بسمه‌تعالی

گزارش و تحلیل مقاله

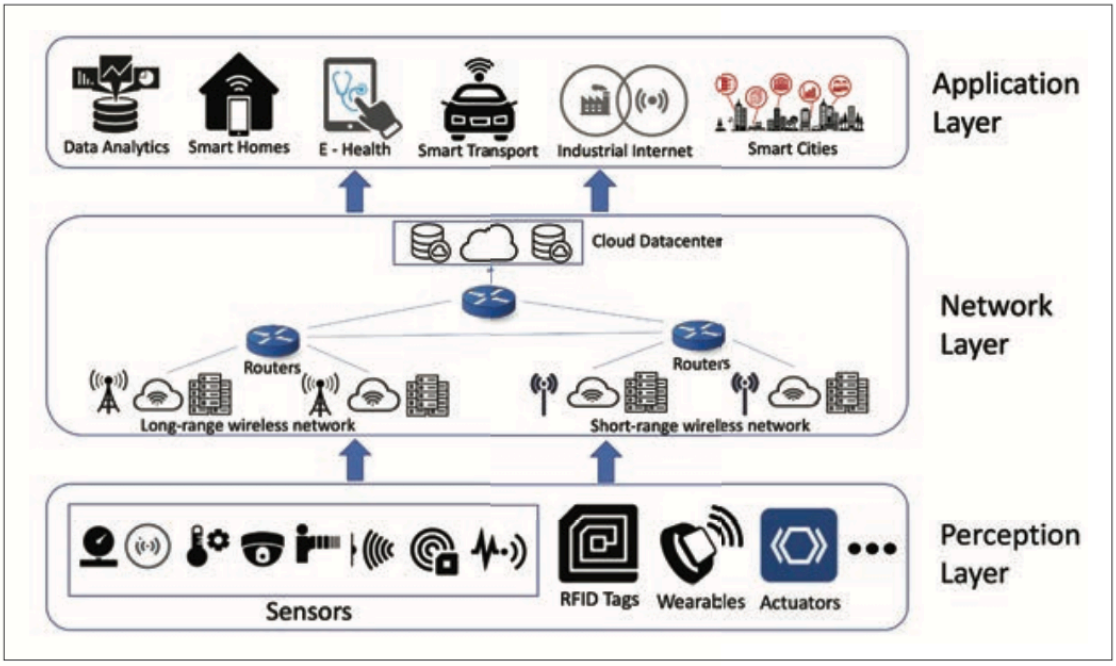
Software Defined Internet of Things Security- Properties, State of the Art, and Future Research

تعریف مسئله و هدف اصلی مقاله

از یک گوشی هوشمند تا شهر هوشمند، اینترنت اشیا به مرور جز لاینفکی از زندگی نوین شده است که کاربردهای آن سالانه چندین برابر می‌شود. منابع محدود و ماهیت ناهمگن دستگاه‌های اینترنت اشیا، کنترل امنیت را برای مدیران شبکه و امنیت کاری دشوار ساخته است. رمزنگاری صرف و آنتی‌ویروس‌ها به تنهایی از پس چالش‌های امنیتی این حوزه برنمی‌آیند.

در طول زمان مقالات زیادی در راستای چالش‌های امنیتی این حوزه ارائه شده‌اند. اما امروزه، شبکه‌های نرم‌افزارمحور (SDN) با ارائه روش‌های واضح و فراگیر، مورد توجه ویژه در خصوص رفع مشکلات امنیتی سنتی این حوزه قرار گرفته‌اند.

شبکه‌های نرم‌افزارمحور با تفکیک Control plane و Data plane، مدیریت جامعی بر شبکه را ایجاد می‌کند. این تفکیک و وجود یک کنترلر مرکزی جهت مدیریت جامع شبکه، راه‌کارهایی کارا، امن و پایدار در مقابله با چالش‌های امنیتی اینترنت اشیا، ارائه می‌کند. در این مقاله به چالش‌های موجود در این حوزه و راه‌حل‌های آن بر اساس شبکه‌های نرم‌افزارمحور پرداخته می‌شود.

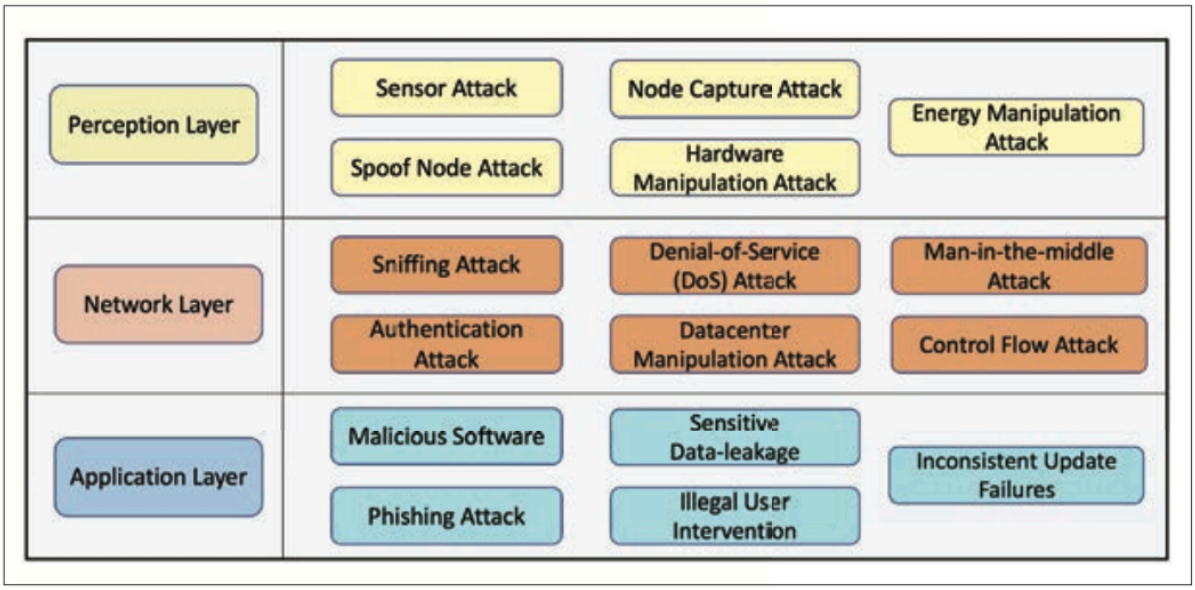


تصویر- ۱

دامنه کاربردهای اینترنت اشیا، محبوبیت و استقبال زیادی پیدا کرده است. بنابراین ایجاد امنیت در برابر حملات و تهدیدات خصمانه، بسیار مهم است. در ادامه در سه بخش:

- ساختار چارچوب اینترنت اشیا (تصویر- ۱)
- دسته‌بندی تهدیدات رایج در حوزه اینترنت اشیا بر اساس لایه تحت تاثیر (تصویر- ۲)
- فهم رابطه بین ذات هر لایه و تهدیدات مربوط به آن

موضوعات بررسی می‌شوند.



تصویر- ۲

لایه Perception

همان‌طور که از نام این لایه مشخص است، لایه ادراک، مسئول درک فیزیک طبیعی اشیا در محدوده پیاده‌سازی اینترنت اشیا و جمع‌آوری اطلاعات در مورد آن است. این فرآیند شامل درگیری سنسورها و فعال‌کننده‌ها[1]، RFID، تجهیزات هوشمند قابل پوشیدن و...، است. این لایه، سطح[2] جمع‌آوری اطلاعات است و به همین دلیل همیشه منبع جذابی برای حملات جهت دستیابی به اطلاعات حساس و ایجاد اختلال در سرویس‌های شبکه است. در ادامه به حملات این لایه می‌پردازیم.

Sensor Attack

بر اساس ساختار سنتی اینترنت اشیا، هر سنسور منطق کنترلی خود را دارد و قوانین جریان خود را برقرار می‌کند. این روند مطلوب است چون‌که حتی سنسورها در صورت عدم نظارت، بازهم کار می‌کنند. در این شرایط، مهاجمان می‌توانند اطلاعات شبکه را ضبط و دستکاری کنند. بنابراین حسگرهای متخاصم می‌توانند، اطلاعات نادرست ارائه کرده، بر دیگر دستگاه‌ها تاثیر بگذارند و به عنوان گره قابل اعتماد، فعالیت کنند.

[1] Actuator

[2] Plane

Node Capture Attack

بر اساس مکانیزم اجرای از راه‌دور یک گره از اینترنت اشیا که نیازمند مداخله و نظارت نیست، می‌توان با اعمال یک عمل فیزیکی یا الکترونیکی، گره فیزیکی را دستکاری کرد. دسترسی فیزیکی به دستگاه باعث کسب کنترل کامل فیزیکی آن توسط مهاجم و خرابی دستگاه می‌شود. این نوع حمله در صورت نادیده گرفته شدن، منجر به گسستگی کل پیاده‌سازی می‌شود.

Spoof-Node Attack

هر گره از اینترنت اشیا قوانین جریان خود را دارد، بر همین اساس یک مهاجم مخرب می‌تواند با تکرار مشخصات خاص یک گره واقعی، یک گره متخاصم ایجاد کند. این گره جعلی و متخاصم می‌تواند مجاز شناخته شود و منجر به آسیب‌پذیری شدید شبکه مثل اجازه دسترسی، استخراج کلیدهای امنیتی، ارائه اطلاعات بازخوردی نادرست و حذف گره مجاز شود.

Hardware Manipulation Attack

سخت‌افزار و نرم‌افزار اینترنت اشیا ارتباط تنگاتنگی دارد. نرم‌افزارهای مخربی مانند ویروس‌ها، کرم‌ها، تروجان‌ها و نرم‌افزارهای جاسوسی، باعث تغییر رفتار سخت‌افزار می‌شود و اطلاعات سنسور در دسترس مهاجم قرار می‌گیرد.

هر دستگاه اینترنت اشیا دارای نرم‌افزار اختصاصی است که ردیابی کدهای مخرب تزریق شده در زمان ساخت یا طراحی که باعث فعال‌شدن بدافزارها می‌شود را دشوار می‌کند.

Energy Manipulation Attack

بسیاری از حسگرها و فعال‌کننده‌ها با استفاده از باتری و منبع ثابت انرژی، کار می‌کنند. مهاجم با تخلیه منبع انرژی می‌تواند دستگاه را از کار بیندازد. گره‌های اینترنت اشیا با بهینه‌سازی چرخه فعالیت، عمر منبع انرژی را بیشتر می‌کنند. مهاجم با دستکاری در گره آسیب دیده، برنامه عادی خواب گره را خراب کرده و گره را تا زمان اتمام منابع روشن نگه می‌دارد. با استفاده از تعداد زیادی بسته‌های بی‌اهمیت و اجبار به پردازش آن‌ها توسط گره، منابع را سریعا به اتمام می‌رساند.

لایه Network

لایه شبکه اطلاعات ارسالی از لایه Perception را به لایه Application جهت آنالیز و مصرف، می‌رساند. حمله به این لایه موجب از کار افتادن کل سامانه می‌شود. در ادامه نقاط ضعف و حملات مربوط به این لایه را بررسی می‌کنیم.

Sniffing Attack

شنود با دستیابی به اطلاعات خصوصی بین دستگاه‌ها و کنترلر انجام می‌شود. با عدم وجود یک شیوه رمزگذاری، هر ارتباطی قابل شنود است. برای جلوگیری از این نوع حمله باید نقاط متعدد مناسب برای شنود را با رمزگذاری، ایمن ساخت.

Authentication Attack

بیشتر پروتکل‌های موجود در شبکه اینترنت اشیا از احراز هویت متقابل جهت حفظ حریم خصوصی و یکپارچگی، بین چندین دستگاه بهره می‌برند. در این شرایط مهاجمین با تخریب یکی از دستگاه‌های احراز هویت، به شبکه و منابع آن دسترسی پیدا می‌کنند. این نوع دسترسی راه را برای حملات دیگری نظیر Man-in-the-Middle و جعل هویت، باز می‌کند.

Denial of Service Attack

یکی از حملات رایج، حمله DOS است که با دستیابی به لینک‌های ارتباطی و ایجاد سیلی از داده‌های عظیم، منابع شبکه را هدر داده و شبکه را از دسترس خارج می‌کند. از آنجایی که بیشتر تجهیزات از ارتباطات بی‌سیم استفاده می‌کنند، این حملات باعث قطع ارتباط و تخریبات جدی می‌شود. با ایجاد شبکه بزرگی از Botها می‌توان حملات DDOS را برای استفاده بهتر از آسیب‌پذیری‌ها، صورت داد.

Datacenter Manipulation Attack

امروزه شبکه‌های اینترنت اشیا از راه‌کارهای ابری استفاده می‌کنند. در صورت دستکاری دیتاسنتر ابری توسط مهاجم، کنترل تجهیزات اینترنت اشیا به دست مهاجم خواهد افتاد. این هجوم باعث نشت اطلاعات، عدم سازگاری داده‌ها، وقفه‌های عمدی در جمع‌آوری اطلاعات و یکپارچگی داده‌ها شود.

Man-in-the-Middle Attack

با سو استفاده از تایید هویت در شبکه، هر دو دستگاه موجود در یک ارتباط، جعل شده و مهاجم ترافیک را قطع کرده و پیام جعلی ارسال می‌کند. هر دو طرف ارتباط با فریب خوردن، گره جعلی را معتبر دیده و اطلاعات حساسی مانند کلیدهای امنیتی، داده‌های شخصی مشتریان، جریان کنترل شبکه و... به مهاجم درز می‌کند.

Control Flow Attack

هر دستگاه و کنترلر مرتبط با آن به صورت سنتی جریان کنترلی خود را دارند و بر همین اساس مهاجم با بمباران شبکه توسط بسته‌های جعلی، عملکرد شبکه را کاهش می‌دهند.

لایه Application

این لایه به دلیل ارتباط با مصرف‌کنندگان، محبوبیت زیادی دارد. همه برنامه‌های معروف مانند خانه هوشمند، حمل و نقل هوشمند و سلامت الکترونیکی در این لایه تعریف می‌شوند.

ماهیت آسیب‌پذیری‌های این لایه با دیگر لایه‌ها به دلیل حساسیت اطلاعات، متفاوت است. حملات این لایه ممکن است سامانه را از کار نیندازند ولی افشای اطلاعات عواقب ناگواری دارد. در ادامه، حملات این لایه را بررسی می‌کنیم.

Malicious Software

برنامه‌های اینترنت اشیا، در صورت عدم وجود وصله‌های امنیتی به روز شده، در معرض بدافزارها، ویروس‌ها و کرم‌ها هستند. نرم‌افزار مخرب موجب نشت داده‌ها و مشکلات یکپارچی داده می‌شود. کرم‌هایی با توانایی انتشار می‌توانند اجزای دیگر شبکه را به خطر بیندازند.

Phishing Attack

مهاجم با استفاده از ایمیل‌های سودآور و تبلیغات دروغین که حاوی بدافزارها هستند، این حمله را ترتیب می‌دهد. در صورت استفاده برنامه اینترنت اشیا از این رسانه ارتباطی، مهاجم با فیشینگ، اطلاعات حساس کاربر مانند گواهی‌ها و مجوزهای دسترسی را به دست آورد و دیگر تجهیزات را کنترل کند.

Sensitive Data Leakage

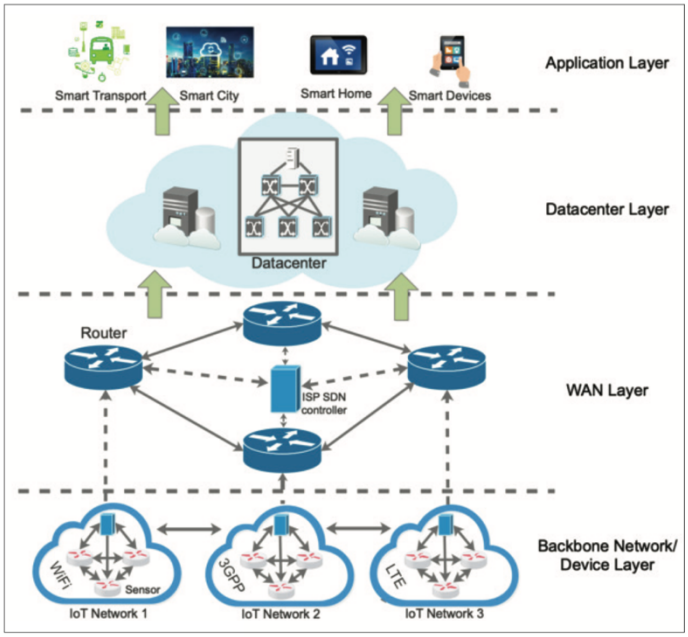
در عصر حریم خصوصی، داده‌ها قدرتمندترین دارای هستند که باید به صورت جدی از نشت آن‌ها جلوگیری شود. دسترسی به زمینه‌های[3] عملیاتی یک برنامه علاوه بر حمله به آن برنامه خاص، اطلاعات درون آن را مورد استنتاج، قرار می‌دهد. حتی یک لغزش جزیی می‌تواند عواقب فاجعه‌باری برای کاربران در پی داشته باشد.

Illegal User Intervention

برنامه‌های اینترنت اشیا اغلب توسط چندین کاربر مورد استفاده قرار گرفته و اطلاعات آن نیز توسط یک شبکه ارائه می‌شود. اگر یک مهاجم بتواند اطلاعات هویتی یک کاربر را جعل کند، با درک زمینه‌های برنامه کاربر و مهندسی معکوس، می‌تواند به اطلاعات کاربران واقعی دست پیدا کند. در این شرایط مهاجم می‌تواند با ایجاد تعاملات جعلی با برنامه در شبکه، حمله DDOS را ترتیب دهد.

Incompatible Update Failures

هر دستگاه اینترنت اشیا نسخه نرم‌افزار مخصوص خود را دارد که به‌روزرسانی تمامی گره‌ها کاری بسیار دشوار است. به صورت ویژه هنگام نیاز به وصله امنیتی فوری برای هر نسخه نرم‌افزار جهت جلوگیری از آسیب‌پذیری‌ها، این امر بسیار مهم می‌شود. در صورت به‌روزرسانی متناقض، نسخه‌های ناسازگار، آسیب‌پذیری‌ها را در اختیار مهاجم قرار می‌دهد.

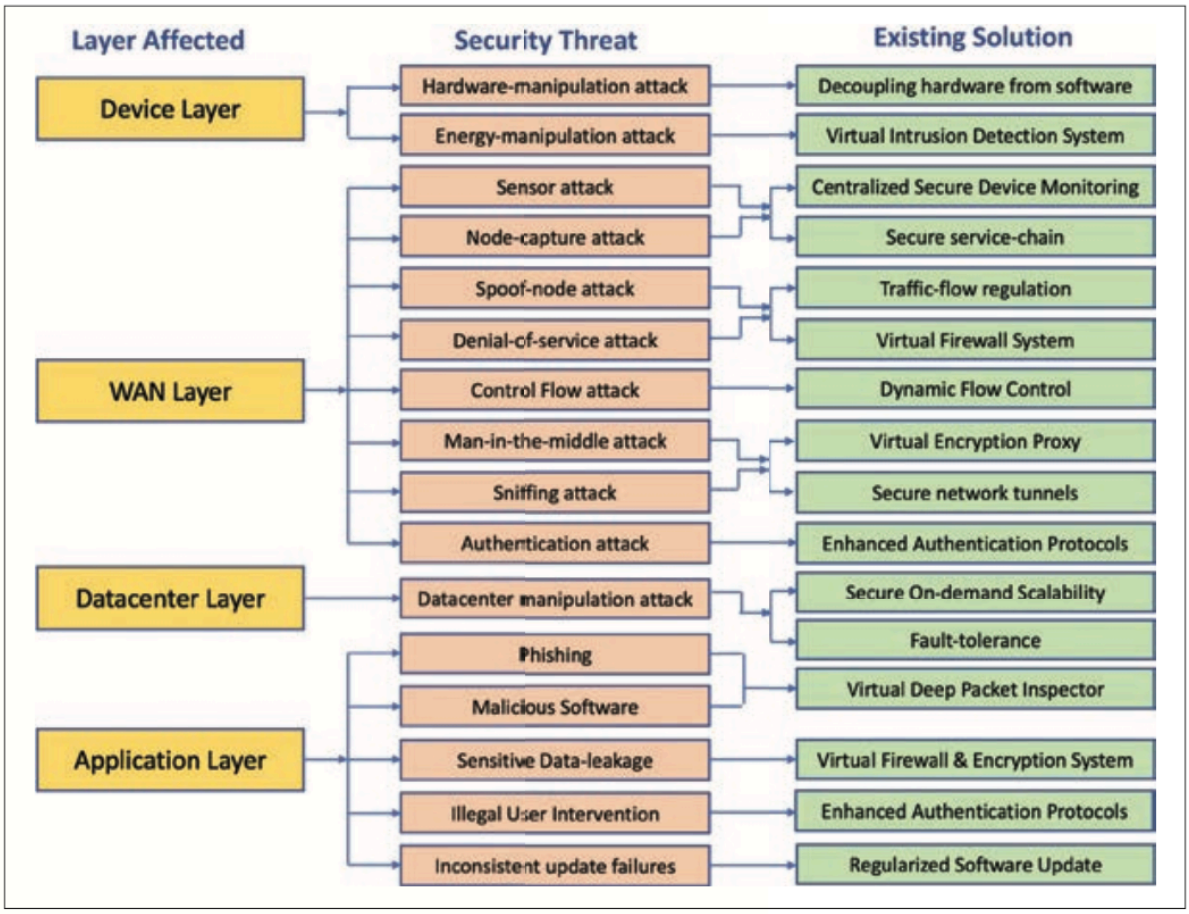


تصویر- ۳

[3] Context

راه‌حل پیشنهادی مقاله برای مسئله

در این بخش می‌خواهیم به ویژگی‌هایی از SDN-IOT بپردازیم که به نحو مطلوبی از تهدیدات جلوگیری می‌کنند و راه‌حل‌های پیشنهادی را در خود دارد. در تصویر- ۳ ویژگی‌های اصلی این چارچوب را نمایش می‌دهد. در ادامه تمرکز بر لایه‌های مختلف SDN-IOT و شیوه مقابله با حملات، خواهد بود. در تصویر- ۴ طبقه‌بندی و ساختار مقابله با تهدیدات مشاهده می‌شود.



تصویر- ۴

لایه Device

لایه دستگاه پایین‌ترین لایه از معماری SDN-IOT است. ماهیت آن مشابه لایه درک معماری اینترنت اشیا است. تفاوت اصلی در این است که هیچ جریان انفرادی یا مکانیزم نظارتی برای دستگاه وجود ندارد. بلکه همه دستگاه‌ها به صورت متمرکز کنترل می‌شوند و قوانین جریان از طریق کنترل‌کننده‌های متمرکز بین دستگاه‌ها توزیع می‌شود.

در این ساختار، چندین شبکه دستگاه وجود دارد که هر شبکه دستگاه دارای چندین نقطه ادغام مانند مسیریاب‌ها، دروازه‌ها و یک کنترل‌کننده متمرکز برای آن شبکه دستگاه خاص است. این کنترل‌کننده‌ها، اطلاعات را به روترهای موجود در لایه WAN منتقل می کنند. در این بخش بیشتر مزایای امنیتی اصلاح معماری اینترنت اشیا سنتی را بررسی می‌کنیم.

Decoupling Hardware from Software

یکی از مزایای SDN-IOT حذف وابستگی سخت‌افزار به یک نرم‌افزار خاص است. شبکه نرم‌افزارمحور یک نسخه از نرم‌افزار را جهت اعمال در تمامی کنترلرهای مجازی که وظیفه مدیریت جریان ترافیک را به یکایک دستگاه‌های سخت‌افزاری برعهده دارند، حفظ می‌کند. بنابراین سخت‌افزار از حملات دستکاری محافظت شده و با دریافت به‌روزرسانی‌های منظم و متمرکز، با تهدیدات کمتری روبرو می‌شود.

Virtual Intrusion Detection System

سیستم تشخیص نفوذ مجازی (vIDS) از امضاهای از پیش تعریف شده یا الگوهای حمله و گزارشات وقایع برای تعیین ترافیک غیر عادی در یک شبکه استفاده می‌کند. این حملات معمولا در اثر حمله دستکاری انرژی ایجاد می‌شود. از vIDS می‌توان برای شناسایی فعالیت‌های خصمانه مثل مصرف زیاد پهنای باند، طغیان بسته‌های بی اهمیت، حملات DOS و... استفاده کرد. vIDS برای شناسایی چنین حملاتی به دلیل اجرا در کنترلر متمرکز شبکه، برتری دارد.

لایه WAN

این لایه به عنوان لایه اینترنت در ساختار در نظر گرفته می‌شود. تجهیزاتی مانند مسیریاب‌ها و دروازه‌ها در data plane، با استفاده از کنترلر مرکزی نرم‌افزارمحور ISP به عنوان control plane، مدیریت می‌شوند. در مدیریت متمرکز و مرکزی data plane، مزایای بسیاری برای جلوگیری از آسیب‌پذیری‌های امنیتی وجود دارد.

Centralized Secure Device Monitoring

به دلیل طراحی متمرکز و مرکزی کنترلر در SDN-IOT، نظارت موثرتری بر data plane انجام می‌شود. با استفاده از درخواست‌های آماری دوره‌ای و بررسی سلامت، اطلاعات وضعیت کل شبکه جمع‌آوری می‌شود. بر این اساس کنترلر همیشه اطلاعات به روز از شبکه تجهیزات دارد که می‌تواند بر اساس آن جریان ترافیک را تغییر دهد. این روش علاوه بر تشخیص گره‌های خاص و یا گره‌های جعلی، در استراتژی‌های کاهشی ضمن حملات، کاربرد دارد. در پاسخ به حملات، قوانین جریان اصلاح شده به سهولت در گره مورد نظر اعمال می‌شوند.

Secure Service Chain

زنجیره سرویس شبکه، که به عنوان زنجیره تابع سرویس شبکه هم مطرح می‌شود، یک زنجیره امن و به هم پیوسته از سرویس‌های شبکه را در یک زنجیره مجازی، ایجاد می‌کند. سرویس‌های شبکه مثل دیواره‌های آتش، محافظ نفوذ، NAT و.. امنیت زیربنایی دستگاه‌ها را فراهم می‌کند و مدیران مجموعه را قادر می‌سازد تا مجموعه خدمات امنیتی را در قالب یک اتصال واحد به شبکه، تنظیم کنند. این ارتباط مجازی شبکه به صورت خودکار قادر به کنترل همه سرویس‌های متصل است.

Traffic Flow Regulation

در حملات DOS که کنترلر با بمباران توسط بسته‌های زائد جهت از کار افتادن سامانه، روبرو است، محدود کردن نرخ کانال کنترل می‌تواند باعث مقاومت سامانه در مقابل سیلی از درخواست‌ها شود. تنظیم ترافیک بسته‌ها را بر اساس اولویت و QOS حذف کند. هم‌چنین راه‌کارهای مبتنی بر QOS و حرکات، برای رسیدگی به چالش‌های جریان ترافیک، ارائه شده‌اند.

Virtual Firewall System

دیواره آتش مجازی در SDN-IoT یک سرویس جهت فیلتر کردن ترافیک شبکه برای موارد مجازی که به نمایندگی از تجهیزات شبکه هستند، می‌باشد. بسته‌های جریان را بازرسی می‌کند و با سیاست‌های امنیتی از پیش تعریف شده از ارتباط ناخواسته ناشی از حملاتی مانند حمله DoS، جلوگیری می‌کند. دیواره آتش مجازی بسیار انعطاف پذیر است و می تواند براساس تغییرات سیاست‌های شبکه‌های مجازی اصلاح شوند.

Dynamic Flow Control

یکی از ویژگی‌های اساسی چارچوب SDN، توانایی کنترلر در تغییر پویا قوانین جریان و انتشار به‌روزرسانی‌های یکپارچه در دستگاه‌های سراسر شبکه است. با استفاده از این قابلیت مدیریتی، راه حل‌های دفاعی می‌توانند با ویژگی‌هایی مانند بازتابنده‌های شبکه[۴] و قرنطینه پویا به مبارزه با جریان بسته خصمانه در شبکه بپردازند. همچنین این ویژگی به ایجاد شبکه‌ای با امتیازات[۵] خاص و سیاست‌های یکسان کمک می‌کند.

Virtual Encryption Proxy

یک پروکسی رمزگذاری مجازی با سیستم‌های رمزنگاری متقارن و نامتقارن برای محافظت از شبکه در برابر حملات استشمام[۶] و شنود استفاده می‌کند. پروکسی به عنوان یک واسطه بین دو ابزار ارتباطی عمل می‌کند و به جلوگیری از حملاتی مانند Man-in-the-Middle کمک می‌کند، زیرا پروکسی تنها موجودیتی است که تعیین مقصد را برای هر دو گره انجام می دهد.

Secure Network Tunnels

تونل‌های شبکه ایمن امکان ارتباط بسته‌های داده را به صورت رمزگذاری شده برای جلوگیری از حملات شنود فراهم می‌کنند. ترافیک شبکه را می توان از طریق vProxy با استفاده از تونل‌های داده ایمن تغییر مسیر داد تا انتقال داده ایمن را تسهیل کند و از حملات Man-in-the-Middle جلوگیری کند. هم‌چنین می توان از تونل‌های شبکه امن برای هدایت ترافیک از طریق سایر مکانیسم های امنیتی (vIDS، vFirewall و...) برای جلوگیری از سایر اشکال حملات استفاده کرد.

---

[4] Network reflector

[5] Privileges

[6] Eavesdropping

Enhanced Authentication Protocols

پروتکل‌های احراز هویت پیشرفته مانند احراز هویت دو طرفه، مجوز مبتنی بر نقش برای هر دستگاه و احراز هویت چند لایه، می‌توانند در یک لایه متمرکز کنترلر اجرا شوند و در دستگاه‌ها توزیع شوند. از چارچوب احراز هویت، مجوز و حسابداری مجازی (vAAA) می‌توان برای طراحی پروتکل‌های امنیتی هوشمند برای نمونه‌های مجازی درگاه‌های اینترنت اشیا استفاده کرد.

لایه Datacenter

لایه مرکز داده را می‌توان لایه ماندگاری خدمات کاربردی دانست. با ظهور و محبوبیت راه حل‌های مبتنی بر ابر، معماری SDN-IOT ذخیره‌سازی داده‌های جمع آوری شده و پردازش شده توسط دستگاه و لایه‌های WAN را در مراکز داده ارائه شده توسط ابر برای تجزیه و تحلیل بیشتر توسط برنامه‌های کاربردی لایه Application حفظ می‌کند.

Secure On-Demand Scalability

با بهره‌گیری از مفهوم مدیریت چرخه زندگی پویا منابع شبکه مجازی در چارچوب SDN-IOT، مدیران شبکه می‌توانند راه حل‌های امن بسیار مقیاس پذیر را که باعث بهینه‌سازی منابع کارآمد می‌شوند را تسهیل کنند. توابع شبکه مجازی (VNF) را می‌توان در مراکز داده ابری پیاده سازی کرد که با توجه به حجم درخواست‌های ورودی، می توانند به صورت خودکار مقیاس‌بندی شوند. ویژگی مقیاس‌پذیری راه حل‌های امنیتی، احتمال کاهش عملکرد در حین تجزیه و تحلیل شبکه را کاهش می‌دهد و تشخیص تهدید بهینه را صرف نظر از بار شبکه، تضمین می‌کند.

Fault Tolerance

پیاده‌سازی ابرها به دلیل خرابی‌های ذاتی و یا حملات خصمانه، مستعد از کار افتادن هستند. تحمل‌پذیری اشکال، بار را در گره‌های دیگر توزیع می‌کند و دسترسی به سرویس را در همیشه تضمین می‌کند. بنابراین شبکه SDN-IOT را قادر می‌سازد در برابر خرابی‌های ناخواسته و حملات هوشمندانه ایمن شود. با افزونگی نمونه کنترلرهای مجازی و گره‌ها، مقابله با اشکالات انجام می‌شود.

لایه Application

این لایه در دسترس کاربران قراردارد و با لایه Application در اینترنت اشیا تفاوت چندانی ندارد ولی نیاز است راه‌کارهای امنیتی در مقابله با حملات خصمانه تقویت و ارائه شوند.

Virtual Deep Packet Inspector

بازرسی عمیق بسته‌ها، یکی از قوی‌ترین بازیگران در امنیت لایه Application است و پتانسیل بسیار خوبی برای مقابله با حملات وب و برنامه‌های مدرن دارد. این بازرسی شامل فیلتر کردن بسته‌های شبکه است با بررسی بخش داده‌های یک بسته است و هرگونه هرزنامه، ویروس و انواع نفوذها را تشخیص می‌دهد. بر اساس تعاریف قانون سامانه، بسته را می‌توان ارسال، مسدود یا برچسب گذاری کرد. بازرس سبک و کارا می‌تواند برای کشف ناهنجاری‌ها در لایه هفتم شبکه (OSI) پیاده شود.

Firewall and Encryption System

دیواره آتش برنامه، ورودی، خروجی و دسترسی به یک برنامه یا سرویس را کنترل می‌کند. نه تنها از حملات یک برنامه خصمانه به برنامه‌های والد خود جلوگیری می‌کند، بلکه والدین را از دسترسی به برنامه‌هایی که ممکن است به یک‌پارچگی سیستم آسیب برساند، محافظت می‌کند. افزون بر این، سیستم رمزگذاری تضمین می‌کند که داده‌ها، در هنگام ذخیره سازی یا در حین ارتباط، به راحتی قابل رمزگشایی نباشند.

Enhanced Authentication Protocols

احراز هویت کاربران برنامه باید با استفاده از پروتکل‌های احراز هویت پیشرفته از بیومتریک، آدرس MAC، رمزهای مبتنی بر تایمر و... انجام شود. مجوز مبتنی بر نقش اطمینان می‌دهد که همه موجودیت‌ها نمی‌توانند به داده‌ها دسترسی داشته باشند و هیچ یک از واحدها هم نمی‌توانند به تمام بخش‌های داده دسترسی داشته باشند. این نوع احراز هویت و مجوز برای پیش‌بینی و جلوگیری از تهدیدات مدرن باید مرتبا به روز شود.

Regular Software Update

نگهداری یک نسخه واحد از نرم‌افزار در یک مکان متمرکز باعث به‌روزرسانی منظم و انتشار آن در کل شبکه می‌شود. این روش از مخاطرات به‌روزرسانی پیگیری می‌کند.

جمع‌بندی و پیشنهادات برای کارهای آتی

چارچوب SDN-IOT بسیاری از مشکلات امنیتی را حل کرده و سامانه را پایدار می‌سازد ولی چالش‌های بازی هستند که نیازمند بررسی هستند. در ادامه به برخی از این چالش‌ها اشاره می‌کنیم (تصویر- ۵).

Single Point of Failure

وجود یک کنترلر مرکزی که از مهم‌ترین ویژگی‌های معماری SDN است، که خود می‌تواند به عنوان SPOF مخاطره ایجاد کند. هنگامی که بر اثر حمله، کنترلر با شکست روبرو شود، روش‌های مانند IDS دیگر کاربرد خود را در خنثی‌سازی حملات از دست می‌دهند. استفاده از چندین کنترلر مانند راه‌کار TinySDN، برای مقابله با این چالش بررسی شده‌اند.

روش‌هایی مانند تکثر کنترلرها و سیاست‌های کنترل کننده پیشنهاد شده‌اند که سعی در غلبه بر این چالش دارند. به دلیل ماهیت ساختاری این مسئله هنوز راه‌کار جامع و کاملی برای حل این چالش ارائه نشده است.

Critical issue	Layers affected	Existing solutions
Single point of failure	✓ Device layer ✓ WAN layer	• Multiple controllers • Replication strategies • Clean-slate recovery • Controller access restriction
Data confidentiality issues	✓ WAN layer ✓ Data center layer ✓ Application layer	• Rigid authentication mechanism • Systematic trust model • Autonomous trust management • Sandboxing techniques
Troubleshooting and speed recovery	✓ WAN layer ✓ Data center layer	• Reliable system snapshots • Immutable logs
Orchestration issues	✓ WAN layer ✓ Device layer	• FRESCO • OrchSec
Denial of service attacks	✓ WAN layer ✓ Device layer	• Rate-limiting of control channel • Event filtering • Traffic prioritization • Timeout adjustment • Localized central control
Man-in-the-middle attacks	✓ WAN layer ✓ Device layer	• Bloomfilter • Dynamic device association • Increase in data-plane programmability
Policy definition issues	✓ WAN layer	• HiPoLDS • HLP/MLP language protocols

تصویر- ۵

Data Confidentiality Issues

فقدان شیوه رمزگذاری کارآمد بین سوییچ‌ها و کنترلر SDN، می‌تواند به نقض محرمانگی اطلاعات شود. برای مبارزه با این دسته از حملات استفاده از شیوه‌های احراز هویت صلب و مدل‌های اعتماد سیستماتیک، می‌تواند راهگشا باشد. تکنیک Sandboxing اجازه می‌دهد عملیات محدود و تجهیزات محفوظ از خطا غیر قابل نفوذ، اطلاعات حساس را ذخیره کنند. این تکنیک به عنوان یک رویکرد باید در طراحی‌ها در نظر گرفته شود. هم‌چنین، شیوه مدیریت اعتماد مستقل بین برنامه‌ها نیز باید طراحی و پیاده‌سازی شود.

Fast Secure Mode Recovery

بازیابی سریع و قابل اعتماد با کمترین میزان از دست رفتن اطلاعات، نیاز به یک تصویر[۷] ایمن و قابل اعتماد از سیستم و یک مکانیزم بازیابی لحظه ای دارد تا شبکه را به حالت قبلی خود برگرداند. شیوه‌های تضمین

[7] Snapshot

کننده چنین رویه ای در حال حاضر موجود نیستند. از طرف دیگر، برای بررسی و ایجاد اطلاعات مربوط به حمله یا عدم موفقیت، باید اطلاعات موثق را از تمام اجزای سیستم بازیابی کرد. این داده ها فقط در صورت قابل اعتماد بودن، صحت و اعتبار، قابل استفاده هستند. شیوه‌های لاگ‌برداری غیرقابل تغییر، که تضمین می‌کنند که لاگ پاک نشده و دستکاری نشود، چالش برانگیز هستند.

Orchestration Issues

اینترنت اشیا ترکیبی از انواع فنآوری‌های ناهمگن است که هر فنآوری مجموعه‌ای از مشکلات و آسیب‌پذیری‌های خاص خود را دارد. بنابراین طراحی یک چارچوب امن برپایه SDN-IOT به دلیل همین وسعت دامنه مدیریت‌ها و تجهیزات، بسیار چالش برانگیز است. البته این چالش و هزینه‌های آن، ویژگی‌های بی‌نظیر این ساختار را تحت تاثیر قرار نمی‌دهد.

یک چارچوب بر پایه پروتکل OpenFlow به نام FRESCO جهت درهم آمیختن استراتژی‌های مختلف و اصلاح امنیت معرفی شده است. راه‌کار برجسته دیگری به نام OrchSec، در جهت توسعه استراتژی‌های امن از برنامه‌های نظارت بر شبکه و کنترل توابع SDN استفاده کرده است. با این حال، هنوز چالش‌های بسیاری هستند که باید بر آن غلبه کرد.

Denial of Service Attacks

علی رغم مکانیسم‌های امنیتی موجود، تحقیقاتی وجود دارد که تایید می‌کند حملات DOS هنوز تهدید بزرگی برای این دامنه، محسوب می‌شود. محدودیت نرخ کانال کنترل، فیلتر کردن رویدادها توسط یک کنترل کننده که امکان کنترل انتخابی رویدادها را دارد، اولویت‌بندی ترافیک و تنظیم زمان‌بندی، روش‌هایی است که برای مقابله با این حملات پیشنهاد شده است که حتی برخی از آن‌ها توسط پروتکل OpenFlow استاندارد شده‌اند. کارهای پیشنهادی با تمرکز بر کنترلر مرکزی محلی، درج/حذف جریان پویا و تجزیه و تحلیل خودکار ترافیک برای مقابله با حملات، شکل گرفته‌اند. اما این مسئله هنوز یک مسئله بسیار چالش برانگیز برای حل و فصل است.

Man-in-the-Middle Attacks

گاهی اوقات مکانیزم صدور گواهینامه/احراز هویت، امنیت ارتباطات را به خطر می‌اندازد. گواهینامه Self-Signed، ارتباطات مبتنی بر TLS/SSL و زیرساخت‌های کلید عمومی (PKI) موجود آسیب‌پذیری در برابر حملاتی مانند Man-in-the-Middle می‌شوند. در این حوزه، اقدامات متقابلی مانند Bloomfilter، یک پروتکل سبک که سیستم را برای چنین حملاتی رصد می‌کند ، پیشنهاد شده است. هم‌چنین، تجمیع پویا دستگاه، مکانیسمی که در آن یک سوییچ می تواند به صورت پویا خود را با چندین کنترلر بر اساس نیاز مرتبط کند، برای کنترل خودکار خطاهای ناشی از این حملات توصیه شده است. افزایش قابلیت برنامه‌ریزی data plane با استفاده از CPU همه منظوره یا پروکسی‌ها در سوییچ ها نیز یک راه حل احتمالی است. این موضوع اخیرا مورد توجه بسیاری قرار گرفته است.

Policy Definition Issues

به دلیل حیاتی بودن یکپارچه سازی data plane و control plane، تعریف سیاست‌های امنیتی به یک موضوع فوری تبدیل شده است. برای اتخاذ قابلیت استفاده گسترده، لازم است تعاریف سیاست زمینه‌ای گنجانده شود. هدف ایده‌آل این است که ضمن یکپارچه سازی الزامات امنیتی سطح بالا به طور همزمان از تنظیمات سطح پایین اقدامات امنیتی اعمال شده اطمینان حاصل کنید.

برای دستیابی به این هدف، راه حل‌هایی مانند زبان سیاست سلسله مراتبی برای سیستمهای توزیع شده (HiPoLDS) بر تمرکز زدایی از چارچوب‌های اجرایی مبتنی بر خدمات متمرکز شده است.

رویکرد دیگر، فرموله کردن الزامات امنیتی با استفاده از زبان سیاست‌های سطح بالا (HLP)، که ساختار ویژگی-موضوع-شی را اجرا می کند، است. این فرآیند دو مرحله ای است زیرا خروجی HLP توسط اسکریپت‌های زبان سطح متوسط (MLP) برای اصلاح سیاست پردازش می شود. اما سیاست‌های طراحی ناهمگنی شبکه اینترنت اشیا همراه با انعطاف‌پذیری آن برای طراحی، خسته کننده است.

مشخصات دقیق مقاله

Mishra, Pritish, Ananya Biswal, Sahil Garg, Rongxing Lu, Mayank Tiwary, and Deepak Puthal, "Software Defined Internet of Things Security: Properties, State of the Art, and Future Research", IEEE Wireless Communications 27, no. 3, pp. 10-16, 2020