زنجیره بلوکی و امنیت اینترنت اشیا

نام و نام خانوادگی نویسنده : محمدرضا منتظری
وابستگی سازمانی نویسنده (کارمند شهرداری قهجاورستان)

چکیده

دستگاه‌های اینترنت اشیا[۱] به‌طور فزاینده‌ای در زمینه‌های غیرنظامی و نظامی، از شهرهای هوشمند و شبکه‌های هوشمند گرفته تا اینترنت پزشکی اشیا[۲]، اینترنت رسانگرها[۳]، اینترنت نظامی اشیا[۴]، اینترنت میدان نبرد اشیا[۵] و غیره، دیده می‌شوند. در این مقاله به بررسی و مرور مقالاتی در زمینه‌ی راه‌حل‌های امنیتی IoT پرداخته‌ایم که از ژانویه‌ی سال ۲۰۱۶ به زبان انگلیسی چاپ شده‌اند. از مشاهدات ما، عدم وجود مجموعه‌داده‌های[۶] IoT با دسترسی عمومی، جهت استفاده در جوامع تحقیقاتی و شغلی است. با توجه به ماهیت حساس بالقوه‌ی مجموعه‌داده‌های IoT، نیاز به تدوین و توسعه‌ی استاندارد اشتراک‌گذاری مجموعه‌داده‌های IoT میان جوامع تحقیقاتی و شغلی و سایر ذینفعان احساس می‌شود. بنابراین، ابتدا به پتانسیل فن‌آوری زنجیره‌ی بلوکی[۷] در تسهیل امنیت اشتراک‌گذاری مجموعه‌داده‌های IoT (مثلاً استفاده از زنجیره‌ی بلوکی برای اطمینان از یکپارچگی مجموعه‌داده‌های به اشتراک گذاشته شده) و امن کردن سیستم‌های IoT، قبل از ارائه‌ی دو روش مفهومی مبتنی بر زنجیره‌ی بلوکی پرداخته‌ایم.

واژگان کلیدی: زنجیره‌ی بلوکی، امنیت زنجیره‌ی بلوکی، امنیت مبتنی بر همکاری[۸]، اینترنت نظامی اشیا، مجموعه‌داده‌ی IoT، IoT خود-بهبود[۹]، امنیت IoT، سامانه‌ی پیشگیری از نفوذ[۱۰]

---

۱ Internet of Things (IoT)
۲ Internet-of-Medical-Things (IoMT)
۳ Internet-of-Vehicles (IoV)
۴ Internet-of-Military-Things
۵ Internet-of-Battlefield-Things (IoBT)
۶ dataset
۷ blockchain
۸ Collaborative security
۹ IoT self-healing
۱۰ Intrusion-prevention system (IPS)

۱. مقدمه

مقالات باید در قالب نرم افزار مایکروسافت وُرد (۲۰۰۷ یا ۲۰۰۳ - MS-Word) ارسال گردد. متن اصلی مقاله به صورت تک ستونی با فونت B Nazanin - اندازهٔ ۱۲ - تک فاصله تهیه شود. عنوان بخش‌های اصلی با فونت B Nazanin و اندازه ۱۲- پررنگ و عنوان زیربخش‌ها با اندازه ۱۱- پررنگ تایپ شود. تنظیمات صفحه باید از بالای صفحه ۳ سانتیمتر و از پایین، چپ و راست صفحه ۲/۵ سانتیمتر باشد. در مقدمه به بیان مسأله، اهمیت موضوع، ادبیات و پیشینه، اهداف و فرضیه‌های پژوهش پرداخته شود (مقالات غیر پژوهشی از این چارچوب مستثنی هستند). طول مقاله با شکلها و جدولها نباید حداقل از ۵ صفحه کمتر و حداکثر از ۲۰ صفحه بیشتر باشد. برای رفرنس دهی داخل متن، باید از نام خانوادگی و سال استفاده شود. به عنوان مثال، برای منبع فارسی: (محمودی، ۱۳۹۳) و برای منبع انگلیسی: (Kumar, ۲۰۱٤). از شماره گذاری رفرنس ها در داخل متن جدا خودداری شود.

فن‌آوری‌ها شیوه و نحوه‌ی زندگی ما را، به‌ویژه در جامعه‌ی داده‌محور ما، تغییر داده‌اند. دلیل بخشی از این امر، پیشرفت فن‌آوری‌های نیم‌رسانا[۱۱] و ارتباطات است که باعث اتصال و ارتباط چندین دستگاه از طریق شبکه شده و راه‌های اتصال و ارتباط میان ماشین‌ها و انسان‌ها (برای مثال، ماشین به ماشین[۱۲]) را فراهم می‌کنند. عموماً چنین روندی اینترنت همه‌چیز[۱۳] نامیده شده و شامل اینترنت اشیا، اینترنت پزشکی اشیا، اینترنت میدان نبرد اشیا، اینترنت رسانگرها و غیره است. با توجه به فراگیر بودن چنین دستگاه‌هایی در جامعه‌ی ما (برای مثال، در شهرهای هوشمند، شبکه‌های هوشمند و سامانه‌های سلامت هوشمند)، امنیت و حریم شخصی دو مورد از نگرانی‌های اساسی این حوزه است. برای نمونه، در سال ۲۰۱۴ گزارش شد که بیش از ۷۵۰۰۰۰ دستگاه مصرف‌کننده در معرض توزیع فیشینگ[۱۴] و ایمیل‌های اسپم بودند. در کاربردهای حساس به داده چون IoMT و IoBT، تضمین امنیت داده، سامانه‌ها و دستگاه‌ها، همراه با حفظ حریم شخصی داده و محاسبات داده حیاتی است. هرچند احتمال دارد تهدید یک سامانه ناشی از یک اقدام امنیتی باشد که به درستی بررسی نشده است. برای مثال، در یک محیط بیمارستانی نظامی یا غیرنظامی معمول، معمولاً گروه فناوری اطلاعات[۱۵] کنترل کل شبکه، شامل دستگاه‌های نقاط پایانی[۱۶] و دستگاه‌های IoMT (اصولاً هر وسیله‌ای با نشانی آی‌پی[۱۷]) را برعهده دارند. انتظار آشنایی تیم IT با تمامی دستگاه‌های متصل‌شده، یک انتظار غیرواقعی است، هرچند آن‌ها از قابلیت مدیریت سامانه برای نصب پچ‌ها[۱۸]، دسترسی به دستگاه‌ها و داده‌های آن‌ها از راه دور و غیره برخوردارند.

[۱۱] semiconductor
[۱۲] machine-to-machine
[۱۳] Internet-of-Everything
[۱٤] phishing
[۱۵] Information Technology (IT)
[۱٦] endpoint devices
[۱۷] IP address
[۱۸] patches

چه اتفاقی می‌افتد اگر در حین عمل جراحی، یکی از دستگاه‌های IoMT که داروها را مدیریت می‌کند یکباره خاموش شده و بعد از اعمال پچ از راه دور توسط مدیر سامانه‌ی IT بازراه‌اندازی[۱۹] شود؟ احتمالاً این امر باعث هرج و مرج در اتاق عمل خواهد شد، چرا که گروه حراجی تصوری از آنچه که رخ داده، نخواهند داشت، نیازی به اشاره‌ی تروما و عواقب احتمالی برای بیمار (مثلاً محروم شدن بیمار از اکسیژن منجر به آسیب مغزی و مرگ می‌شود) نیست. به بیان دیگر، عملیات به‌ظاهر معمول، مانند اعمال پچ‌ها و بازراه‌اندازی دستگاه‌ها، می‌توانند منجر به فاجعه شود.

۲. بررسی و مرور IoT موجود و روش‌های امنیتی مربوطه

۲.۱. روش‌های شناسایی و پیشگیری از نفوذ

طراحان بدافزار[۲۰] امروزی و مهاجمین سایبری خلاق و نوآور بوده و به‌طور مداوم به‌دنبال دور زدن اقدامات موجود هستند (برای مثال، تولید نسخه‌های مختلف بدافزار با استفاده از جهش[۲۱]). اکثر روش‌های IDS و IPS موجود برای شناسایی تلاش‌های دسترسی غیرمجاز و حملات محروم‌سازی از سرویس توزیع‌شده[۲۲] طراحی شده‌اند. به‌عنوان مثال، آل‌سونبول[۲۳] و همکاران [۱۱] یک سیستم دفاعی شبکه برای شناسایی و پیشگیری از تلاش‌های دسترسی غیرمجاز، با تولید پویای پروتکل جدید جهت جایگزینی پروتکل استاندارد ارائه کرده‌اند. هدف این امر، مغشوش کردن تلاش‌های پویش است. همچنین مسیر شبکه متناوباً برای جلوگیری از دسترسی غیرمجاز و پویش ترافیک تغییر می‌کند. با این حال، تعداد بسته‌های تولیدی می‌تواند بیش از حد باشد. در روش زیتا[۲۴]، نرودا[۲۵] و وویتک[۲۶] [۱۹]، از رزپری پای ۳[۲۷] برای امن کردن بازخوان‌های[۲۸] سامانه‌ی بازشناسایی با امواج رادیویی[۲۹] فرکانس فرابالایی[۳۰] استفاده شده که از پروتکل بازخوان سطح‌پایین[۳۱] استفاده می‌کنند. به‌طور خاص، دو نرم‌افزار Fail۲ban و سوریکاتا[۳۲] به‌دلیل عملکرد و مقیاس‌پذیری[۳۳] بالا به‌عنوان راه‌حل انتخاب شدند. Fail۲ban از معماری پیچیده پشتیبانی می‌کند؛ بنابراین، مناسب پیاده‌سازی در محیط ابری با حسگرها و سرورهای متعدد است. عملکرد سوریکاتا بهتر از اسنورت[۳۴] بوده و پردازش چندریسمانی[۳۵] مورد نیاز CPU چندهسته‌ای رزبری پای ۳ را فراهم

[۱۹] reboot
[۲۰] malware
[۲۱] mutation
[۲۲] Distributed Denial of Service (DDoS) attack
[۲۳] Alsunbul
[۲۴] Zitta
[۲۵] Neruda
[۲۶] Vojtech
[۲۷] Raspberry Pi ۳
[۲۸] reader
[۲۹] Radio Frequency IDentification (RFID)
[۳۰] Ultra High-Frequency (UHF)
[۳۱] Low-Level Reader Protocol (LLRP)
[۳۲] Suricata
[۳۳] scalability
[۳۴] Snort
[۳۵] multithread processing

می‌کند. پارک[۳۶] و آن[۳۷] [۵۰] شناسایی و عملکرد اسنورت و سوریکاتا را هنگام مواجهه با حملات DoS را تحلیل و مقایسه کرده و نتیجه گرفتند مصرف CPU اسنورت کمتر است. هرچند، سوریکاتای چندریسمانی عملکرد شناسایی تک‌هسته‌ای و چندهسته‌ای بهتری دارد.

در ادامه به بررسی سامانه‌های شناسایی و/یا پیشگیری از نفوذ پرداخته‌ایم. برای سادگی از IDPS جهت ارجاع به سامانه‌های شناسایی و/یا پیشگیری از نفوذ استفاده شده است.

۲.۱.۱. طبقه‌بندی بر اساس روش‌ها

رمزنگاری[۳۸] یک روش رایج است که برای تامین محرمانگی و یکپارچگی داده، همانند روش‌های امنیتی چندلایه‌ای گزارش شده در [۲۷، ۳۲]، استفاده می‌شود. به‌طور خاص، چانگ[۳۹] و راماچاندران[۴۰] [۲۷] یک راه‌حل امنیتی چندلایه برای محاسبات ابری پیشنهاد داده‌اند. اولین لایه‌ی امنیتی، دیوار آتش[۴۱] و کنترل دسترسی است که برای اطمینان از دسترسیِ تنها کاربران مجاز و معتبر به سیستم‌ها و داده‌ها، طراحی شده است. وظیفه‌ی لایه‌ی دوم، مدیریت هویت و پیشگیری از نفوذ، جهت شناسایی مجدد کاربران و حذف تمامی پرونده‌های[۴۲] مخرب شناسایی شده، است. لایه‌ی سوم رمزنگاری همگرا[۴۳] است که یک خط‌مشی امنیتی از بالا به پایین را ارائه می‌دهد. برای ارزیابی روش پیشنهادی، نویسندگان آزمایش نفوذ روی ۱۰ پتابایت داده از مراکز داده انجام داده‌اند. با توجه به نتایج آزمایش، زمان مورد نیاز برای بازیابی بعد از تلاش دسترسی غیرمجاز حداقل ۱۲۵ ساعت است. مککائوئی[۴۴] و همکاران [۳۲] یک مدل امنیتی و حفظ حریم شخصی ابری[۴۵] چندلایه ارائه کرده‌اند که شامل پنج لایه است: لایه‌ی امنیت فیزیکی و محیطی[۴۶]، لایه‌ی امنیتی زیرساخت ابری[۴۷]، لایه‌ی امنیتی شبکه[۴۸]، لایه‌ی داده[۴۹] و لایه‌ی کنترل دسترسی و مدیریت امتیاز[۵۰].

---

[۳۶] Park
[۳۷] Ahn
[۳۸] Cryptography
[۳۹] Chang
[۴۰] Ramachandran
[۴۱] firewall
[۴۲] file
[۴۳] convergent encryption
[۴۴] Makkaoui
[۴۵] Cloud Security and Privacy Model (CSPM)
[۴۶] Physical and Environmental Security Layer (PESL)
[۴۷] Cloud Infrastructure Security Layer (CISL)
[۴۸] Network Security Layer (NSL)
[۴۹] Data Layer (DL)
[۵۰] Access Control and Privilege Management Layer (ACPML)

جین[۵۱]، توموشی[۵۲] و ماتسورا[۵۳] [۳۶] یک روش پیشرفته‌ی احراز هویت شبکه‌ی خصوصی مجازی[۵۴] با استفاده از سامانه‌ی موقعیت‌یابی جهانی[۵۵] ارائه کرده‌اند. روش پیشنهادی حفاظت حریم شخصی-جغرافیایی [۵۶] روی دستگاه‌های همراه را فراهم می‌کند. در اینجا، یک کاربر VPN مقدار هش[۵۷] اطلاعات GPS را به‌جای مقدار خام ارسال کرده و از حریم شخصی-جغرافیایی کاربر حافظت می‌شود. به جای ارائه‌ی فقط مختصات GPS، یک ناحیه برای ثبت‌نام با سرور احراز هویت برای هر کاربر فراهم شده است. از گوگل مپس[۵۸] برای صحت‌سنجی نرخ برخورد[۵۹] مختصات GPS کاربر در ناحیه‌ی مورد نظر استفاده شده و نتایج ارزیابی نویسندگان، نرخ دقت ۹۹/۲۹٪ برای عرض و ۹۲/۹۶٪ برای طول جغرافیایی گزارش شده است.

اولاگونجو[۶۰] و سامو[۶۱] [۴] یک هانی‌پات خودکار[۶۲] برای شناسایی نفوذ، پیشگیری و تصحیح در زمان واقعی با استفاده از رویکرد مدیریتی سامانه‌ی رخدادنگاری مرکزی[۶۳] (که به نام‌های پاپت[۶۴] و ماشین‌های مجازی[۶۵] نیز شناخته می‌شود) طراحی کرده‌اند. سامانه‌ی مرکزی اطلاعاتی را از آدرس منبع، زمان و کشور مهاجمین جمع‌آوری می‌کند. این روش نیاز به تلاش دستی جهت تصحیح پویای سامانه‌ی هانی‌پات به‌شدت تعاملی[۶۶] را با استفاده از فن‌آوری‌های آزاد در دسترس و متن‌باز کاهش می‌دهد. پروتکل انتقال پرونده در جذب مهاجمانی مفید است که ردپا یا اثری از نام‌های کاربری، گذرواژه‌ها و پورت‌های منبع از کشورهای مختلف برجای می‌گذارند. هرچند، کار دستی برای تبدیل هانی‌پات‌ها به هانی‌نت زیاد و قابل توجه است. آگراوال[۶۷] و تاپاسوی[۶۸] یک IDS چندلایه‌ی مبتنی بر هانی‌پات، برای شناسایی و پیشگیری از حملات نقطه دسترسی سرکش[۶۹] پیشنهاد کرده‌اند. این روش، IDS موجود و یک هانی‌پات را برای بهبود دقت IDS موجود ترکیب می‌کند و شامل فیلتر، شناسایی نفوذ و هانی‌پات است. این سیستم در یک شبکه‌ی بی‌سیم پیاده‌سازی شده است. با این وجود، می‌تواند به‌کاراندازی سیستم روی ابر و استفاده از روش یادگیری ماشین با حفظ نرخ پایین آژیر کاذب[۷۰] و سربار پایین هانی‌پات عملکرد کلی را ارتقا بخشد.

---

۵۱ Jin
۵۲ Tomoishi
۵۳ Matsuura
۵۴ Virtual Private Network (VPN)
۵۵ Global Positioning System (GPS)
۵۶ geo-privacy
۵۷ Hash
۵۸ Google maps
۵۹ Hit rate
۶۰ Olagunju
۶۱ Samu
۶۲ automated honeypot
۶۳ centralized logging system management technique
۶۴ puppet
۶۵ virtual machines
۶۶ Highly interactive
۶۷ Agrawal
۶۸ Tapaswi
۶۹ Rogue access point
۷۰ low false alarm rate

مرلو[۷۱]، میگلیاردی[۷۲] و اسپاداسینی[۷۳] [۱۳] یک مکانیزم وفقی[۷۴] پیشنهاد کرده‌اند که تمام خطاهای پیش‌بینی حساب‌کاربری و ترافیک باقی‌مانده را در نظر می‌گیرد. این مدل توسط شبیه‌ساز شبکه، ارزیابی و تاخیرها محاسبه شده است. با توجه به نتایج، کمینه تاخیری به دلیل تحلیل امنیت ایجاد شده است. با این حال، این مدل فاقد الگوریتم پیش‌بینی ایده‌آل است؛ بنابراین، برای پیش‌بینی‌های اشتباه و کاذب تاخیر، بسته تولید می‌کند.

ایندر[۷۵] و لمنارو[۷۶] [۱۶] یک IPS برای مقابله با حملات سایبری و بدافزار باتنت[۷۷] ارائه کرده‌اند. نویسندگان با تمرکز بر انتخاب ویژگی[۷۸] و مراحل استخراج، الگوریتم‌های یادگیری متفاوتی ارائه دادند که نتایج ارزیابی آن‌ها ۹۸٪ امتیاز پیش‌بینی گزارش شده است. علاوه‌براین، بر اساس ارزیابی آن‌ها با استفاده از مجموعه‌داده‌ی بنچمارک DARPA، نتیجه گرفتند که سوابق تکراری و اضافی بر ترافیک زمان واقعی تاثیر گذاشته و منجر به طبقه‌بندی ضعیف می‌شود. یک مجموعه‌ی آموزشی جدید با شناسایی موفق امضای حمله ایجاد شد. این روش حملاتی جدیدی را شناسایی می‌کند که در مجموعه‌ی DARPA اولیه وجود ندارند. کشری[۷۹] و همکاران [۲۱] یک روش پیشگیری محروم‌سازی از سرویس با استفاده از دیوارآتش و IDS مبتنی بر تکنیک‌های داده‌کاوی[۸۰] ارائه داده‌اند که شامل انتخاب داده، پردازش داده، انتقال و انتخاب مدل و ارزیابی است. آن‌ها از مجموعه‌داده‌ی NSL-KDD برای ارزیابی استفاده کرده‌اند که نسخه‌ی تصفیه شده از مجموعه‌داده‌ی KDD۹۹ cup است.

ساتو[۸۱] و همکاران [۴۳] یک معماری آرایه‌های دروازه‌ی برنامه‌پذیر در محل[۸۲] با طراحی مشترک مدارهای مجتمع با کاربرد خاص[۸۳] - FPGA پیشنهاد کرده‌اند که هدف آن ساده‌سازی پردازش IDPS و بهبود سرعت پردازش FPGA در مقایسه با ASIC/CPU (واحد پردازش مرکزی) است. در اینجا، FPGAها با استفاده از فن‌آوری منطق انتقال رجیستر[۸۴] طراحی شده و مدارهای محاسباتی[۸۵] در ASIC پیکربندی شده است. برای تایید نتیجه، جمع‌کننده‌های[۸۶] ASIC در FPGA با فن‌آوری نیم‌رسانای اکسید-فلز مکمل[۸۷] توسعه یافته است.

---

[۷۱] Merlo
[۷۲] Migliardi
[۷۳] Spadacini
[۷۴] adaptive mechanism
[۷۵] Indre
[۷۶] Lemnaru
[۷۷] Botnet
[۷۸] Feature selection
[۷۹] Keshri
[۸۰] Date mining
[۸۱] Satu
[۸۲] Field Programmable Gate Arrays (FPGA)
[۸۳] Application Specific Integrated Circuits (ASIC)
[۸۴] Register Transfer Logic (RTL)
[۸۵] arithmetic circuits
[۸۶] adder
[۸۷] Complementary Metal-Oxide-Semiconductor (CMOS)

خلاصه‌ای از روش‌های اخیر IDS و IPS در جدول ۱ آورده شده است.

جدول ۱ خلاصه‌ای از IDS و IPS اخیر، بر اساس روش‌ها

روش	منابع
رمزنگاری	کنترل دسترسی [۲۷، ۳۲]
	حفاظت حریم شخصی-جغرافیایی [۳۶]
وفقی	[۱۳، ۱۶، ۲۱]
مدارهای مجتمع با کاربرد خاص – طراحی مشترک معماری آرایه‌های دروازه‌ی برنامه‌پذیر در محل (ASIC-FPGA)	[۴۳]

۲.۱.۲. طبقه‌بندی بر اساس ساختار شبکه

یودوکیمنکو[۸۸] یک روش وفقی برای شناسایی و پیشگیری از حملات اکتیو در سیستم‌های مخابراتی طراحی کرده است. هرچند این روش قادر به شناسایی حملات جدید (مانند حملات با استفاده از استثمارات روز صفر[۸۹]) نیست. هیچ راه‌حل بی‌عیب و نقصی وجود ندارد و حذف تمام تهدیدهای امنیتی در یک شبکه غیرعملی است. جهت دست‌یابی به اطلاعات گره‌های شبکه و اولیت آن‌ها براساس موقعیت آن‌ها در گراف حمله، اباذری[۹۰]، مدنی[۹۱] و قرایی[۹۲] [۴۹] مدلی پیشنهاد داده‌اند که تهدیدها را بر اساس گراف حمله‌ی وزن‌دار محاسبه می‌کند. به‌طور خاص، این مدل جهت پاسخ تهدید چندمنظوره‌ی پیش‌کنشگری پویا برای کمینه کردن تهدیدها و هزینه‌ها طراحی شده است. در آینده می‌توان سایر روش‌های بهینه‌سازی مانند الگوریتم‌های ژنتیک را جهت پاسخ بهینه و سریع به تهدیدها پیاده‌سازی کرد.

سامانه‌های امنیتی مختلفی برای شبکه‌های بی‌سیم متفاوتی چون شبکه‌های اد هاک متحرک[۹۳]، وای-فای[۹۴]، شبکه‌های محلی[۹۵]، هانی‌پات‌ها و شبکه‌های حسگر ارائه شده است. برای مثال، فیلیپک[۹۶] و هودک[۹۷] [۱۰۲] یک مدل امنیتی برای MANETها بر اساس عملکرد زیرساخت‌های کلید عمومی[۹۸] توزیع شده، دیوار آتش و IPS پیشنهاد کرده‌اند. هر گره شامل مدل امنیتی یکسانی است،

[۸۸] Yevdokymenko
[۸۹] zero-day exploits
[۹۰] Abazari
[۹۱] Madani
[۹۲] Gharaee
[۹۳] Mobile Ad Hoc Networks (MANETs)
[۹۴] Wi-Fi
[۹۵] Local Area Networks (LANs)
[۹۶] Filipek
[۹۷] Hudec
[۹۸] Public Key Infrastructure (PKI)

بنابراین، مسیریابی امن، ارتباطات داده و نظارت حملات کارآمد فراهم می‌شود. مسیریابی و اطلاعات داده امضا و رمزنگاری می‌شوند و گره‌ها تنها به گره‌ها و خدماتی دسترسی دارند که مجاز هستند. هرچند IPS مورد استفاده در این سیستم، تنها شرایطی از شبکه را کنترل می‌کند که توسط PKI و دیوار آتش ایجاد شده باشند. IPSهای انرژی آگاه[۹۹] امکان شناسایی زودهنگام و حذف بسته‌های مخرب را فراهم کرده و منجر به تاخیرهای اضافی در تحویل بسته می‌شوند. فیلیپک و هودک [۲۵] یک معماری امن برای MANETها، شامل پروتکل مسیریابی مبتنی بر RSA امن، PKI، دیواره‌ی آتش و IPS ارائه کرده‌اند. بسته‌های مسیریابی امضا شده و از کلیدهای متقارن مذاکره شده[۱۰۰] با اعتبار کوتاه مدت جهت رمزگذاری ترافیک استفاده شده است. IPS بر ترافیک نظارت کرده و به گره‌ها با فعالیت‌های مشکوک هشدار می‌دهد. محدودیت‌های این روش، شامل محدودیت ترافیک به‌خاطر حضور دیوار آتش، و سربارهای قابل توجه به‌خاطر ارسال پیغام‌ها توسط گره‌ها، جستجوهای پایگاه داده[۱۰۱]، بسته‌های کنترل و رمزگذاری است.

یکچیرینا[۱۰۲] و همکاران [۳۱] یک شبکه‌ی وای-فای بی‌سیم توسعه داده‌اند که در سیستم عامل لینوکس کار کرده و به‌ترتیب از اسنورت و کیسمت[۱۰۳] به‌عنوان IDS و IPS استفاده می‌کند. آزمایش‌های نفوذ با Backtack ۵ R۳ با استفاده از کرکر فرن[۱۰۴] و اترکپ[۱۰۵] برای مطالعه‌ی پاسخ IPS انجام شده است. در تئوری، ادغام عملکردهای اسنورت و کیسمت می‌تواند عملکرد سیستم را با افزایش نرخ شناسایی در لایه‌های بالایی کیسمت و شبکه‌های بی‌سیم وای-فای اسنورت بهبود بخشد.

دیوانجی[۱۰۶] [۱۸] یک سیستم فیلتر نفوذ[۱۰۷] پیشنهاد کرده است که از امنیت قوی و توانایی خاتمه‌ی اجرا و توزیع پرونده‌های خراب برخوردار است. این سیستم به‌صورت آفلاین قابل استفاده بوده و توان عملیاتی[۱۰۸] بالایی فراهم می‌کند. در این روش، تمام پرونده‌های موجود در سیستم بررسی می‌شود، بدین‌گونه که رخداد[۱۰۹] سیستم پویش شده و اطلاعات مربوط به تمام برنامه‌ها و نرم‌افزارهای نصب شده در سیستم، در پایگاه داده‌ی IFS ذخیره می‌شود. بروزرسانی منظم پایگاه داده جهت خاتمه‌ی انتشار پرونده‌های خراب طراحی شده است. هرچند، هیچ پیاده‌سازی از IFS در دنیای واقعی وجود ندارد. لیو[۱۱۰] و کیو[۱۱۱] [۴۷] سودمندی استاندارد ۸۰۲.۱۱w را با استفاده از داده‌های آزمایشی عظیم و مدل صف[۱۱۲] برای جلوگیری از حملات DoS مبتنی بر پیشگیری حمله‌ی هجومی[۱۱۳] ارزیابی کردند. در

[۹۹] Energy aware
[۱۰۰] negotiated symmetric keys
[۱۰۱] database lookups
[۱۰۲] Yacchirena
[۱۰۳] Kismet
[۱۰۴] Fern Cracker
[۱۰۵] Ettercap
[۱۰۶] Dewanjee
[۱۰۷] Intrusion Filtration System (IFS)
[۱۰۸] throughput
[۱۰۹] Log
[۱۱۰] Liu
[۱۱۱] Qiu
[۱۱۲] Queuing model
[۱۱۳] Rushing Attack Prevention (RAP)

این مطالعه، یک مدل صف مبتنی بر STA معتبر جهت تحلیل عملکرد ۸۰۲.۱۱w ارائه شده است. علاوه‌براین، برای جلوگیری از حملات DeauthF و DisassF در نرخ پایین و بالای حملات، یک روش منسجم با ۸۰۲.۱۱w و شکل‌دهی ترافیک[۱۱۴] (در این مقاله با ۸۰۲.۱۱w-TS به آن ارجاع خواهیم داد) ارائه شده است.

کالنور[۱۱۵] و جی.آگارکد[۱۱۶] [۸] IDS برای شبکه‌های حسگر بی‌سیم با استفاده از تکنیک تطبیق الگو[۱۱۷] پیشنهاد داده‌اند. تطبیق الگو مجموعه‌ای از امضاها برای توصیف رویدادهای نامطلوب تعریف می‌کند و زمانی که الگویی با رویدادی مطابقت داشته باشد، یک عمل خاص توسط مجموعه‌ی امضاها یا قوانین اجرا و تعریف می‌شود. سپس، IDS داده‌های جمع‌آوری شده را تحلیل و این داده‌ها را با مجموعه امضای بزرگ مقایسه می‌کند. عدم تطابق مداوم بین الگوهای فعلی و قبلی باعث ایجاد هشدار و آلارم می‌شود. واسکیتا[۱۱۸]، سوهارتانتو[۱۱۹] و هندوکو[۱۲۰] [۴۵] به مطالعه‌ی روش آنتروپی[۱۲۱] برای یک سیستم تشخیص ناهنجاری[۱۲۲] پرداخته و ارزیابی‌ها در آزمایشگاه تحقیقاتی اینتل برکلی با استفاده از داده‌های واقعی از شبکه‌های حسگر توزیع‌شده انجام شده است. ارزیابی‌ها در فضای دو-بُعدی با محاسبه‌ی آنتروپی از سری‌های داده‌ی گره‌های دما و رطوبت اجرا شده است. با توجه به نتایج، بر خلاف روش بیضوی[۱۲۳]، روش آنتروپی از قابلیت تشخیص ناهنجاری‌های پراکنده بدون الگوی خاص برخوردار است.

جوکار[۱۲۴] و لئونگ[۱۲۵] [۱۵] مدلی پیشنهاد کرده‌اند که از IDPS برای شبکه‌های خانگی[۱۲۶] مبتنی بر زیگ‌بی[۱۲۷] استفاده می‌کند. این مدل از تکنیک پیشگیری مبتنی بر یادگیری ماشین پویا با نرخ مثبت اشتباه[۱۲۸] پایین استفاده می‌کند که بر دانش قبلی در مورد حملات متکی نیست. در این مدل مجموعه‌ای از اقدامات دفاعی (مانند پیشگیری از کلاه‌برداری[۱۲۹]، اجتناب از مداخله[۱۳۰] و حذف بسته‌های مخرب) جهت جلوگیری از حملات تعریف شده است. از کیو-یادگیری[۱۳۱] برای تعیین بهترین استراتژی مقابله با حمله استفاده شده است.

---

[۱۱۴] traffic shaping
[۱۱۵] Kalnoor
[۱۱۶] J. Agarkhed
[۱۱۷] Pattern matching
[۱۱۸] Waskita
[۱۱۹] Suhartanto
[۱۲۰] Handoko
[۱۲۱] Entropy method
[۱۲۲] anomaly detection system
[۱۲۳] elliptical method
[۱۲۴] Jokar
[۱۲۵] Leung
[۱۲۶] Home area networks
[۱۲۷] ZigBee
[۱۲۸] false positive rate
[۱۲۹] spoofing prevention
[۱۳۰] interference avoidance
[۱۳۱] Q-learning

سجلماسی[۱۳۲]، سنوسی[۱۳۳] و مسوس[۱۳۴] [۲۰] برای محافظت از یک پرنده‌ی هدایت‌پذیر از دور (پهپاد)[۱۳۵] یک سیستم امنیت سایبری مبتنی بر IDS را پیاده‌سازی کردند. این سیستم بر مدل تخمین تهدید مبتنی بر روش باور[۱۳۶] متکی است که هدف آن کمینه کردن نرخ مثبت اشتباه و منفی اشتباه است. هر پهپاد می‌تواند عامل نظارت IDS را برای مشاهده‌ی رفتار همسایگانش فعال کند. اگر عامل IDS به یک گره مخرب مشکوک شود، آن گره خاص نمی‌تواند به‌عنوان گره ناظر عمل کند.

راه‌حل‌های مختلفی برای شبکه‌های نرم‌افزارمحور[۱۳۷] ارائه شده است. برای مثال، منشی‌زاده[۱۳۸]، خَتری[۱۳۹] و کانتولا[۱۴۰] [۳۳] مدل چندین‌لایه‌ی IDS با ویژگی‌های قابل برنامه‌ریزی برنامه‌ی SDN، برای شناسایی و جلوگیری از حملات غیرمجاز، با استفاده از سوییچ‌های کنترلی برنامه‌ریزی SDN پیشنهاد داده‌اند. معماری پیشنهادی دارای یک برنامه‌ی SDN، کنترلر SDN، یک الگوریتم خوشه‌بندی[۱۴۱]، دو سوییچ و چندین گره شناساگر (با عنوان تشخیص سرویس-DaaS ارجاع داده می‌شود) است. این معماری شامل سه لایه بوده که عبارتند از: لایه‌ی کاربرد، لایه‌ی مدیریت و لایه‌ی داده. لایه‌ی کاربرد شامل برنامه‌ی SDN و یک رابط برنامه است. لایه‌ی مدیریت شامل کنترلر SDN و سوییچ‌ها و لایه‌ی داده دارای سوییچ، الگوریتم خوشه‌بندی و چندین گره DaaS برای شناسایی ترافیک غیرمجاز است. دو رویکرد پیشنهاد شده است: اول، خوشه‌بندی روی بسته‌های مجزای ترافیک آینه‌شده[۱۴۲] اعمال می‌شود؛ دوم، خوشه‌بندی روی ترافیک نمونه‌برداری شده اعمال می‌شود. ترکیبی از روش متعادل‌سازی بار و خوشه‌بندی روی ترافیک نمونه‌برداری شده استفاده می‌شود تا هزینه‌ی محاسباتی و تاخیر کنترلر SDN کاهش یابد. ماچادو[۱۴۳]، گرنویل[۱۴۴] و شیفر-فیلو[۱۴۵] [۳۷] معماری ANSwer را پیشنهاد کرده‌اند که دارای ویژگی‌های مجازی‌سازی عملکرد شبکه[۱۴۶] و SDN برای ایجاد استراتژی‌های تاب‌آوری شبکه[۱۴۷] است. نکته‌ی اصلی این روش استفاده از حلقه‌ی کنترلی بازخورد برای تحلیل رفتار زیرساخت شبکه جهت شناسایی ناهنجاری شبکه است. عمار[۱۴۸] و همکاران [۳۸] چارچوبی برای بهبود امنیت در مرکز داده‌ی مبتنی بر SDN ارائه داده‌اند. نویسندگان پیشنهاد داده‌اند که ویژگی‌های قابل برنامه‌ریزی SDN همراه با یکپارچه‌سازی لایه‌های کاربرد و امنیت، با ارائه‌ی یک لایه‌ی وقفی باعث افزایش

---

۱۳۲ Sedjelmaci
۱۳۳ Senouci
۱۳۴ Messous
۱۳۵ Unmanned Aerial Vehicle (UAV)
۱۳۶ Belief approach
۱۳۷ Software-Defined Networks (SDN)
۱۳۸ Monshizadeh
۱۳۹ Khatri
۱۴۰ Kantola
۱۴۱ Clustering algorithm
۱۴۲ Mirrored traffic
۱۴۳ Machado
۱۴۴ Granville
۱۴۵ Schaeffer-Filho
۱۴۶ Network Function Virtualization (NFV)
۱۴۷ network resilience
۱۴۸ Ammar

امنیت مرکز داده می‌شود. در این روش، با جستجوی الگوهای غیرطبیعی و تحلیل ترافیک شبکه، تهدیدهای مقاوم پیشرفته شناسایی می‌شوند. سپس یک از عامل امنیتی برای جمع‌آوری و تحلیل رخدادهای امنیتی و همچنین مسدود کردن مهاجمین استفاده می‌شود.

مک‌کین[۱۴۹] و شای[۱۵۰] [۴۱] یک IPS در زمانی واقعی برای شبکه‌ی خورد[۱۵۱]، خصوصاً کن باس[۱۵۲]، پیشنهاد داده‌اند. این طرح شامل واحدهای کنترل الکترونیکی[۱۵۳]، امنیت در شبکه‌ی پایه و رابط‌های خارجی است. پیغام‌ها به سه روش طبقه‌بندی می‌شود. پیغام‌های معتبر از تولیدکننده در ECUهای مختلف رمزگذاری می‌شوند. پیغام‌های بازپخشی، پیغام‌هایی هستند که از سگمنت کن باس دریافت شده یا از قبل شناسایی شده‌اند. یک پیغام نامعتبر با شناسه‌ی داوری[۱۵۴] نامنطبق بر ECU در سگمنت کن باس منجر به هشدار خواهد شد.

خلاصه‌ای از IDS و IPSهای اخیر مبتنی بر ساختارهای شبکه در جدول ۲ آورده شده است.

جدول ۲ خلاصه‌ای از IDS و IPSهای اخیر، بر اساس ساختار شبکه

ساختار شبکه	منابع
شبکه‌های مخابراتی	[۴۹ ،۵]
شبکه‌های اد هاک متحرک (MANETها)	[۲۵ ،۱۲]
وای-فای	[۳۱]
شبکه‌های محلی (LAN)	[۴۷ ،۱۸]
شبکه‌های حسگر	[۴۵ ،۸]
شبکه‌های هوشمند	[۱۵]
شبکه‌های رسانگر هوایی	[۲۰]
شبکه‌های نرم‌افزار محور	[۳۸ ،۳۷ ،۳۳ ،۲۴]
شبکه‌های محلی کنترلی	[۴۱]

[۱۴۹] McCune
[۱۵۰] Shay
[۱۵۱] Automotive network
[۱۵۲] Controller Area Network (CAN) bus
[۱۵۳] Electronic Control Units (ECU)
[۱۵۴] arbitration identifier

۲.۱.۳. طبقه‌بندی بر اساس کاربردها

چندین مطالعه به ارائه‌ی طرح‌های دستگاه‌های هوشمند محرک مختلف، مانند تلفن‌های هوشمند پرداخته است. برای مثال، ویج[۱۵۵] و جین[۱۵۶] [۷] رویکردهای IDPS موجود را برای تلفن‌های هوشمند بررسی کردند. با توجه به این بررسی، IDPS مبتنی بر شبکه می‌تواند برابرسازی بی‌درنگ[۱۵۷] را اجرا کرده و شناسایی پرونده‌های مخرب را قبل از بارگیری واقعی، برخلاف IDPSهای مبتنی بر میزان، تسهیل کند. از طرف دیگر، IDPSهای مبتنی بر میزان ارزان‌تر بوده و به سخت‌افزار زیاد (اختصاصی) نیازی ندارد. معمولاً، IDPS مبتنی بر شبکه بر IDPS مبتنی بر میزبان ارجح است. ساراسینو[۱۵۸] و همکاران [۱۰] یک آشکارساز ناهنجاری مبتنی بر رفتار چندسطحی برای دستگاه‌های اندروید طراحی کرده‌اند که برای تحلیل و همبستگی چندین ویژگی در چهار سطح مختلف اندروید (یعنی هسته (کرنل)[۱۵۹]، برنامه، کاربر و بسته) طراحی شده است. آشکارساز پیشنهادی با تشخیص الگوهای رفتاری خاص، تهدیدهای مظنون را شناسایی و مسدود می‌کند و هر باری که یک برنامه‌ی جدید نصب می‌شود، با بررسی مجوز مورد تقاضا و اعتبار فراداده، خطر امنیتی را ارزیابی می‌کند.

رشید[۱۶۰] و همکاران [۱۷] یک IPS هوشمند برای خانه‌های مجهز به سیستم روی یک تراشه[۱۶۱] مبتنی بر فن‌آوری‌های پردازش تصویر و شناسایی صدا توسعه داده‌اند تا بین مهمانان واقعی و مزاحمان تفاوت قائل شود. این سیستم، قفل در را برای چهره‌های شناخته شده و مجاز باز می‌کند. برای چهره‌های ناشناس و همچنین چهره‌های غیرمجاز، با استفاده از یک برنامه‌ی تلفن هوشمند، تماس صوتی با صاحب‌خانه برقرار کرده و به بازدیده‌کننده متصل می‌شود. در صورت تایید صاحب‌خانه، بازدیدکننده می‌تواند وارد حانه شود. اگر صاحب‌خانه اجازه‌ی دسترسی ندهد، می‌تواند به‌طور مستقیم با پلیس تماس بگیرد.

کدت[۱۶۲] و فوکوم[۱۶۳] [۲] IPSی برای صدا روی پروتکل اینترنت[۱۶۴] طراحی و پیاده‌سازی کردند. اگرچه این سیستم کارآمد و ساده است ولی سربار قابل توجهی به دلیل استفاده از اسنورت ایجاد می‌کند. چنت[۱۶۵] و همکاران [۲۹] طراحی و پیاده‌سازی VoIP IPS ارائه دادند که شامل معماری سلسله مراتبی روش‌های تشخیص مبتنی بر ناهنجاری آماری[۱۶۶] و تشخیص ناهنجاری پروتکل حالتمند[۱۶۷] است. با وجود اینکه دقت تشخیص و عملکرد SAD بهینه نیست، ولی می‌تواند به‌سرعت مانند فیلتر ترافیک، ترافیک نرمال و ترافیک غیرنرمال

---

[۱۵۵] Vij
[۱۵۶] Jain
[۱۵۷] real-time emulation
[۱۵۸] Saracino
[۱۵۹] kernel
[۱۶۰] Rashid
[۱۶۱] system-on-chip computer
[۱۶۲] Cadet
[۱۶۳] Fokum
[۱۶۴] Voice over Internet Protocol (VoIP)
[۱۶۵] Chenet
[۱۶۶] Statistical Anomaly-based Detection (SAD)
[۱۶۷] Stateful Protocol Anomaly Detection (SPAD)

را از هم تفکیک کند. از سوی دیگر، به‌دلیل الگوریتم تحلیل پیچیده‌ی SPAD، توان عملیاتی آن پایین است. زمانی که SAD و SPAD به‌صورت مکمل و همزمان استفاده شود، عملکرد پردازش IPS به‌طور چشمگیری افزایش می‌یابد. از ماژول تحلیل پروفایل برای کاهش نرخ مثبت اشتباه SAD، با بروزرسانی آستانه‌ی پروفایل SAD استفاده شده است.

اوسوپ[۱۶۸] و ساهاما[۱۶۹] [۳۰] سه اقدام کنترل امنیتی، به نام‌های اقدامات پیشگیرانه، تشخیص‌گری و تصحیحی، برای اطمینان از امنیت و حفظ حریم شخصی سامانه‌های ثبت الکترونیکی سلامت[۱۷۰] پیشنهاد کرده‌اند. هدف کنترل پیشگیرانه، جلوگیری از حمله قبل از وقوع آن است که با استفاده از گذرواژه، بازنویسی[۱۷۱] و اقدامات احراز هویت مختلف قابل دست‌یابی است. راه‌حل کنترل تشخیص‌گری از IDS/IPS برای شناسایی یک حمله استفاده می‌کند. کنترل تصحیحی (مانند اقدامات پشتیبان‌گیری سیستم) بعد از وقوع حمله به‌منظور کنترل خسارت ناشی از مهاجمان اعمال می‌شود. با اتخاذ راه‌حل‌های مختلف برای هر اقدام، از سیستم EHR در برابر حملات مختلف حفاظت می‌شود.

سیستم ایمنی مصنوعی[۱۷۲] یک روش هوش محاسباتی وفقی است که می‌توان از آن برای شناسایی و پیشگیری از حملات سایبری استفاده کرد. کوماوات[۱۷۳]، شارما[۱۷۴] و کوماوات [۹] یک مدل مبتنی بر ابر هیبرید برای شناسایی نفوذ و پیشگیری، جهت تشخیص حملات ناشناس ارائه کرده‌اند. در این روش، از اسنورت برای شناسایی نفوذ و پیشگیری استفاده شده و امضاهای جدید مربوط به حملات فعلی و ناشناس به IDS مبتنی بر رفتار فرستاده می‌شود که منجر به کمینه شدن نرخ‌های هشدار اشتباه بعدی می‌شود. فرهائویی[۱۷۵] [۲۳] IPSی بر اساس سیستم ایمنی مصنوعی با الهام از سیستم ایمنی طبیعی توسعه داده است. این سیستم از نظریه‌ی پاسخ ایمنی استفاده می‌کند: نظریه‌ی گزینش هم‌سانه‌ای[۱۷۶] و نظریه‌ی گزینش منفی[۱۷۷]. نظریه‌ی اول مناسب تحلیل سناریو IDPS مبتنی بر شبکه و نظریه‌ی دوم مناسب تحلیل رفتار IDPS مبتنی بر میزبان است. در این تحقیق، IDPS هیبرید به‌صورت سلسله مراتبی طراحی و در میان چندین ماشین توزیع شده است که نیازمند تحلیل داده از منابع مختلف است. الدوری[۱۷۸]، پنگریشز[۱۷۹] و الدوری [۴۴] یک سیستم ایمنی مصنوعی دوسطحی[۱۸۰] ارائه کرده‌اند که میان دسترسی عادی و سوابق حمله (پادگِن[۱۸۱]) با تولید

[۱۶۸] Osop
[۱۶۹] Sahama
[۱۷۰] Electronic Health Record (EHR)
[۱۷۱] paraphrase
[۱۷۲] Artificial Immune System (AIS)
[۱۷۳] Kumawat
[۱۷۴] Sharma
[۱۷۵] Farhaoui
[۱۷۶] theory of clonal selection
[۱۷۷] theory of negative selection
[۱۷۸] Al-Douri
[۱۷۹] Pangracious
[۱۸۰] Two-Level Artificial Immune System (TLAIS)
[۱۸۱] antigen

پادتن‌های[۱۸۲] تصمیم‌گیری (قوانین) تمایز قائل می‌شود. از الگوریتم ژنتیک برای تعریف سطح اول و از طبقه‌بندی درخت تصمیم[۱۸۳] برای تعریف سطح دوم استفاده شده است. سوابق دسترسی به صورت عادی، پادگن یا ناشناس دسته‌بندی می‌شوند. یک سابقه‌ی دسترسی ناشناس در سطح ۱ به سطح ۲ منتقل می‌شود تا در مورد عادی یا پادگن بودن آن تصمیم‌گیری شود. اگر سابقه مجدداً به‌عنوان ناشناس طبقه‌بندی شود، پادگن در نظر گرفته می‌شود.

چینگلین[۱۸۴] و جیوجوان[۱۸۵] [۲۶] یک الگوریتم فیلتر نشانی وب (مکان یکنواخت منبع[۱۸۶]) طراحی کرده‌اند. الگوریتم مذکور از ترکیب جدول هش برای فهرست‌بندی اطلاعات میزبان و درخت AVL برای مرتب‌سازی اطلاعات مسیر URL استفاده می‌کند. با این حال، روش فشرده‌سازی URL به دلیل نیاز به حافظه‌ی زیاد هنگام پردازش، ساختار خوبی ندارد. پروخورنکو[۱۸۷] و همکاران [۲۸] یک چارچوب نظارت بی‌درنگ برای برنامه‌های وب مبتنی بر پردازنده‌ی ابرمتن[۱۸۸] پیشنهاد داده و برای یک IPS طراحی کردند. حفاظت در سمت سرور تامین شده و نیازی به کمک سمت مشتری ندارد. معماری پیشنهادی تضمین‌گر رفتار مورد انتظار اجرایی برنامه‌ی وب توسط نویسنده‌ی برنامه بوده و رفتاری را اعمال می‌کند که توسط مدیر محافظت تعیین شده است.

سو[۱۸۹] و همکاران [۴۶] با استفاده از TCP به شبیه‌سازی حملات پرداخته و نتایج را با استفاده از UDP برای بررسی انواع مختلف حملات DDoS در دیوار آتش ارزیابی کرده‌اند. همچنین آن‌ها یک روش مصورسازی[۱۹۰] جهت کمک به تشخیص وقوع/عدم وقوع حمله، شناسایی ترکیب‌های غیرعادی بسته و ترافیک با مدل‌سازی رفتار مهاجم پیشنهاد کرده‌اند.

سجلماسی، سنوسی و مسوس [۵۲] برای محافظت از یک پرنده‌ی هدایت‌پذیر از دور (پهپاد) یک سیستم امنیت سایبری مبتنی بر IDS را پیاده‌سازی کردند. این سیستم بر مدل تخمین تهدید مبتنی بر روش باور متکی است که هدف آن کمینه کردن نرخ مثبت اشتباه و منفی اشتباه است. هر پهپاد می‌تواند عامل نظارت IDS را برای مشاهده‌ی رفتار همسایگانش فعال کند. اگر عامل IDS به یک گره مخرب مشکوک شود، آن گره خاص نمی‌تواند به‌عنوان گره نظارت عمل کند.

میرزا[۱۹۱]، محی‌الدین[۱۹۲] و آوان[۱۹۳] [۱] یک سیستم امنیتی با بهره‌وری کارآمد انرژی مبتنی بر ابر پیشنهاد کرده‌اند که شامل دو ماژول اصلی است: یک موتور ابری و یک عامل محلی. از موتور شناساگر مبتنی بر ابر برای تشخیص ناهنجاری استفاده می‌شود که شامل ۱۵

[۱۸۲] antibody
[۱۸۳] decision tree classifier
[۱۸۴] Qinglin
[۱۸۵] Xiujuan
[۱۸۶] Uniform Resource Locator (URL)
[۱۸۷] Prokhorenko
[۱۸۸] Hypertext Preprocessor (HPP)
[۱۸۹] Su
[۱۹۰] visualization method
[۱۹۱] Mirza
[۱۹۲] Mohi-Ud-Din
[۱۹۳] Awan

موتور ضدویروس[۱۹۴]، یک ماژول تحلیل بدافزار و یک ماژول جمع‌آوری اطلاعات هوشمند تهدید سایبری است. عامل محلی، یک عاملی میزبان سبک‌وزن است که برای شناسایی پرونده‌های مشکوک با اعمال قدرت به موتور ابری، استفاده می‌شود. با توجه به نتایج ارائه شده توسط نویسندگان، از ۱۰۰۰۰ نمونه بدافزار، ۹۸٪ آن شناسایی شده، درحالی که حداکثر ۶٪ قدرت CPU استفاده شده است. هرچند ابزار تحلیل آماری متن‌باز در موتور ابری تنها برای اجرا در مایکروسافت ویندوز، نه سیستم عامل دیگری، طراحی شده است. علاوه‌بر این، عامل میزبان نمی‌تواند پرونده‌های مخرب در سیستم را تا قبل از اجرا و ظاهر شدن آن‌ها در رخداد پردازش، شناسایی کند و این امر باعث آسیب‌پذیرتر شدن سیستم در مقابل حمله می‌شود. شارما، دوتی[۱۹۵] و پاتی[۱۹۶] [۳] یک چارچوب امنیت-به‌عنوان-سرویس مدیریت نفوذ[۱۹۷] قابل حمل[۱۹۸] بنابر تقاضا[۱۹۹] پیشنهاد داده‌اند. این سیستم مبتنی بر ابر از امکان شناسایی نفوذ، پیشگیری و پاسخ، گزارش‌دهی و رخدادنگاری برخوردار است. با نظارت بر ترافیک وب، تلاش‌های حمله را شناسایی می‌کند. در صورت نیاز، جریان‌های ورودی[۲۰۰]، تایید و فیلتر می‌شوند. برای اثبات این مفهوم، چارچوب پیشنهادی در یک ابر عمومی پیاده‌سازی شد و باتوجه به ارزیابی نویسندگان، سربار کلی به ترافیک در ابر عمومی وابسته است. علاوه‌بر ناکارآمد بودن، سیستم در معرض نقطه‌ی شکست نیز است.

چن[۲۰۱] و همکاران [۱۴] یک سیستم بهداشت و درمان مبتنی بر ابر کوچک[۲۰۲] ارائه داده‌اند که از عملکردهای ابر کوچک، مانند حفظ حریم شخصی، اشتراک‌گذاری داده و شناسایی و پیشگیری از نفوذ بهره‌مند است. از واحد تحقیق نظریه‌ی اعداد[۲۰۳]، برای حفاظت اطلاعات هنگام انتقال داده استفاده شده است. یک مدل اعتماد برای تصمیم‌گیری راجع‌به سطح اعتماد و اینکه داده باید به اشتراک‌گذاشته شود یا نه، طراحی شده است. سپس داده‌های ذخیره شده در ابرهای راه دور به سه بخش تقسیم و به روش‌های مختلف رمزگذاری می‌شود تا بهره‌وری انتقال بیشینه شود. در یک تحقیق مستقل دیگر، یک IDS مشارکتی توسط شقاقی[۲۰۴]، کافر[۲۰۵] و جا[۲۰۶] [۲۴] ارائه شده است. به‌طور خاص، نویسندگان یک دم‌گوه‌ای[۲۰۷]، یک IPS تشخیصی کنترلی، برای برقراری امنیت فرستنده‌ی داده[۲۰۸] شبکه‌ی نرم‌افزارمحور طراحی کرده‌اند. دستگاه‌های فرستنده‌ی مخرب و رفتار دقیق آن‌ها را می‌توان با تحلیل مسیر واقعی و مورد انتظار بسته، به‌صورت خودکار شناسایی کرد. هرچند، دقت در سناریوهای مختلف حمله و موارد مورد استفاده، نیازمند تحقیق و بررسی بیشتر

---

[۱۹۴] antivirus
[۱۹۵] Dhote
[۱۹۶] Potey
[۱۹۷] intrusion management Security-as-a-Service (lM-SecaaS)
[۱۹۸] portable
[۱۹۹] On-demand
[۲۰۰] Incoming streams
[۲۰۱] Chen
[۲۰۲] cloudlet
[۲۰۳] NTRU (Number Theory Research Unit)
[۲۰۴] Shaghaghi
[۲۰۵] Kaafar
[۲۰۶] Jha
[۲۰۷] WedgeTail
[۲۰۸] Data Plane

است. پایداری تصاویر لحظه‌ای[۲۰۹] در تحلیل سیستم نیز چالش‌برانگیز است. در حال حاضر، دم‌گوه‌ای با کنترلر SDN توزیعی سازگار نیست.

اوسانایی‌یه[۲۱۰]، چو[۲۱۱] و دی‌لودلو[۲۱۲] [۳۴] به مطالعه‌ی حملات DDoS در ابر پرداخته‌اند و دو دسته‌بندی، یکی برای حملات DDoS و دیگری برای دفاع DDoS ابری ارائه داده‌اند. با توجه به مطالعه‌ی آن‌ها، شناسایی مبتنی بر ناهنجاری و راه‌اندازی‌های نقاط دسترسی مناسب استراتژی‌های کاهش DDoS است. علاوه‌براین، یک چارچوب مفهومی برای شناسایی نقطه‌ی تغییر بسته ارائه دادند که به زمان ورود به داخل[۲۱۳] بسته وابسته است. سوپنا[۲۱۴] و همکاران [۳۵] یک مدل ابری پیشنهاد داده‌اند که در آن منطق فازی با دیوار آتش در یک ابر هیبریدی ادغام شده است. نویسندگان عملکرد مدل دیوار آتش فازی را در یک ابر هیبریدی شبیه‌سازی شده، با استفاده از پایگاه داده‌ی بار سنگین و یک برنامه‌ی وب‌سرور ارزیابی کردند. با توجه به این ارزیابی‌ها، دیوار آتش فازی از زمان پاسخ نسبتاً کمتری (برای مثال، ۱۰٪) در مقایسه با دیوار آتش معمولی برخوردار است.

سالک[۲۱۵] و مدنی [۴۲] یک IPSی بر اساس ناظر ماشین مجازی[۲۱۶] در محاسبات ابری ارائه کرده‌اند. هدف نویسندگان بهبود تلفات بسته و استفاده از منابع بدون تاثیرگذاری بر کارآیی است. این رویکرد امکان پیکربندی پویا بر اساس سطح خطر کاربران را فراهم می‌کند که در آن سطح خطر هر کاربر با سطح اعتمادش نسبت عکس دارد. کاربران به دسته‌ی پُرخطر، با خطر متوسط و کم خطر تقسیم می‌شوند. IDS نیز به طور مشابه، به IDS پرخطر (HIDS)، IDS با خطر متوسط (MIDS) یا IDS کم خطر (LIDS) تقسیم می‌شوند. بعد از شناسایی سطح خطر، یک عامل IDS پیش‌پیکربندی به VM هر کاربر اختصاص می‌یابد. با این حال، معماری حاضر از پیکربندی پویای IDS مبتنی بر سطوح امنیتی پویا پشتیبانی نمی‌کند.

خلاصه‌ی IDS و IPSهای اخیر بر اساس کاربرد در جدول ۳ آورده شده است.

جدول ۳ خلاصه‌ای IDS و IPSهای اخیر، بر اساس کاربرد

کاربرد	منابع
تلفن‌های هوشمند و امنیت اندروید	[۷، ۱۰، ۱۷]
صدا روی پروتکل اینترنت (VoIP)	[۲، ۲۹]

[۲۰۹] snapshots
[۲۱۰] Osanaiye
[۲۱۱] Choo
[۲۱۲] Dlodlo
[۲۱۳] Inter-Arrival Time (IAT)
[۲۱۴] Swapna
[۲۱۵] Salek
[۲۱۶] Virtual Machine Monitor (VMM)

ثبت الکترونیکی سلامت	[۳۰]
سیستم ایمنی مصنوعی	[۹، ۲۳، ۴۴]
وب‌سرور	[۲۶، ۲۸]
دیوار آتش	[۴۶]
پرنده‌ی هدایت‌پذیر از دور (پهپاد)	[۵۲]
ابر	[۱، ۳، ۱۴، ۲۷، ۳۲، ۳۴، ۳۵، ۴۲]

۲.۱.۴. خلاصه

واضح است که IDPS یک موضوع فعال در حوزه‌ی تحقیقاتی است. علاوه‌بر مواردی که در بخش‌های ۱.۱.۲ تا ۳.۱.۲ بحث شد، چندین تحقیق دیگر در این زمینه انجام شده است. برای مثال، فورد[۲۱۷] و همکاران یک IDPS سازمانی[۲۱۸] وفقی توسعه داده‌اند. از یک نرم‌افزار متن‌باز جلوگیری از دزدی، Fail۲ban، برای ایجاد عامل جمع‌آوری داده استفاده شده است. در اینجا، تمام عوامل نرم‌افزار، به سرویس پایگاه داده‌ی تحلیل رفتار مرکزی متصل بوده و فراداده‌ی[۲۱۹] حمله را در حین تلاش‌های قبلی جمع‌آوری و ضبط می‌کند. عوامل با اعمال قوانین ادغام روش تحلیل اطلاعات در سیاست‌های پیشگیری نفوذ، هم از داده‌های بی‌درنگ و هم از داده‌های قبلی، استفاده می‌کنند. با این وجود، سیستم پیشنهادی دارای نرخ مثبت اشتباه بالایی است. غریب[۲۲۰] و همکاران [۲۲] یک چارچوب ارزیابی برای مجموعه‌داده‌های IDS و IPS، بر اساس ویژگی‌های گوناگون مانند تنوع حمله، ناشناسی[۲۲۱]، پروتکل‌های در دسترس، ضبط کامل، تعامل کامل، پیکربندی کامل شبکه، ترافیک کل، مجموعه ویژگی، ناهمگونی[۲۲۲]، مجموعه‌داده‌ی دارای برچسب و فراداده معرفی کرده‌اند. ضریب انعطاف‌پذیری W تعریف شده که وزن هر ویژگی بر اساس نوع IDS/IPS انتخابی برای ارزیابی است. از KDD۹۹ و KYOTO برای ارزیابی چارچوب پیشنهادی استفاده شده است. پاتل[۲۲۳]، پاتل و کلوپا[۲۲۴] [۳۹] چارچوبی ارائه کرده‌اند که در آن، مدیر شبکه می‌تواند ترافیک شبکه را با جزییات بیشتری نسبت به یک دیوار آتش معمول بررسی کند. این روش از امکان جمع‌آوری اطلاعات

[۲۱۷] Ford
[۲۱۸] enterprise
[۲۱۹] Metainformation (metadata)
[۲۲۰] Gharib
[۲۲۱] anonymity
[۲۲۲] heterogeneity
[۲۲۳] Patel
[۲۲۴] Kleopa

مربوط به مصرف پهنای باند هر برنامه‌ی شبکه برخوردار است که بر اساس آن برنامه‌های ناخواسته را مسدود می‌کند. مدیران می‌توانند آشکارسازهای برنامه ایجاد کنند که به زبان برنامه‌نویسی لوآ[۲۲۵] نوشته شده‌اند. این آشکارسازها می‌توانند با اسنورت تعامل کنند.

۲.۲. روش‌های امنیتی مبتنی بر همکاری

امنیت به‌تنهایی کارآیی چندانی ندارد و در این اواخر، به دلیل پتانسیل شناسایی و پیشگیری از حملات در طیف وسیع‌تر، محققان به نمونه‌های امنیتی مبتنی بر همکاری علاقه‌مند شده‌اند. در این زیربخش، به بررسی کارهای اخیر راجع‌به روش‌های امنیتی مبتنی بر همکاری پرداخته‌ایم.

چندین مکانیزم کنترل دسترسی چندجانبه[۲۲۶] ارائه شده است. برای مثال، ژانگ[۲۲۷]، پاتوا[۲۲۸] و سندهو[۲۲۹] [۸۶] مکانیزم کنترل دسترسی برای مشتریان پلتفرم سرویس‌های وب آمازون[۲۳۰] ارائه کرده‌اند که اشتراک‌گذاری ایمن اطلاعات را تسهیل می‌کند. خصوصاً، برای سازمان‌ها این امکان را فراهم می‌کند تا با تبادل داده‌های امنیتی خود با سایر سازمان‌ها در بازه‌ی حمله‌ی سایبری، با یکدیگر همکاری و ارتباط برقرار کنند.

ایندوماتی[۲۳۱] و ساکتویل[۲۳۲] [۵۹] یک IDS برای MANETها پیشنهاد داده‌اند که از یک طرح امضای دیجیتالی برای حذف تصادم‌های گیرنده و محدودسازی توان انتقال برای کمینه کردن نرخ هشدار اشتباه استفاده می‌کنند.

روش‌های امنیتی مبتنی بر همکاری مختلفی برای حفظ حریم شخصی ارائه شده است. برای نمونه، فرویدیگر[۲۳۳] و همکاران [۶۴] پروتکل‌های حفظ حریم شخصی برای اندازه‌گیری کیفیت داده‌ی ماتریس‌های کامل[۲۳۴]، اعتبار، یکتایی، ثبات و به‌هنگام بودن[۲۳۵] با استفاده از تکنیک رمزنگاری هم‌ریختی[۲۳۶] پیشنهاد داده‌اند. در اینجا، کاربر تنها مقدار متریک کیفیت برای یک جانب نیمه‌صادق[۲۳۷] را می‌بینند. ارزیابی کیفیت داده تضمین می‌کند که داده‌های بی‌کیفیت رد خواهند شد و این امر باعث کاهش سربار مورد نیاز در پاک کردن داده در پلتفرم‌های وافادارانه[۲۳۸] می‌شود. واسیلومانولاکیس[۲۳۹] و همکاران [۸۵] یک IDS مبتنی بر همکاری آگاه از محل[۲۴۰] پیشنهاد داده‌اند که هشدارها را به حسگرهای ناظر توزیع می‌کند. با تبادل داده‌ی هشدار فشرده، سیستم پیشنهادی از مدیریت محلی و ارتباطات

---

۲۲۵ Lua
۲۲۶ multiparty
۲۲۷ Zhang
۲۲۸ Patwa
۲۲۹ Sandhu
۲۳۰ Amazon Web Services (AWS)
۲۳۱ Indumathi
۲۳۲ Sakthivel
۲۳۳ Freudiger
۲۳۴ matrices of completeness
۲۳۵ timeliness
۲۳۶ homomorphic encryption technique
۲۳۷ semi-honest party
۲۳۸ high-fidelity platform
۲۳۹ Vasilomanolakis
۲۴۰ locality-aware

با حفظ حریم شخصی برخوردار است. همچنین نویسندگان یک مکانیزم انتشار داده با حفظ حریم شخصی بر اساس فیلتر بلوم[۲۴۱] معرفی کردند. فرویدیگر، کریستوفرو[۲۴۲] و بریتو[۲۴۳] [۹۰] یک روش اشتراک‌گذاری داده‌ی کنترل‌شده در لیست سیاه قابل پیش‌بینی مشارکتی برای کاهش تهدید مشارکتی ارائه کرده‌اند. از ابزار رمزنگاری برای تصمیم‌گیری در مورد چگونگی اشتراک‌گذاری مجموعه‌داده با حفظ حریم شخصی استفاده شده است. استراتژی‌های اشتراک‌گذاری مختلف، با استفاده از مجموعه‌داده‌های دنیای واقعی ارزیابی شده است.

هیران[۲۴۴]، کارلسون[۲۴۵] و شهمهری[۲۴۶] [۶۳] یک چارچوب توزیع‌شده برای نظارت و محافظت از پروتکل دروازه‌ای مرزی[۲۴۷] مشارکتی در برابر حملات پیشوند/زیرپیشوند[۲۴۸] و مبتنی بر لبه پیشنهاد داده‌اند. این سرویس، یک سرویس لایه‌ی کاربردی است که اشتراک‌گذاری فعالیت شبکه را کنترل می‌کند که توسط مسیریاب‌ها و ناظرهای شبکه مشاهده می‌شود. سربارها، نرخ‌های هشدار و مقیاس‌پذیری، از اعلامیه‌ی عمومی BGP در ناحیه‌ی وسیع، نتایج شبیه‌سازی و آثار محاسبه می‌شود.

شارما، بوریا[۲۴۹] و سینگ[۲۵۰] [۸۴] یک روش رمزنگاری هیبرید با استفاده از RSA و الگوریتم امضای دیجیتال پیشنهاد کرده‌اند تا به توان عملیاتی و امنیت بالا دست‌یابند و سربار MANETها را کاهش دهند. عملکرد روش پیشنهادی با استفاده از پروتکل مسیریابی بردار مسافت بنابر تقاضای اد هاک امن[۲۵۱] و ابزار شبیه‌ساز شبکه‌ی NS-۲ ارزیابی شده است.

از روش نظریه‌ی بازی برای IDS مبتنی بر همکاری نیز استفاده شده است. نارنگ[۲۵۲]، مهتا[۲۵۳] و هوتا[۲۵۴] [۶۶] در مورد یک روش تصادفی، غیرقطعی و نظریه‌ی بازی برای شناسایی نفوذ در شبکه‌های همتابه‌همتای[۲۵۵] مشارکتی بحث کرده‌اند تا احتمال حمله‌ی موفقیت‌آمیز را کاهش دهند. در این روش گره‌های هدف به‌صورت دلخواه انتخاب شده و هیچ روش جامعی برای انتخاب گره‌های هدف وجود ندارد. علاوه‌بر این، این روش بر یک IDS تکی در هر مقطع زمانی متمرکز است. از آنجایی که این روش بر اساس ثبت تصویر لحظه‌ای از توپولوژی‌های شبکه است، توپولوژی‌های شبکه باید ثابت بمانند. علاوه‌بر این، فرض شده است که بازیکنان همیشه منطقی هستند. هرچند، لازم نیست رفتار مهاجمان و مدافعان در هر سناریو منطقی باشد. قربانی، قربانی و هاشمی [۷۰] در مورد یک چارچوب

---

[۲۴۱] Bloom filter
[۲۴۲] Cristofaro
[۲۴۳] Brito
[۲۴۴] Hiran
[۲۴۵] Carlsson
[۲۴۶] Shahmehri
[۲۴۷] Border Gateway Protocol (BGP)
[۲۴۸] Prefix/sub-prefix
[۲۴۹] Bhuriya
[۲۵۰] Singh
[۲۵۱] Secure Ad hoc On-Demand Distance Vector (SAODV)
[۲۵۲] Narang
[۲۵۳] Mehta
[۲۵۴] Hota
[۲۵۵] peer-to-peer network

IDS مشارکتی با مدل‌سازی بازی اتفاقی مجموع ناصفر[۲۵۶] چند بازیکنی بحث کرده‌اند تا تعاملات میان مهاجمان و IDS را نشان دهند. رفتار مورد انتظار از مهاجمان، مدافعان و پیکربندی بهینه‌ی هر IDS توسط راه‌حل تعادل ساکن نش[۲۵۷] توصیف می‌شود. وو[۲۵۸] و همکاران [۷۱] یک مکانیزم آگاهی موقعیتی امنیتی بر اساس تحلیل کلان‌داده[۲۵۹] برای شبکه‌های هوشمند توصیف کرده‌اند. تحلیل‌های موقعیتی امنیتی از روش مشارکت مبتنی بر خوشه‌ی فازی، نظریه‌ی بازی و یادگیری تقویتی[۲۶۰] استفاده می‌کنند. مکانیزم پیشنهادی به استخراج فاکتورهای موقعیتی امنیتی شبکه و تعیین پیش‌بینی موقعیتی امنیتی در شبکه‌های هوشمند کمک می‌کند.

روش امنیتی مبتنی بر همکاری بنیاسور[۲۶۱] و همکاران [۶۰] امنیت وفقی و تطبیق مبتنی بر همکاری را ترکیب کرده است. در این روش، امنیت وفقی به شناسایی کنترل‌های امنیتی مورد نیاز الزامات امنیتی بدون توجه به تغییرات محیط کمک می‌کند در حالی که تطبیق مبتنی بر همکاری بر مکانیزم مورد نیاز برای همکاری چندین اجزا متمرکز است. پیاده‌سازی رباتیک مشارکتی نیز ارائه شده است.

کریستوفوریدیس[۲۶۲] و ولاچوس[۲۶۳] [۵۸] یک برنامه‌ی کاربری سبک‌وزن مشارکتی ارائه دادند که از هوش مبتنی بر همکاری برای جلوگیری از حملات آنلاین استفاده می‌کند. به‌طور مشابه، ویلسون[۲۶۴]، براون[۲۶۵] و بیدل[۲۶۶] یک سیستم تجزیه و تحلیل فرضیه‌های رقابتی[۲۶۷] مشارکتی پیشنهاد کرده‌اند که با فرآیند راهنما[۲۶۸] فعال می‌شود. این مقاله پتانسیل فن‌آوری‌های سطح[۲۶۹]، در تحلیل هوش مشارکتی را مشخص کرده است. هدف این سیستم جستجوی تحلیل ACH با استفاده از بحث‌های چهره-به-چهره در مورد جنبه‌های مختلف تحلیل، مانند کامل بودن و صحت، است. این مدل از روش‌های مصورسازی نیز استفاده می‌کند؛ بنابراین امکان همکاری و تامل فراهم می‌شود. کیم[۲۷۰]، وو[۲۷۱] و کیم [۷۳] یک چارچوب کلی برای تحلیل همبستگی کارآمد حوادث تهدید سایبری با استفاده از هوش تهدید سایبری پیشنهاد کرده‌اند. در این چارچوب، از درخت رابطه‌ی رویداد[۲۷۲] برای نمایش رویدادهای مرتبط و از گراف انتقال رویداد[۲۷۳] برای توصیف انتقال گذرای مشخصات یک رویداد استفاده شده است. روش پیشنهادی با ردیابی انتقال حوادث سایبری مرتبط، می‌تواند قصد یک مهاجم را استنباط کند.

---

[۲۵۶] nonzero-sum stochastic game
[۲۵۷] stationary Nash equilibrium
[۲۵۸] Wu
[۲۵۹] Big data
[۲۶۰] reinforcement learning
[۲۶۱] Bennaceur
[۲۶۲] Christoforidis
[۲۶۳] Vlachos
[۲۶۴] Wilson
[۲۶۵] Brown
[۲۶۶] Biddle
[۲۶۷] Analysis of Competing Hypotheses (ACH)
[۲۶۸] walkthrough process
[۲۶۹] surface technologies
[۲۷۰] Kim
[۲۷۱] Woo
[۲۷۲] Event Relation Tree (ERT)
[۲۷۳] Event Transition Graph (ETG)

۲.۲.۱. طبقه‌بندی بر اساس ساختارهای شبکه

آریا، سینگ و سینگ [۸۳] به مطالعه‌ی حملات کرم‌چاله[۲۷۴] و حملات سیاه‌چاله‌ی مشارکتی[۲۷۵] در MANETها و چگونگی تشخیص این حملات با استفاده از الگوریتم‌های مسیریابی بردار مسافت بنابر تقاضای اد هاک مطمئن پرداخته‌اند. مقادیر اعتماد برای دو سناریوی حمله با پارامترهای مختلف (مانند انرژی، توان عملیاتی، نرخ تحویل بسته) محاسبه شده است. ارزیابی با شبیه‌سازی NS-۲ انجام شده است.

سانچک[۲۷۶] و آویو[۲۷۷] [۶۲]، LESS را که یک شبیه‌ساز مبتنی بر عامل میزبان است، برای ارزیابی مقیاس بزرگ سیستم‌های امنیتی پیشنهاد کرده‌اند. این یک روش مبتنی بر میزبان تصافی است که در آن عوامل میزبان ترافیک پس‌زمینه را از اثرهای واقعی و ترافیک مخرب را از پارامترهای مدل‌های تهدید تعریف شده توسط کاربر، تولید می‌کند. با استفاده از این نمونه‌ها، به‌صورت خودکار رفتار عامل میزبان را ایجاد و پیکربندی می‌کند و تمام فعالیت‌های آن‌ها را در تمام نتایج شبیه‌سازی‌ها نظارت می‌کند تا مجموعه‌داده‌های تجربی را تولید کند.

سعید و همکاران [۶۵] طرح‌های مبتنی بر همکاری برای سه شبکه‌ی مختلف ارائه کرده‌اند: مسیریابی، امنیت و رادیو در ارتباطات اد هاک بی‌سیم. نویسندگان در مورد دو راه‌حل امنیتی برای مقابله با حملات داخلی بحث کرده‌اند که عبارتند از: مکانیزم امنیت با طراحی و مکانیزم مبتنی بر اعتماد. مکانیزم دوم به دلیل رویه‌های امنیتی خودکار، منعطف‌تر و کارآمدتر است؛ هرچند، برای طراحی مدل مبتنی بر موقعیت شفاف، به ورودی و جنبه‌های سرویس نیاز دارد.

راتی[۲۷۸] و سائینی[۲۷۹] [۷۵] یک پروتکل مسیریابی AODV امن مبتنی بر کش ارائه کرده‌اند که از آخرین عدد دنباله‌ی بسته، برای کاهش حملات چاله‌ی خاکستری[۲۸۰] و سیاه‌چاله در یک شبکه‌ی مش بی‌سیم استفاده می‌کند. با استفاده از این روش، توان عملیاتی شبکه به‌طور چشمگیری افزایش می‌یابد. هرچند، تعداد محاسبات و مقدار سربار ذخیره‌سازی مورد نیاز قابل توجه است.

پن[۲۸۱] و همکاران [۷۶] یک شبکه از نوع هانی‌پات بر اساس SDN طراحی کرده‌اند که به جانب‌های مختلف امکان همکاری پویا و جداسازی دروازه‌ها و هانی‌پات‌ها را فراهم می‌کند. همچنین یک بازار نرم‌افزارمحور به‌نام HogMap، پیشنهاد داده‌اند که جانب‌های مختلف می‌توانند به سرویس‌های هوشمند تهدید سایبری عضو شوند.

---

[۲۷۴] Worm hole
[۲۷۵] collaborative black hole attack
[۲۷۶] Sonchak
[۲۷۷] Aviv
[۲۷۸] Rathee
[۲۷۹] Saini
[۲۸۰] Grey hole
[۲۸۱] Pan

لی[۲۸۲] و همکاران [۶۷] یک آشکارساز مشارکتی بر اساس میزبان توزیعی برای کاهش حملات تزریق داده‌ی اشتباه[۲۸۳]در سیستم فیزیکی-سایبری یک شبکه‌ی هوشمند پیشنهاد داده‌اند. یک الگوریتم رای‌گیری اکثریت بی‌درنگ مبتنی بر قانون برای تشخیص ناهنجاری‌ها در واحدهای اندازه‌گیری فازوری[۲۸۴] ارائه شده است. برای ارزیابی وضعیت کلی PMUها، یک سامانه‌ی اعتبار[۲۸۵] جدید طراحی شده است که از الگوریتم به‌روزرسانی اعتبار وفقی استفاده می‌کند. این روش با استفاده از داده‌های اندازه‌گیری بی‌درنگ شبیه‌ساز پاوررولد[۲۸۶] ارزیابی شده است.

لیو و بی[۲۸۷] [۸۲] یک سیستم مبتنی بر همکاری توزیعی برای دفاع در برابر کلاه‌برداری بین سامانه‌های خودگردان[۲۸۸] پیشنهاد داده‌اند. این سیستم باعث تسهیل همکاری موثر و منعطف هنگام دفاع از کلاه‌برداری به‌صورت پراکنده می‌شود. با توجه به نتایج ارزیابی با مجموعه‌داده‌های واقعی، این سیستم از نرخ مثبت اشتباه پایین، مصرف متوسط منابع و سطح امنیتی بالا برخوردار بوده و انگیزه‌ی راه‌اندازی را افزایش می‌دهد. یک صفحه‌ی کنترلی توزیع شده و سازگاری عقب‌گرد با صفحه‌ی داده‌ی قابل تحویل تدریجی برای IPv٤ و IPv٦ طراحی شده است.

۲.۲.۲. طبقه‌بندی بر اساس کاربردها

گنش[۲۸۹] و راماپراساد[۲۹۰] [۵۷] یک مدل کنترل دسترسی چندجانبه به همراه مشخصات خط مشی چندجانبه و سیستم ارزیابی برای شبکه‌های اجتماعی آنلاین پیشنهاد دادند. یک سیستم رای‌گیری برای دست‌یابی به حل موثر و منعطف مناقشه‌ی چندجانبه ارائه شده است. موضوعات امنیتی مختلف، در سه موقعیت متفاوت بررسی شده است: اشتراک‌گذاری پروفایل کاربر، اشتراک‌گذاری روابط و اشتراک‌گذاری محتوا در شبکه‌های اجتماعی آنلاین. در مورد پیاده‌سازی یک نمونه‌ی اولیه به نام کنترلر-دی[۲۹۱] جهت اثبات مفهوم بحث شده است. بوچامی[۲۹۲] و همکاران [۸۱] ارتقایی برای مکانیزم‌های کنترل دسترسی موجود با روش‌های خطر امنیتی در شبکه‌های اجتماعی حرفه‌ای[۲۹۳] ارائه دادند. خطر برای یک درخواست، توسط سه مقدارِ تاثیر، تهدید و آسیب‌پذیری تعریف می‌شود. یک سازمان می‌تواند با تعیین آستانه‌ی خطر، درخواست دسترسی را رد کند.

---

[۲۸۲] Li
[۲۸۳] False Data Injection (FDI)
[۲۸۴] Phasor Measurement Units (PMU)
[۲۸۵] reputation system
[۲۸۶] PowerWorld
[۲۸۷] Bi
[۲۸۸] AS (Autonomous Systems)
[۲۸۹] Ganesh
[۲۹۰] RamaPrasad
[۲۹۱] DController
[۲۹۲] Bouchami
[۲۹۳] Professional Social Networks (PSN)

کارانتجیاس[۲۹۴]، پولمی[۲۹۵] و پاپاسترگیو[۲۹۶] [۵۵] یک سیستم مدیریت امنیت مبتنی بر همکاری برای زیرساخت‌های حیاتی پیشنهاد داده‌اند که یک روش مدیریت خطر بر اساس مدل‌سازی و توانایی‌های تصمیم‌گیری گروهی را ادغام و یکپارچه کرده‌اند. این روش از دانش جمعی هر کاربر استفاده می‌کند و تهدیدهای فیزیکی و سایبری، حالت‌های حمله و مناطق جغرافیایی را تحلیل می‌کند. کوئل[۲۹۷]، مارکاریان[۲۹۸] و کولف[۲۹۹] [۵۶] مدیریت امنیت مبتنی بر همکاری را به‌عنوان یک قابلیت مدیریت موقعیت توصیف کرده‌اند که عملکرد امنیتی بر اساس گره‌های شبکه‌های مدیریت امنیت ATM[۳۰۰] جهانی[۳۰۱] طراحی شده است. یک حلقه‌ی تصمیم‌گیری با جمع‌آوری این گره‌های مفهومی شکل گرفته و وضعیت امنیتی موجود را ایجاد می‌کند. کولوت[۳۰۲] و همکاران [۸۰] در مورد قابلیت مدیریت موقعیت امنیتی مبتنی بر همکاری برای حمل و نقل هوایی و ناوبری بحث کرده‌اند. این روش از شناسایی پویا و ارزیابی تهدیدهای امنیتی و هماهنگی اقدامات امنیتی استفاده می‌کند. یک مدل با قابلیت پیش‌بینی تهدید برای فرمول‌بندی مسائل مدیریت موقعیت توسعه یافته است. این روش به‌منظور تامین قابلیت‌های امنیتی در چارچوب‌های مدیریت ترافیک هوایی آینده، مانند SESAR و NextGen طراحی شده است. پاپاسترگیو، پولمی و کارانتجیاس [۸۹] یک سیستم مدیریت امنیت سایبری-فیزیکی مبتنی بر همکاری برای زیرساخت‌های اطلاعاتی حیاتی پیشنهاد داده‌اند. ماژول ارزیابی خطر، روش‌های خودکار مختلف و ارزیابی خطرِ خود سفارشی را ارائه می‌دهد که توسط ابزار مصورسازی متن‌باز پیاده‌سازی شده است.

سالابی[۳۰۳] و شعیب[۳۰۴] [۶۹] یک معماری سیستم مدیریت شبکه برای مدیریت IoT مراقبت سلامت هوشمند پیشنهاد کرده‌اند. یک مدل شبکه‌ی مدیریت مخابرات[۳۰۵] چندلایه برای مدیریت اجزای مختلف سیستم مراقبت سلامت تعریف شده است. معماری مدیریت پیشنهادی از چهار لایه تشکیل شده که عبارتند از: عناصر مراقبت سلامت هوشمند، زمینه‌ی مراقبت سلامت هوشمند، مدیریت منابع و مدیریت سرویس. الموتیری[۳۰۶]، خان[۳۰۷] و الغمدی[۳۰۸] [۷۲] یک سیستم مراقبت سلامت محرک براساس زیرساخت اینترنت اشیا تعریف کرده‌اند تا هزینه‌های مراقبت سلامت و بستری غیرضروری را کاهش دهند. سیستم پیشنهادی شامل حسگرهای هوشمند و دستگاه‌های ارتباطی برای نظارت بر فشار خون، میزان قند خون، ECG، آسم و غیره است. این دستگاه‌ها به‌صورت بی‌سیم به سرورهای IoT وصل

[۲۹۴] Karantjias
[۲۹۵] Polemi
[۲۹۶] Papastergiou
[۲۹۷] Koelle
[۲۹۸] Markarian
[۲۹۹] Kolev
[۳۰۰] Air Traffic Management (ATM)

مدیریت ترافیک هوایی

[۳۰۱] GAMMA (Global ATM Security Management)
[۳۰۲] Kolevet
[۳۰۳] Sallabi
[۳۰۴] Shuaib
[۳۰۵] Telecommunications Management Network (TMN)
[۳۰۶] AlMotiri
[۳۰۷] Khan
[۳۰۸] AlGhamdi

شده‌اند و داده‌ها را دریافت، منتقل و ذخیره می‌کنند. به بیان دیگر، این معماری، یک معماری چند لایه شامل لایه‌های جمع‌آوری داده، ذخیره‌سازی داده و پردازش داده است.

چن و همکاران [۵۱] یک سیستم بهداشت و درمان مبتنی بر ابر کوچک ارائه داده‌اند که برای حفظ حریم شخصی، اشتراک‌گذاری داده و شناسایی و پیشگیری از نفوذ طراحی شده است. به‌طور خاص، از واحد تحقیق نظریه‌ی اعداد برای رمزگذاری اطلاعات جمع‌آوری شده از بدن کاربر توسط دستگاه‌های پوشیدنی، قبل از انتقال به ابر کوچک در همسایگی استفاده شده است. زی[۳۰۹] و همکاران [۶۸] یک چارچوب تشخیص ناهنجاری مشارکتی برای مدل‌سازی رفتار شبکه‌ی توزیع شده بر اساس میدان تصادفی مارکفی پنهان[۳۱۰] پیشنهاد داده‌اند. الگوریتم‌های مختلفی برای تخمین پارامتر، تخمین پیش‌رو[۳۱۱]، صاف‌کردن پس‌رو[۳۱۲] و ارزیابی نرمال بودن مدل‌های رفتار جهانی و محلی توسعه یافته است. صحت راه‌حل پیشنهادی با استفاده از مجموعه‌داده‌ی واقعی برای چهار نوع سناریوی شبکه، یعنی شبکه‌های معمولی، بی‌مقیاس، تصادفی و جهانی کوچک، تایید شده است. بوختوتا[۳۱۳] و همکاران [۷۴] با استفاده از تکنیک داده‌کاوی، یک مطالعه‌ی ترکیبی برای طبقه‌بندی بسته‌های مخرب در سطح شبکه ارائه داده‌اند. IDSهای مبتنی بر همکاری برای محیط ابری پیشنهاد شده است. برای مثال، میزرا و همکاران [۵۳] استفاده از روش هوک‌کردن تابع ویندوز[۳۱۴] را برای کاهش تهدیدهای پیشرفته و مستمر[۳۱۵] یا حملات روز صفر پیشنهاد کرده‌اند. از یک نسخه‌ی متن‌باز مدیریت رویداد و امنیت اطلاعات[۳۱۶] برای شناسایی حملات DoS استفاده شده است. چارچوب IDS مشارکتی لیانگ[۳۱۷] و همکاران [۸۷] شامل سه بخش است: مدیر کنترل ناحیه شناسایی نفوذ[۳۱۸]، کنترلر ناحیه شناسایی نفوذ[۳۱۹] و عامل شناسایی نفوذ[۳۲۰]. یک مکانیزم هشدار میان IDAها در یک ناحیه‌ی ابری معرفی شده تا اطلاعات مربوط به حملات را به اشتراک بگذارند. در یک مطالعه‌ی دیگر، مک‌درموت[۳۲۱]، شی[۳۲۲] و کیفایات[۳۲۳] [۸۸] چارچوبی برای ساخت یک IDS مبتنی بر همکاری استوار جهت حفاظت از خدمات زیرساخت در محیط ابری فدرال[۳۲۴] پیشنهاد کرده‌اند.

[۳۰۹] Xie
[۳۱۰] hidden Markov random field
[۳۱۱] forward prediction
[۳۱۲] backward smooth
[۳۱۳] Boukhtouta
[۳۱۴] windows function hooking technique
[۳۱۵] Advanced Persistent Threats (APTs)
[۳۱۶] Security Information and Event Management (SIEM)
[۳۱۷] Liang
[۳۱۸] Intrusion Detection Region Control Manager (IDRCM)
[۳۱۹] Intrusion Detection Region Controller (IDRC)
[۳۲۰] Intrusion Detection Agent (IDA)
[۳۲۱] MacDermott
[۳۲۲] Shi
[۳۲۳] Kifayat
[۳۲۴] federated cloud environment

در [۹۱] نویسندگان طرح تحلیل بسته برنامه‌ی اندروید[۳۲۵] بر اساس طبقه‌بندی/خوشه‌بندی برای تعیین کمیت خطر یک APK پیشنهاد داده‌اند. این امر با استفاده از طبقه‌بندی و خوشه‌بندی اطلاعات تولیدی از فراداده‌ی آنلاین حاصل شده است. عملکرد طرح مبتنی بر خوشه‌بندی، به خاطر ویژگی‌های عملکردی دقیق‌تر ثبت، بهتر است. کوردرو[۳۲۶] و همکاران [۹۲] یک IDS توزیع شده‌ی بر اساس انجمن و مشارکتی برای یادگیری مدل‌های ناهنجاری و سپس شناسایی ناهنجاری‌های شبکه پیشنهاد داده‌اند. از انجمن‌های حسگرها برای تبادل ترافیک شبکه و شناسایی مشارکتی ناهنجاری استفاده شده است. الگوریتم‌های تصادفی جهت گروه‌بندی حسگرها در انجمن‌های مختلف و برای نظارت نمونه‌های ترافیک شبکه توسعه یافته است.

جونیور[۳۲۷] و همکاران [۷۹] یک معماری سیستم دیوار آتش توزیع‌شده‌ی خودتطبیقی[۳۲۸]، بر اساس همکاری عناصر مختلف در زیر شبکه پیشنهاد داده‌اند. در این معماری، یک سیستم ارزیابی آسیب‌پذیری با سیستم پیشنهادی برای کاهش حملات از آسیب‌پذیری‌های شناخته شده، همکاری می‌کند. برای این منظور، از دو واحد موتورهای تحلیل و تصمیم‌گیری استفاده شده است.

هرالد[۳۲۹]، کینکلین[۳۳۰] و کارل[۳۳۱] [۷۷] یک سیستم رسیدگی حادثه‌ی مشارکتی بر اساس الگوی تخته‌سیاه[۳۳۲] ارائه کرده‌اند. این سیستم امکان جای‌دهی[۳۳۳] و تعامل مشارکتی میان گام‌های رسیدگی حادثه را فراهم می‌کند که بعداً این گام‌ها، به واحدهای عملیاتی قابل تعویض تقسیم شده و در شبکه توزیع می‌شوند. بخش‌های اصلی سیستم، مدل اطلاعاتی برای تخته‌سیاه و مدل اجرا برای دسترسی به اطلاعات در تخته‌سیاه است.

واگنر[۳۳۴] و همکاران [۷۸] یک پلتفرم اشتراک‌گذاری اطلاعات بدافزار و پلتفرم پروژه‌ی اشتراک‌گذاری تهدید ارائه کرده‌اند تا شاخص‌های سازش[۳۳۵] مهم اهداف حمله را جمع‌آوری کرده و به اشتراک بگذارند. هدف این پروژه ارائه‌ی پلتفرمی است که در آن کاربران از سازمان‌های خصوصی تا عمومی بتوانند اطلاعات و IoC تهدیدهای موجود را در یک محیط قابل اعتماد به اشتراک بگذارند.

چن [۵۴] و همکاران یک سیستم نمونه‌ی امنیتی شبکه‌ی مبتنی بر همکاری با طرح همکاری مرکزی برای تامین امنیت شبکه در مراکز داده‌ی چندمستاجری[۳۳۶] ارائه کرده‌اند. این سیستم با طرح رای بسته‌ی هوشمند برای بازرسی بسته و حفاظت از حملات احتمالی شبکه در درون شبکه‌ی مرکز داده یکپارچه شده است.

---

[۳۲۵] AndroidPackage (APK)
[۳۲۶] Cordero
[۳۲۷] Jónior
[۳۲۸] Self-adaptive
[۳۲۹] Herold
[۳۳۰] Kinkelin
[۳۳۱] Carle
[۳۳۲] Blackboard pattern
[۳۳۳] interleaving
[۳۳۴] Wagner
[۳۳۵] Indicators of Compromise (IoC)
[۳۳۶] multiple-tenant

خلاصه‌ای از روش‌های اخیر امنیت مبتنی بر همکاری بر اساس کاربرد در جدول ۴ آورده شده است.

جدول ۴ خلاصه‌ای از امنیت مبتنی بر همکاری اخیر، بر اساس کاربرد

کاربرد	منابع
شبکه‌ی اجتماعی آنلاین	[۵۷، ۸۱]
حمل و نقل	[۵۵، ۵۶، ۸۰، ۸۹]
مراقبت سلامت هوشمند	[۶۹، ۷۲]
نفوذ	شناسایی [۵۱، ۵۳، ۶۸، ۷۰، ۷۴، ۸۵، ۸۷، ۸۸، ۹۱، ۹۲]
	کاهش [۷۵، ۷۹، ۸۹، ۹۰]
رسیدگی حادثه	[۷۷]
محاسبات ابری و IoT	[۵۳، ۵۴، ۷۲، ۷۸]

۲.۳. روش‌های امنیتی پیشگویانه

همان‌طور که از تعداد اندک مقالات و بررسی‌ها پیداست، امنیت پیشگویانه یک موضوع تحقیقاتی نسبتاً جدید است. با توجه به ضرب‌المثل معروف، می‌دانیم که پیشگیری بهتر از درمان بوده و معادل این ضرب‌المثل در این حوزه، شناسایی و تعمیر است. برای اطمینان از تاب‌آوری سایبری در سیستم IoT هوشمند و کارآمد، داشتن توانایی پیش‌بینی حملات آینده در شبکه، حیاتی است (علاوه‌بر شناسایی و جلوگیری از حملات فعلی). زیربخش ۳.۲. بر این موضوع متمرکز است.

با در نظر گرفتن این نکته که سیستم کاملاً امن در واقعیت وجود ندارد، معیارهای کمّی امنیت می‌توانند برای تعیین کمّی امنیت نسبی سیستم مفید باشند. واضح است که رابطه‌ی قوی و مستقیمی میان خطاهای انسانی و شکاف‌های امنیتی وجود دارد و تحقیقات کثیری در این راستا انجام شده است. برای نمونه، نورالدین[۳۳۷] و همکاران [۹۳] مدلی بر اساس نظریه‌ی بازدارندگی کلی[۳۳۸] طراحی کرده‌اند که از فرآیند تصمیم‌گیری انسان مشتق شده است. برای این امر، نویسندگان با مطالعه‌ی علوم اجتماعی و روانشناسی، به بررسی نظریه‌های رفتار انسان در امنیت سایبری پرداخته و مدل‌های امنیتی پیشگویانه برای مطالعه‌ی اثربخشی امنیت گذرواژه و ممیزی امنیتی مورد نیاز در یک سازمان مبتنی بر مشتری، ساخته‌اند. به‌طور خاص در این مدل، کارمندان برای پردازش ایمیل‌های شخصی و کاری با حساب‌های

[۳۳۷] Noureddine
[۳۳۸] general deterrence theory

محافظت‌شده با گذرواژه، به منابع محاسباتی سازمان دسترسی دارند. سازمان مکرراً بررسی‌های امنیتی را برای کشف تخلفات انجام می‌دهد. یک مطالعه‌ی موردی برای نمایش رفتار نمایندگان خدمات مشتری و شبکه‌های فعالیت تصادفی[۳۳۹] [۹۴] برای مدل‌سازی تعامل میان کارکنان و خط‌مشی امنیتی سازمان استفاده شده است. روش پیشنهادی، با چندین چالش مواجه است. اول، طراحی یک مدل از نقطه‌نظر مهاجمان، کارکنان و مدیران در سطوح مختلف و با جزییات بسیار مشکل است. دوم، رفتار انسان از نظریه‌ی توصیفی[۳۴۰]، نه نظریه‌ی هنجاری[۳۴۱]، پیروی کرده و مدل‌سازی ریاضی آن دشوار است. در نهایت، دست‌یابی به رفتار نامشخص نظریه، اعتبارسنجی و صحت‌سنجی نتایج چالش‌برانگیز است. نویسندگان یک مدل مبتنی بر عامل پیشنهاد داده‌اند که می‌توان به‌عنوان روش جایگزین به‌کار رود. این سیستم جایگزین به‌صورت گروهی از عوامل مستقل طراحی شده که از توانایی ارزیابی موقعیت فعلی خود و تصمیم‌گیری برای خود برخوردارند.

آبراهام[۳۴۲] و نیر[۳۴۳] [۹۵] در مورد یک استراتژی امنیت سایبری پیشگویانه تحقیق کرده‌اند که برای حفاظت از زیرساخت‌های حیاتی در برابر تهدیدهای خارجی و کاهش خطر مرتبط قبل از وقوع طراحی شده است. نویسندگان یک مدل تصادفی جدید برای ارزیابی امنیت بر اساس گراف‌های حمله پیشنهاد کرده‌اند که جنبه‌های زمانی آسیب‌پذیری‌ها را در نظر گرفته است. یک مدل مارکفی غیرهمگن، با استفاده از گراف‌های حمله تعریف شده است که متغییرهای کمکی وابسته‌به زمان[۳۴۴] (مانند سن آسیب‌پذیری و نرخ کشف آسیب‌پذیری) را برای پیش‌بینی حالت‌های امنیتی آینده‌ی شبکه جهت شناسایی حملات روز صفر ترکیب می‌کند. از یک چارچوب امتیازدهی آسیب‌پذیری باز، سیستم امتیازدهی آسیب‌پذیری عام[۳۴۵] [۹۶-۹۹] برای جمع‌آوری تمام مشخصات پیچیده‌ی بهره‌برداری (مانند بردار دسترسی، پیچیدگی دسترسی و احراز هویت) جهت ارائه‌ی بینش عملی قدرتمند استفاده شده است. مطالعات موردی مختلفی، با استفاده از تولید گراف حمله و امنیت و تحلیل تاثیرگذاری جهت ارزیابی مفهوم انجام شده است. این روش از لحاظ استفاده از چارچوب CVSS با در نظر گرفتن بهره‌برداری و تاثیرگذاری و همچنین گسترش مدل برای دربرگرفتن جنبه‌های زمانی آسیب‌پذیری در درخت حمله، منحصر به‌فرد است. یکی از اصلی‌ترین چالش‌های این روش، بهبود بیشتر قابلیت تصمیم‌گیری معماری و مدل پیشنهادی با پیش‌بینی شکاف‌های امنیتی در آینده است.

دستگاه‌های متحرک (تلفن همراه) می‌توانند جزئی از زیرساخت IoT بوده و به‌تبع آن در برابر تهدیدهای تاثیرگذار بر سایر فن‌آوری‌های مصرف‌کننده‌ی محبوب، آسیب‌پذیر باشند. با توجه به نیازمندی‌های محاسباتی و انرژی، تاکید بر رمزگذاری جهت حفاظت اطلاعات،

[۳۳۹] Stochastic Activity Networks (SAN)
[۳۴۰] descriptive theory
[۳۴۱] normative theory
[۳۴۲] Abraham
[۳۴۳] Nair
[۳۴۴] time-dependent covariates
[۳۴۵] Common Vulnerability Scoring System (CVSS)

معمولاً برای دستگاه‌هایی با توان پایین محاسباتی مناسب نیست. شی، ابهیلش[۳۴۶] و هوانگ[۳۴۷] [۱۰۰] یک مدل امنیتی با ساختار سلسله مراتبی بر اساس زنجیره‌ی اعتماد میان دستگاه‌های متحرک، مش ابر کوچک و یک پلتفرم ابری از راه دور ارائه کرده‌اند. هدف این روش شناسایی نفوذ مشارکتی میان ابرهای کوچک فعال شده با وای-فای چندگانه، توسط دسترسی به خدمات ابری با وای-فای یا شبکه‌های موبایل است. فیلتر بی‌درنگ حملات مخرب از طریق ابرهای از راه دور قابل اعتماد قابل انجام است که از تحلیل‌های امنیتی پیشگویانه برای پویش امضای بدافزار و حذف اسپم/بدافزار خودکار استفاده شده است. ابرهای از راه دور، از قابلیت داده‌کاوی جهت ارائه‌ی امنیت-به‌عنوان-سرویس به تمام کابران نهایی برخوردارند. روش پیشنهادی روی ابر EC۲ با MapReduce پیاده‌سازی و با بیش از ۱ ترابایت داده‌ی توییتر ارزیابی شد. یک سیستم شناسایی نفوذ هیبریدی می‌تواند از مش ابر کوچک برای تشخیص بدافزار و ناهنجاری‌های شبکه استفاده کند، همچنین با یکپارچه‌سازی این مدل با روش‌های رنگ‌آمیزی داده[۳۴۸] [۱۰۱]، می‌توان از پایگاه داده‌ی عظیم در ابر حفاظت کرده و به آن دسترسی داشت.

با در نظر گرفتن ماهیت حملات و ویژگی‌های مدل ورهولست خاکستری مرسوم[۳۴۹]، لیائو[۳۵۰]، یو-بنگ[۳۵۱] و مانیکم[۳۵۲] [۱۰۲] یک مدل پیش‌بینی ورهولست خاکستری وفقی برای پیش‌بینی موقعیت امنیتی شبکه در آینده، در یک سازمان عادی پیشنهاد کرده‌اند. در مدل پیشنهادی، ترکیبی از قانون ذوزنقه[۳۵۳] و قانون سیمپسون یک سوم[۳۵۴] برای یافتن مقدار پس‌زمینه در معادله‌ی دیفرانسیلی خاکستری و به‌تبع آن پیش‌بینی خروجی آینده استفاده شده است. جهت ارزیابی کارآیی روش پیشنهادی، از خطای درصدی مطلق میانگین[۳۵۵] و خطای جذر میانگین مربعات[۳۵۶] استفاده شده است. با توجه به نتایج، مدل جدید از دقت پیش‌بینی ۹۳/۳٪ برخوردار است، در حالی که دقت GM(۱،۱) ۸۷/۳ ٪ و دقت مدل ورهولست خاکستری ۹۲/۰٪ است. نویسندگان برای بهبود دقت پیش‌بینی، یک مدل مکمل با الگوریتم پیش‌بینی باقی‌مانده طراحی کرده‌اند.

۳. بحث و بررسی

با توجه به جدول ۵، تعداد اندکی از مطالعات به ارزیابی روش پیشنهادی پرداخته‌اند و اکثر ارزیابی‌ها در مابقی مطالعات، مبتنی بر نرم‌افزار بوده است.

---

[۳۴۶] Abhilash
[۳۴۷] Hwang
[۳۴۸] data-coloring techniques
[۳۴۹] traditional grey Verhulst model
[۳۵۰] Leau
[۳۵۱] Yu-Beng
[۳۵۲] Manickam
[۳۵۳] Trapezoidal rule
[۳۵۴] Simpson's one-third rule
[۳۵۵] Mean Absolute Percentage Error (MAPE)
[۳۵۶] Root Mean Square Deviation (RMSD)

جدول ۵ خلاصه‌ای از ارزیابی روش‌های استفاده شده در مطالعات

نمونه	IDS/IPS/IDPS	امنیت مبتنی بر همکاری	امنیت پیشگویانه
نرم‌افزار	[۴، ۱۱، ۱۳، ۱۵، ۱۷، ۱۹] [۲۴، ۲۵، ۲۹، ۳۱، ۳۵] [۴۳، ۴۶، ۴۷، ۴۸، ۵۰، ۵۲]	[۵۹، ۶۱، ۷۴، ۷۵، ۸۷]	[۹۳]
سخت‌افزار	[۲]	-	-
نرم‌افزار و سخت‌افزار	[۴۱]	-	-

با توجه به جدول ۶، مجموعه‌داده‌ی KDD پراستفاده‌ترین مجموعه‌داده‌ی داده در ارزیابی تحقیقات IDS/IPS/IDPS، و مجموعه‌داده‌ی DARPA هم در ارزیابی مربوط به IDS/IPS/IDPS و هم ارزیابی مربوط به امنیت مبتنی بر همکاری به‌کار گرفته شده است. به‌نظر می‌رسد علیرغم روند رو به رشد تحقیقات در زمینه‌ی امنیت IoT، مجموعه‌داده‌های IoT از لحاظ وسعت و عمیق، خصوصاً برای تحقیقات امنیت پیشگویانه، محدود هستند.

جدول ۶ خلاصه‌ای از مجموعه‌داده‌های استفاده شده در ارزیابی‌ها

مجموعه‌داده	IDS/IPS/IDPS	امنیت مبتنی بر همکاری	امنیت پیشگویانه
مجموعه‌داده با دسترسی عمومی (شامل دسترسی با درخواست)	KDD۹۹ [۲۲]	سه Routeviewsmonitors عمومی و سه سرور traceroute عمومی [۶۳]	توییت‌ها [۱۰۰]
	KYOTO [۲۲]	CAIDA [۶۸]	DARPA [۱۰۲]
	اپ‌های موبایل [۱۰]	DARPA [۷۱، ۹۲]	
	مرکز داده‌ی ابر – ۱۰پتابایت [۲۷]	VirusTotal [۷۳]	
	DARPA [۱۶، ۴۲]	DShield [۸۵، ۹۰]	
	NSL KDD [۲۱، ۴۴]		
	آزمایشگاه تحقیقاتی اینتل برکلی [۴۵]		
مجموعه‌داده با	مجموعه الگوی URL [۲۶]	اپ‌های موبایل [۹۱]	

دسترسی غیرعمومی	شبکه [۳۷]	
شبیه‌سازی‌ها	[۱، ۹]	[۵۱، ۶۲، ۶۷، ۷۷، ۸۱-۸۴]

نیاز به مجموعه‌داده‌ی IoT با دسترسی عمومی: نقش مجموعه‌داده‌های دنیای واقعی در ارزیابی هر تکنیک امنیتی پیشنهادی، به‌ویژه امنیت پیشگویانه، قابل اغماض نیست. بنا به زمان و تلاش مورد نیاز برای جمع‌آوری و تدوین این مجموعه‌داده، مجموعه‌داده‌ی دنیای واعقی در دسترس بسیار اندک است. حل این چالش با گوناگونی معماری‌ها و دستگاه‌های IoT دشوارتر می‌شود. علاوه‌بر این، در حین بررسی‌های انجام شده، هیچ مجموعه‌داده‌ی IoT دنیای واقعی با دسترسی عمومی مشاهده نشد.

نیاز به اشتراک‌گذاری امن مجموعه‌داده‌ی IoT با دسترسی عمومی: جهت به حداکثر رساندن تلاش‌های تحقیقاتی در زمینه‌ی امنیت IoT، به اهمیت اشتراک‌گذاری مجموعه‌داده‌های دنیای واقعی تاکید می‌کنیم. برای تسهیل اشتراک‌گذاری مجموعه‌داده‌های دنیای واقعی، توصیه می‌کنیم یک استاندارد برای این مجموعه‌داده‌ها توسعه یابد و با استفاده از تکنیک زنجیره‌ی بلوکی، از یکپارچگی مجموعه‌داده‌های اشتراکی اطمینان حاصل شود. علاوه‌بر این، هنگام انتشار عمومی مجموعه‌داده، باید حریم شخصی نیز حفظ شود.

بر اهمیت داشتن طیف گسترده‌ای از مجموعه‌داده‌های IoT، نماینده‌ی سیستم‌ها و دستگاه‌های IoT ناهمگون[۳۵۷] موجود تاکید می‌کنیم. برای مثال، یک مجموعه‌داده ممکن است شامل داده‌های جمع‌آوری شده از چندین منبع مانند ترافیک شبکه و رخدادهای عملیاتی دستگاه‌های IoT مختلف در یک صنعت خاص یا زمینه (مثلاً شبکه‌های هوشمند) باشد. حتا در یک سیستم واحد IoT، ممکن است انواع مختلفی از دستگاه‌های IoT با فرمت‌ها و ساختارهای متفاوت داده موجود باشد. بنابراین، باید منابع اطلاعاتی را طبقه‌بندی کرده و فرمت و ساختار داده را بر اساس صنعت یا زمینه تعریف کنیم.

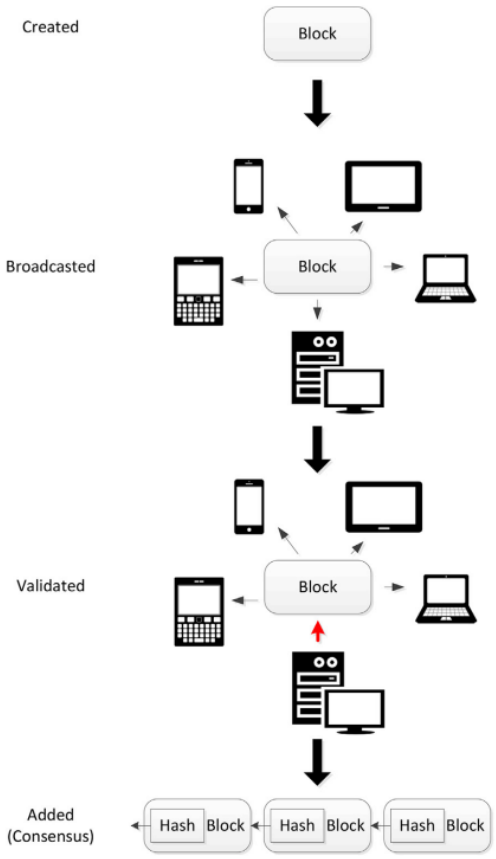
علاوه‌بر این، احتمالاً این مجموعه‌داده‌های دنیای واقعی حجیم خواهند بود. بنابراین یک توزیع مرکزی یا الگوی اشتراکی پاسخگو نخواهد بود. در عوض، می‌توانیم از یک هاب[۳۵۸] مرکزی استفاده کنیم که به سرورهای ذخیره‌سازی توزیع‌شده‌ی مختلفی ارجاع دهد که مجموعه‌داده‌ها در آنجا واقعاً ذخیره شده و امکان دسترسی و توزیع وجود دارد. با ثبت‌نام در سرور ذخیره‌سازی هاب، می‌توان به مجموعه‌داده دسترسی داشته یا آن را به اشتراک گذاشت. زمانی که چارچوب در دسترس عموم قرار بگیرد، باید یکپارچگی مجموعه‌داده‌ها حفظ شود. بنابراین، زنجیره‌ی بلوکی نقش مهمی در حفظ یکپارچگی مجموعه‌داده‌ها خواهد داشت (ر.ک. بخش ۴)

۴. زنجیره‌ی بلوکی برای IoT

[۳۵۷] heterogeneous
[۳۵۸] Hub

در ابتدا زنجیره‌ی بلوکی برای ثبت تراکنش‌های مالی استفاده می‌شد که تراکنش‌ها توسط تمامی شرکت‌کنندگان رمزگذاری و نگه‌داری می‌شد (مانند بیت‌کوین‌ها و رمزارزها[۳۵۹]). از این‌رو، تمام تراکنش‌ها شفاف بوده و هرگونه تغییر را می‌توان به‌راحتی ردیابی کرد و تشخیص داد. از زنجیره‌ی بلوکی جهت بهبود امنیت IoT می‌توان استفاده کرد. در ادامه دو نمونه از استفاده از زنجیره‌ی بلوکی برا بهبود امنیت IoT ارائه خواهیم کرد.

تصویر ۱، یک فرآیند معمول زنجیره‌ی بلوکی را نشان می‌دهد. زمانی که یک تراکنش انجام می‌شود، یک بلوک ایجاد می‌شود. بلوک به تمام گره‌های شبکه اطلاع‌رسانی می‌شود. یکی از گره‌های موجود، بلوک را تایید کرده (در بیت‌کوین این عمل استخراج[۳۶۰] نامیده می‌شود) و مجدداً به شبکه اطلاع‌رسانی می‌کند. اگر این بلوک تایید شده و بلوک به درستی به بلوک قبلی ارجاع داده شده باشد، گره‌ها آن را به زنجیره‌ی بلوکی فعلی خود اضافه می‌کنند.

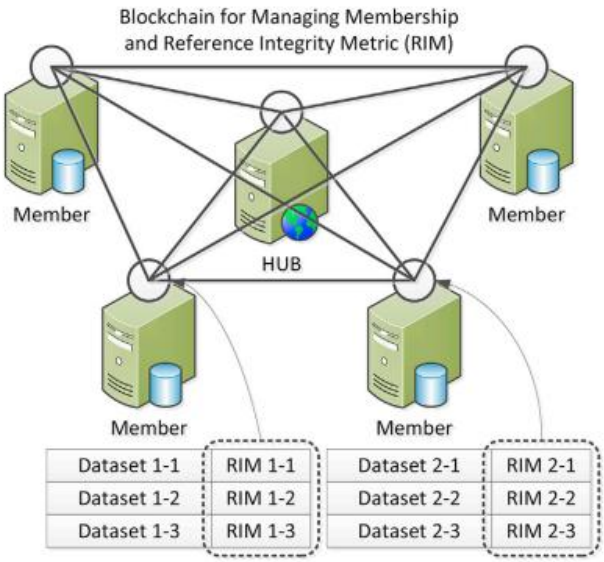


تصویر ۱. فرآیند کار یک زنجیره‌ی بلوکی نمونه (اقتباس شده از [۱۰۴])

۴.۱. زنجیره‌ی بلوکی در اشتراک‌گذاری مجموعه‌داده

[۳۵۹] cryptocurrencies
[۳۶۰] mining

همان‌طور که قبلاً بحث شد، زمانی که مجموعه‌داده‌ها میان جوامع پژوهشی و شغلی یا گسترده‌تر به اشتراک‌گذاشته شود، باید یکپارچگی آن‌ها حفظ شود. در این مقاله، برای اطمینان از یکپارچگی مجموعه‌داده‌ها، با استفاده از زنجیره‌ی بلوکی یک شاخص یکپارچگی مرجع[۳۶۱] حفظ می‌شود. خصوصاً، هر بار که مجموعه‌داده‌ای بارگیری می‌شود، یکپارچگی آن توسط RIM بررسی می‌شود (ر.ک. تصویر ۲).



تصویر ۲مدیریت اعضا و شاخص‌های یکپارچگی مرجع مبتنی بر زنجیره‌ی بلوکی مفهومی

در روش پیشنهادی ما، یک هاب مرکزی وجود دارد که تنها به مخازن[۳۶۲] اعضا، جایی که مجموعه‌داده‌ها ذخیره و توزیع می‌شود، ارجاع می‌دهد. اطلاعات مربوط به عضویت، مانند آدرس، مالک و خط‌مشی اشتراک‌گذاری توسط زنجیره‌ی بلوکی محافظت می‌شود. به بیان دیگر، اطلاعات عضویت توسط تمامی اعضا ازجمله هاب، ثبت و به اشتراک‌گذاشته می‌شود. یک زنجیره‌ی بلوکی دیگری برای حفاظت از RIM مجموعه‌داده‌ها وجود دارد. هدف استفاده از این زنجیره‌ی بلوکی، اطمینان از یکپارچگی مجموعه‌داده‌هاست.

زمانی که مجموعه‌داده‌ها در دسترس عموم باشند، حریم شخصی مجموعه‌داده یک نگرانی اساسی است. برای حفظ حریم شخصی و جلوگیری از هر گونه نقض مقررات مربوط به حریم شخصی، بر نیاز به ابزار خودکار ناشناس‌سازی مجموعه‌داده قبل از انتشار آن، تاکید می‌کنیم.

چالش دیگری که باید در نظر بگیریم، طول عمر مجموعه‌داده‌هاست. ممکن است صاحبان مجموعه‌داده‌ها نخواهند آن‌ها را به‌طور دائم به اشتراک بگذارند. اما هر تعاملی که توسط زنجیره‌ی بلوکی ثبت می‌شود، قابل تغییر یا حذف کردن نیست. هرچند این امر یک ویژگی

[۳۶۱] Reference Integrity Metric (RIM)
[۳۶۲] repositories

امنیتی قوی است، در صورت نیاز به حذف سابقه‌ی ثبت شده‌ای، نباید آن را به اشتراک گذاشت. در چارچوب مجموعه‌داده‌ی پیشنهادی، تنها RIM توسط زنجیره‌ی بلوکی نگه‌داری می‌شود. بنابراین، حتا اگر RIM در زنجیره‌ی بلوکی باقی بماند، مجموعه‌داده‌ها برای اشتراک‌گذاری در دسترس نخواهند بود.

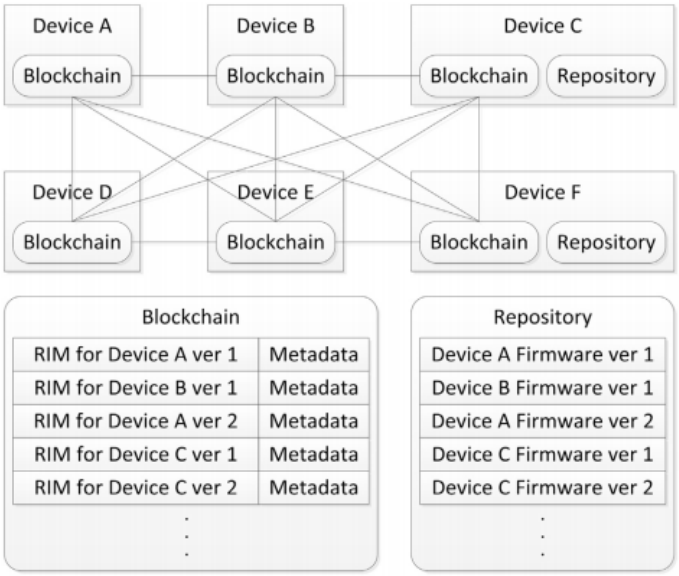
۴.۲. شناسایی ثابت‌افزار[۳۶۳] و خودبهبودی مبتنی بر زنجیره‌ی بلوکی

هیچ تکنیک امنیتی بی‌عیب و نقضی وجود ندارد و سیستم‌ها و دستگاه‌های IoT علیرغم بهترین تلاش‌ها (امنیتی) ممکن است در معرض خطر باشند. بنابراین، دستگاه‌های در معرض خطر یا به خطر افتاده، باید از قابلیت خودبهبودی برخوردار باشند. پیشنهاد ما، استفاده از زنجیره‌ی بلوکی جهت تسهیل خودبهبودی دستگاه‌های به خطر افتاده است.

اکثر تکنیک‌های محافظت از ثابت‌افزار موجود بر اساس بررسی یکپارچگی است. با شروع از بارگذار راه‌انداز[۳۶۴]، یکپارچگی ثابت‌افزار سطح بعدی (سیستم عامل و برنامه‌ها) قبل از اجرا بررسی می‌شود. بارگذار راه‌انداز در یک حافظه‌ی فقط خواندنی[۳۶۵] امن ذخیره شده و تحت هیچ شرایطی قابل تغییر نیست. این امر معمولاً ریشه‌ی اعتماد[۳۶۶] نامیده می‌شود. بارگذار راه‌انداز در حین کپی کردن کد سیستم عامل از حافظه‌ی فلش[۳۶۷] به حافظه‌ی کاری (مثلاً DRAM)، یکپارچگی آن را بررسی می‌کند. با همین روال، سیستم عامل، یکپارچگی برنامه‌ها را قبل از راه‌اندازی بررسی می‌کند. بررسی یکپارچگی غالباً با مقایسه با RIM انجام می‌شود. RIM سیستم عامل و برنامه‌ها از قبل محاسبه شده و در یک مکان امن ذخیره می‌شود. قبل از اجرای سیستم عامل و برنامه‌ها، شاخص یکپارچگی آن‌ها محاسبه شده و با RIM مقایسه می‌شود. تنها زمانی که هر دو مقدار یکسان باشند، سیستم عامل و برنامه‌ها اجرا خواهند شد. برای اطمینان از اعتمادپذیری اجرا یا فعالیت، یکپارچگی RIM بسیار مهم است. اگر ثابت‌افزار نمی‌تواند به‌روزرسانی شود، RIM باید در حافظه‌ی فقط خواندنی ذخیره شود. هرچند به دلایل مختلف مانند پچ‌های امنیتی و ارتقای خدمات، معمولاً مجاز به به‌روزرسانی است. زمانی که ثابت‌افزار به‌روزرسانی می‌شود، RIM مربوطه نیز باید به‌روز شود. اگر به هر طریقی مخربی بتواند RIM مربوط به ثابت‌افزار را به‌روزرسانی کند، روش‌های بررسی یکپارچگی موجود بی‌اثر خواهند بود.

پیشنهاد ما استفاده از زنجیره‌ی بلوکی برای محافظت از RIM است که در تصویر ۳ نشان داده شده است. زنجیره‌ی بلوکی یک پایگاه داده‌ی توزیع شده است که تمامی تراکنش‌ها را پیگیری می‌کند. از آنجایی که تمام دستگاه‌های شرکت‌کننده، از سوابق ثبت‌شده‌ی یکسانی نگه‌داری می‌کنند، یکپارچگی سوابق حفظ می‌شود مگر اینکه مخرب بتواند اکثر دستگاه‌ها را به خطر بیاندازد.

[۳۶۳] firmware
[۳۶۴] bootloader
[۳۶۵] Read-only
[۳۶۶] Root of trust
[۳۶۷] Flash memory



تصویر ۳ روش شناسایی ثابت‌افزار و خودبهبودی مبتنی بر زنجیره‌ی بلوکی مفهومی

معمولاً از افزونگی[۳۶۸] برای تصحیح نرم‌افزارهای تخریب شده استفاده می‌شود که در آن کد یکسان یا مشابه جای‌گزین کد تخریب شده می‌شود. در روش پیشنهادی ثابت‌افزار تخریب شده با ثابت‌افزار «شناخته‌شده‌ی خوب» جای‌گزین می‌شود. با استفاده از زنجیره‌ی بلوکی، پیشینه‌ی ثابت‌افزار را می‌توان ردیابی کرد. بنابراین زمانی که ثابت‌افزار تخریب‌شده‌ای شناسایی می‌شود، مجبور می‌شود به نسخه‌ی قبلی خود بازگردد. به دلیل محدودیت منابع، تمامی دستگاه‌ها نمی‌توانند نسخه‌ی قبلی ثابت‌افزار را ذخیره کنند. از این رو، برخی از دستگاه‌های شبکه (به‌عنوان مثال، گره‌های واسط با ظرفیت ذخیره‌ی زیاد مانند محیط محاسبات لبه‌ای[۳۶۹])، از ورژن قبلی ثابت‌افزار در مخازن خود برای دستگاه‌های همسایه نگه‌داری می‌کنند.

ثابت‌افزار سامانه‌های نهفته[۳۷۰] معمولاً از طریق رابط اشکال‌زدایی[۳۷۱] به‌روزرسانی می‌شود (مثلاً JTAG). از آنجایی که دستگاه‌های IoT همیشه به یک شبکه متصل هستند، به‌روزرسانی از راه دور امکان‌پذیر است. زمانی که ثابت‌افزاری از راه دور به‌روز می‌شود، احراز هویت جهت جلوگیری از دستکاری غیرمجاز حیاتی است. در روش پیشنهادی فرض شده است که احراز هویت با ابزار موجود حاصل می‌شود. چالش این امر، تعریف فرآیندی برای به‌روزرسانی‌های مشروع ثابت‌افزار از طریق رابط اشکال‌زدایی یا نهاد از راه دور است. تمامی به‌روزرسانی‌های ثابت‌افزار باید توسط ماژول‌های سخت‌افزاری جهت خودبهبودی و زنجیره‌ی بلوکی انجام شود. بعد از احراز هویت به‌روزرسانگر، منطق خودبهبود ثابت‌افزار جدید را از طریق رابط اشکال‌زدایی یا شبکه دریافت می‌کند. سپس حافظه‌ی فلش را به‌روز کرده

[۳۶۸] Redundancy
[۳۶۹] edge computing environment
[۳۷۰] embedded system
[۳۷۱] debugging interface

و RIM را محاسبه می‌کند. RIM، فراداده و ثابت‌افزار جدید در زنجیره‌ی بلوکی و مخازن، توسط سخت‌افزار زنجیره‌ی بلوکی ذخیره می‌شود.

روش تحقیق

در این مقاله به بررسی و مرور مقالاتی در زمینه‌ی روش‌های امنیتی طراحی شده برای IoT یا قابل استفاده در آن پرداخته‌ایم که از ژانویه‌ی سال ۲۰۱۶ به زبان انگلیسی چاپ شده‌اند. بررسی روش‌های حریم شخصی IoT را به مطالعات بعدی موکول می‌کنیم. مقالات انتخابی به دوسته‌ی روش‌های واکنشی[۳۷۲] و پیش‌کنشگری[۳۷۳]، و روش‌های واکنشی را به (۱) سامانه‌های شناسایی نفوذ[۳۷۴] تنها و سامانه‌های پیشگیری از نفوذ و (۲) روش‌های امنیتی مبتنی بر همکاری طبقه‌بندی کرده‌ایم.

منابع

[۱] Q.K.A. Mirza, G. Mohi-Ud-Din, I. Awan, A cloud-based energy efficient system for enhancing the detection and prevention of modern malware, in: ۲۰۱٦ IEEE ۳۰th International Conference on Advanced Information Networking and Applications (AINA), ۲۰۱٦, pp. ۷٥٤–۷٦۱. Crans-Montana.
[۲] F. Cadet, D.T. Fokum, Coping with denial-of-service attacks on the IP telephony system, in: SoutheastCon ۲۰۱٦, ۲۰۱٦, pp. ۱–۷. Norfolk, VA.
[۳] D.H. Sharma, C.A. Dhote, M.M. Potey, Implementing intrusion management as security-as-a-service from cloud, in: ۲۰۱٦ International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), ۲۰۱٦, pp. ۳٦۳–۳٦٦. Bangalore.
[٤] Amos O. Olagunju, Farouk Samu, In search of effective honeypot and honeynet systems for real-time intrusion detection and prevention, in: Proceedings of the ٥th Annual Conference on Research in Information Technology (RIIT '۱٦), ACM, New York, NY, USA, ۲۰۱٦, pp. ٤۱–٤٦.
[٥] M. Yevdokymenko, An adaptive algorithm for detecting and preventing attacks in telecommunication networks, in: ۲۰۱٦ Third International Scientific-practical Conference Problems of Infocommunications Science and Technology (PIC S&T), ۲۰۱٦, pp. ۱۷٥–۱۷۷. Kharkiv.
[٦] M. Ford, et al., A process to transfer Fail۲ban data to an adaptive enterprise intrusion detection and prevention system, in: SoutheastCon ۲۰۱٦, ۲۰۱٦, pp. ۱–٤. Norfolk, vol. A.
[۷] S. Vij, A. Jain, Smartphone nabbing: analysis of intrusion detection and prevention systems, in: ۲۰۱٦ ۳rd International Conference on Computing for Sustainable Global Development (INDIACom), ۲۰۱٦, pp. ۲۲۰۹–۲۲۱٤. New Delhi.
[۸] G. Kalnoor, J. Agarkhed, Pattern matching intrusion detection technique for Wireless Sensor Networks, in: ۲۰۱٦ ۲nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-informatics (AEEICB), ۲۰۱٦, pp. ۷۲٤–۷۲۸. Chennai.
[۹] S. Kumawat, A.K. Sharma, A. Kumawat, Intrusion detection and prevention system using K-learning classification in cloud, in: ۲۰۱٦ ۳rd International Conference on Computing for Sustainable Global Development (INDIACom), ۲۰۱٦, pp. ۸۱٥–۸۲۰. New Delhi.
[۱۰] A. Saracino; D. Sgandurra; G. Dini; F. Martinelli, "MADAM: effective and efficient behavior-based android malware detection and prevention," in IEEE Transactions on Dependable and Secure Computing ,vol.PP, no.vol. ۹۹, pp.۱–۱.
[۱۱] S. Alsunbul, P. Le, J. Tan, B. Srinivasan, A network defense system for detecting and preventing potential hacking attempts, in: ۲۰۱٦ International Conference on Information Networking (ICOIN), ۲۰۱٦, pp. ٤٤۹–٤٥٤. Kota Kinabalu.
[۱۲] J. Filipek, L. Hudec, Securing mobile ad hoc networks using distributed firewall with PKI, in: ۲۰۱٦ IEEE ۱٤th International Symposium on Applied Machine Intelligence and Informatics (SAMI), ۲۰۱٦, pp. ۳۲۱–۳۲٥. Herlany.

[۳۷۲] Reactive
[۳۷۳] Proactive
[۳۷٤] Intrusion Detection Systems (IDS)