکه، آمادگی شبکه برای یورش داده‌های دستگاه‌های متصل به IoT را بسیار بیشتر می‌کند.

SDN می‌تواند سیاست‌ها و کنترل دسترسی را تسهیل کرده و امکان احراز هویت از طریق مدیریت مرکزی را فراهم کند. در واقع قابلیت‌های SDN در مهندسی ترافیک می‌تواند به جداسازی یا توقف مسیرهای حمله یا رخنه‌های امنیتی در شبکه کمک نماید. درنتیجه یک هدایتگر SDN که مدیریت مرکزی داشته باشد، می‌تواند آمار خوبی از محل وقوع حملات ارائه دهد و با انجام اقدامات مناسبی ازجمله اضافه کردن عوامل تهدیدآمیز به لیست سیاه و تجزیه و تحلیل آن‌ها و سپس ارسال این اطلاعات به هدایتگر IoT راه را بر آن‌ها بسته و اجازه حملات بعدی را نیز

از آن‌ها سلب نماید و با این تدابیر امنیت و حفظ حریم خصوصی را در IoT توسعه، افزایش و ارتقا دهد.

۶- مراجع

[1] European Commission, "Internet of Things factsheet Privacy and Security," January 2019. Available on: http://ec.europa.eu/information_society [Accessed:]

[2] Zarpelao, B. Bruno, S. M. Rodrigo, T. K. Cláudio, and C. de A. Sean, "A survey of intrusion detection in Internet of Things," Journal of Network and Computer Applications, vol. 84, pp. 25-37, 2017.

[3] T. Itu, "Series y: Global information infrastructure," Internet protocol aspects and next-generation networks, Next Generation Networks - Frameworks and functionalarchitecture models,

[4] International Telecommunication Union, Overview of the Internet of things, Rec. ITU-T Y.2060, January 2019. Available on: https://www.itu.int

[5] M. U. Farooq, W. Muhammad, K. Anjum, and M. Sadia, "A critical analysis on the security concerns of internet of things (IoT)," International Journal of Computer Applications, vol. 111, no. 7, 2015.

[6] A. K. Sikder, P. Giuseppe, A. Hidayet, J. Trent, and A. Selcuk Uluagac, "A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications," arXiv preprint, arXiv:1802.02041, 2018.

[7] N. A. Bruno, M. Marc, N. N. Xuan, O. Katia, and T. Thierry, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," IEEE Communications Surveys and Tutorials, vol. 16, no. 3, pp. 1617-1634, 2014.

[8] J. Li, A. Eitan, and T. Corinne, "A general SDN-based IoT framework with NVF implementation" ZTE communications, vol. 13, no. 4, pp. 42-45, 2015.

[9] Y. Jarraya, M. Taous, and D. Mourad, "A Survey and a Layered Taxonomy of Software-Defined Networking," IEEE Communications Surveys and Tutorials, vol. 16, no. 4, pp. 1955-1980, 2014.

[10] O. Flauzac, C. Gonzalez, and F. Nolot, "New security architecture for IoT network" Procedia Computer Science, vol. 52, pp. 1028-1033, 2015.

[11] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "SDN based architecture for IoT and improvement of the security," In Advanced Information Networking and Applications Workshops (WAINA), IEEE 29th International Conference on, IEEE, pp. 688-693, 2015.

[12] Y. Qiao, F. Richard Yu, G. Qingxiang, and L. Jianqiang, "Software-defined networking (SDN) and distributed denial of service attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602-622, 2016.

Journal of "Innovations of Applied Information and Communication Technologies"
Vol. 1, No. 2, 2019 (Serial No. 2)

Use of Software Defined Networks to Enhance the Security of the Internet of Things

R. Roozbehi, M. Ghasemzadeh*
Potsdam university, Yazd university

Abstract

Promoting security and maintaining privacy policies is one of the most important demands in all areas, including the Internet and its specific aspects, such as the Internet of Things (IoT). To achieve this, several solutions have been proposed. In this article, we show how to get valuable results on the Internet using software defined networks (SDN). In this regard, I will first review the concepts of IoT and SDN, and then we'll come up with a way to integrate the IoT and SDN so that we can quickly identify and discontinue threatening attacks and unsecured connections. Meanwhile, we put such an attacker on a blacklist so that they will not be allowed to connect in the future. To evaluate the operation of the proposed method, we need several objects connected to the Internet of objects and an active software network. Theoretical analysis suggests that the impact of this approach on network readiness against attacking the data of devices connected to the Internet of objects and overcoming DDoS attacks is very significant.

Keywords: Internet of Things, Software Defined Network, Security, IoT, SDN

* Corresponding author E-mail: m.ghasemzadeh@yazd.ac.ir