عنوان:
اینترنت اشیاء، امنیت و چالش های پیش روی آن

خرداد ۱۳۹۷

مولف:

فرهاد رحمتی

Farhad_rahmati@zoho.com

www.jozve.org

بسم الله الرحمن الرحیم

www.jozve.org

فهرست مطالب

عنوان **صفحه**

چکیده ۱

فصل اول : کلیات تحقیق

۱-۱. مقدمه ۳

۱-۲. اصطلاحات مرتبط ۷

۱-۲-۱. تشخیص نفوذ ۷

۱-۲-۲. اینترنت اشیاء ۸

۱-۳. بررسی کارهای مرتبط ۱۵

فصل دوم : روش های تشخیص نفوذ در اینترنت اشیاء

۲-۱. تشخیص نفوذ در اینترنت اشیاء ۲۲

۲-۲. استراتژی‌های قرار گرفتن IDS ۲۴

۲-۲-۱. قرار گرفتن IDS به صورت توزیع شده ۲۵

۲-۲-۲. قرار گرفتن IDS به صورت متمرکز ۲۷

۲-۲-۳. قرار گرفتن IDS به صورت ترکیبی ۲۸

۲-۳. روش‌های تشخیص ۳۱

۲-۳-۱. رویکردهای مبتنی بر امضا ۳۲

۲-۳-۲. رویکردهای مبتنی بر ناهنجاری ۳۴

۲-۳-۳. رویکردهای مبتنی بر مشخصه ۳۷

۲-۳-۴. رویکردهای ترکیبی ۳۹

فصل سوم : چالش های امنیتی اینترنت اشیا

۳-۱. چالش های امنیتی و انواع حملات در اینترنت اشیاء ۴۲

www.jozve.org

۳-۲. مسائل امنیتی در شبکه های حسگر بیسیم (WSNS) ۴۶
۳-۳. حملات انگار سرویس بر لایه های IOT ۴۷
۳-۳-۱. حمله Dos به لایه فیزیکی: ۴۷
۳-۳-۳.حمله DOS به لایه شبکه ۴۸
۳-۳-۴.حملات DOS در لایه انتقال ۴۹
۳-۳-۵.حملات D05 در لابه کاربرد ۵۰
۳-۴. اهمیت داده در اینترنت اشیاء : ۵۰
۳-۵. نبود استاندارد واحد ۵۲
۳-۶.چالش های اینترنت اشیا ۵۳
۳-۶-۱.چالش حریم خصوصی ۵۳
۳-۶-۲.چالش امنیتی ۵۳
۳-۶-۳.چالش هرج و مرج ۵۴
۳-۷.مشخصه های بسیار مرتبط برای امن کردن اینترنت اشیا ۵۵
۳-۸.فایروال و سیاست های تحرک در اینترنت اشیاء ۵۶

فصل چهارم : نتیجه گیری

۴-۱. نتیجه‌گیری ۶۰
۴-۲. پیشنهادات ۶۱
فهرست منابع و مآخذ ۶۲

www.jozve.org

فهرست جدول ها

عنوان **صفحه**

جدول ۲-۱. خلاصه‌ای از سیستم‌های تشخیص نفوذ برای اینترنت اشیاء که در مقالات مختلف ارائه شده‌اند... ۲۳

www.jozve.org

فهرست شکل ها

عنوان **صفحه**

شکل ۲-۱. دسته‌بندی سیستم‌های تشخیص نفوذ در اینترنت اشیاء..... ۲۲

www.jozve.org

چکیده

اینترنت اشیاء (IoT) الگوی جدیدی است که اینترنت و اشیاء فیزیکی را ادغام می‌کند، اشیائی که به دامنه‌های مختلفی از قبیل اتوماسیون منزل، فرآیندهای صنعتی، نظارت بر سلامت انسان و نظارت محیطی تعلق دارند. اینترنت اشیاء حضور وسایل متصل به اینترنت را در فعالیت‌های روزانه‌ی ما عمیق‌تر می‌کند و مزایای زیادی را به همراه داشته و از طرفی چالش‌های مرتبط با مسائل امنیتی را نیز ایجاد می‌کند. در دهه گذشته، اینترنت اشیاء در مرکز توجهات و تحقیقات زیادی قرار داشته است. امنیت و محرمانه بودن، مسایل مهمی برای کاربردهای IOT بوده و همچنان با چالش های بزرگی مواجه است. معماری های اینترنت اشیاء قرار است با جمعیتی حدود میلیاردها اشیاء سر و کار داشته باشد، که با یکدیگر و با دیگر نهادها، مانند انسان ها و یا نهادهای مجازی تعامل خواهند داشت. همه این تعاملات باید به نحوی محافظت شود، از جمله حفاظت از اطلاعات و تأمین خدمات تمام بازیگران مربوطه و نیز محدود کردن تعداد حوادثی که بر کل اینترنت اشیاء تأثیر می گذارد. با این حال، حفاظت اینترنت اشیاء یک کار پیچیده و دشوار است. تعداد حمله های در دسترس حمله کننده های مخرب با توجه به اتصال جهانی (دسترسی هر کسی) و دسترس پذیری (دسترسی به هر مکان، در هر زمان) به عنوان روندهای اصلی اینترنت اشیاء ممکن است گیج کننده باشند. تهدیداتی که می تواند بر نهادهای اینترنت اشیا تأثیر گذارد متعدد هستند، مانند حملات باهدف کانال های ارتباطی مختلف، تهدیدات فیزیکی، محرومیت از خدمات، ساخت هویت، و غیره. در نهایت، پیچیدگی ذاتی اینترنت اشیاء، که در آن نهادهای ناهمگن متعدد واقع در زمینه های مختلف می توانند اطلاعات را با یکدیگر مبادله کنند، پیچیدگی های بیشتر طراحی و بکارگیری مکانیزم های امنیتی کارآمد، سازگار و مقیاس پذیر را می طلبد. دراین تحقیق به طور خاص روش های تشخیص نفوذ در اینترنت اشیاء و چالش های امنیتی اینترنت اشیا مورد بحث و بررسی قرار گرفته است.

کلمات کلیدی: سیستم تشخیص نفوذ؛ اینترنت اشیاء؛ امنیت سایبری، حملات اینترنتی.

www.jozve.org

فصل اول:

کلیات تحقیق

www.jozve.org

۱-۱. مقدمه

تکامل فناوری‌های مختلف از قبیل حسگرها، شناسایی و ردیابی خودکار، محاسبات نهفته، ارتباطات بی‌سیم، دسترسی باند گسترده به اینترنت و سرویس‌های توزیع شده، پتانسیل ادغام اشیاء هوشمند را در زندگی روزانه‌ی ما از طریق اینترنت افزایش می‌دهد. همگرایی اینترنت و اشیاء هوشمندی که می‌توانند به برقراری ارتباط و تعامل با یکدیگر بپردازند، اینترنت اشیاء[1] (IoT) را تعریف می‌کند. این الگوی جدید به عنوان یکی از مهمترین عوامل در صنعت فناوری اطلاعات و ارتباطات[2] (ICT) در سال‌های آینده تشخیص داده شده است (Miorandi و همکارانش، ۲۰۱۲). به گزارش شرکت Gartner، اینترنت اشیاء ممکن است تا سال ۲۰۲۰ دارای ۲۶ میلیارد واحد باشد. سیستم‌های سیسکو پیش‌بینی کرده‌اند که اینترنت اشیاء بین سال‌های ۲۰۱۳ تا ۲۰۲۲ در نتیجه‌ی ترکیب افزایش درآمد و کاهش هزینه‌ها، در آمد ۱۴.۴ تریلیون دلار ایجاد خواهد کرد (Lee و Lee، ۲۰۱۵؛ Bradley و همکارانش، ۲۰۱۳؛ Sicari و همکارانش، ۲۰۱۵؛ Singh و همکارانش، ۲۰۱۴).

بسیاری از حوزه‌های کاربردی از قبیل تدارکات، فرآیندهای صنعتی، ایمنی عمومی، اتوماسیون منازل، نظارت بر محیط و مراقبت از سلامتی ممکن است با استفاده از سیستم‌های اینترنت اشیاء مزایای قابل توجهی داشته باشند (Borgia، ۲۰۱۴). با این حال، ادغام اشیاء موجود در دنیای واقعی با اینترنت می‌تواند تهدیدات امنیتی سایبری را نیز در بسیاری از فعالیت‌های روزانه‌ی ما به همراه داشته باشد. حملات مختلف علیه زیرساخت‌های حیاتی و مهم از قبیل نیروگاه‌های انرژی و سیستم‌های حمل و نقل ممکن است عواقب بسیار وحشتناکی برای تمام شهرها و کشورها داشته باشد. لوازم خانگی ممکن است یک هدف اولیه برای تهدیدات امنیتی و حریم خصوصی خانواده باشد. در مقاله‌ی Notra و همکارانش (۲۰۱۴)، آزمایش‌های انجام شده بر روی سه دستگاه محبوب خانگی، آسیب‌پذیری‌های مختلفی را در رابطه با حریم خصوصی کاربران، فقدان رمزنگاری و

[1] Internet of Things (IoT)
[2] Information and Communication Technology (ICT)

www.jozve.org

احرازهویت نشان می‌دهد. با توجه به استانداردها و پشته‌های ارتباطی مختلف، توان محدود محاسباتی و تعداد بالای وسایل به هم متصل، اقدامات رایج امنیتی در برابر این تهدیدات نمی‌تواند در سیستم‌های اینترنت اشیاء به طور موثری عمل کند. به همین دلیل، توسعه‌ی راه‌حل‌های امنیتی خاص برای اینترنت اشیاء ضروری است تا به کاربران و سازمان‌ها اجازه دهند تمام نقاط ضعف سیستم را شناسایی کنند (Sicari و همکارانش، ۲۰۱۵).

برخی از پروژه‌های در حال انجام برای ارتقای امنیت اینترنت اشیاء شامل روش‌هایی هستند که محرمانگی داده‌ها و احراز هویت، کنترل دسترسی در داخل شبکه‌ی اینترنت اشیاء، حریم خصوصی و اعتماد میان کاربران و اشیاء، و اجرای سیاست‌های امنیت و حریم خصوصی را ارائه می‌دهند (Sicari و همکارانش، ۲۰۱۵). با این حال، حتی با وجود این روش‌ها نیز شبکه‌های اینترنت اشیاء در برابر حمله‌های متعدد آسیب‌پذیر هستند، حمله‌هایی که با هدف مختل کردن و از بین بردن این شبکه‌ها طراحی می‌شوند. به همین دلیل، یک روش دفاعی دیگر مورد نیاز، طراحی روش‌هایی است که مهاجمان را تشخیص دهند. سیستم‌های تشخیص نفوذ[1] (IDSها) برای انجام این هدف می‌باشند.

IDS یکی از ابزارهای اصلی برای حفاظت از شبکه‌های معمولی و سیستم‌های اطلاعاتی است. IDS به اجرای عملیات در یک میزبان یا یک شبکه نظارت می‌کند و در صورت وقوع یک نقض امنیتی در آن، به سیستم مدیریت هشدار می‌دهد. تلاش‌های تحقیقاتی صورت گرفته در زمینه‌ی تشخیص نفوذ از اوایل دهه ۱۹۸۰ آغاز شده است، وقتی که Anderson (۱۹۸۰) کار اولیه‌ی خود در مورد نظارت بر امنیت شبکه را منتشر نمود. از این رو، سیستم تشخیص نفوذ موقعیت خود را به عنوان یک فناوری دفاعی محبوب برای شبکه‌های IP معمولی مستحکم نموده است، موقعیتی که راه‌حل‌های متعددی را به بازار ارائه کرده است[2و3].

با وجود بلوغ فناوری IDS در شبکه‌های معمولی، راه‌حل‌های رایج برای سیستم‌های اینترنت اشیاء ناکافی هستند، چرا که ویژگی‌های خاص اینترنت اشیاء بر روی توسعه‌ی IDS تاثیر می‌گذارند. اول اینکه، ظرفیت

[1] Intrusion Detection Systems (IDSs)
[2] https://www.sans.org/critical-security-controls/vendor-solutions/control/13
[3] http://www.scmagazine.com/intrusion-detection-systems/products/91/0/

www.jozve.org

پردازشی و ذخیره‌سازی موجود در گره‌های شبکه که عامل‌های IDS را میزبانی می‌کنند، یک مسئله‌ی مهم می‌باشد. مدیر سیستم در شبکه‌های معمولی، عامل‌های IDS را در گره‌هایی مستقر می‌کند که ظرفیت پردازشی بالاتری دارند. شبکه‌های اینترنت اشیاء معمولا از گره‌هایی تشکیل می‌شود که منابع محدودی دارند. از این رو، یافتن گره‌هایی که قابلیت پشتیبانی از عامل‌های IDS را دارند، در سیستم‌های اینترنت اشیاء سخت‌تر است. دومین ویژگی خاص مربوط به معماری شبکه است. در شبکه‌های معمولی، سیستم‌های پایانی به طور مستقیم به گره‌های خاصی (مانند نقاط دسترسی بی‌سیم، سوئیچ‌ها، و مسیریاب‌ها) متصل هستند که مسئولیت هدایت بسته‌ها را به مقصد برعهده دارند. از سوی دیگر، شبکه‌های اینترنت اشیاء معمولا چند گامی[1] هستند. از این رو، گره‌های عادی ممکن است به طور همزمان هم به عنوان هدایت‌کننده‌ی بسته‌ها و هم به عنوان یک سیستم پایانی عمل کنند. به عنوان مثال، در سیستم چراغ‌های روشنایی خیابان که مبتنی بر اینترنت اشیاء هستند، حسگرهایی با قابلیت ارتباطات کوتاه برد بر روی دیرک چراغ مستقر شده‌اند (Pantoni و همکارانش، ۲۰۱۲؛ Elejoste و همکارانش، ۲۰۱۳؛ Shahzad و همکارانش، ۲۰۱۶). سپس، داده‌های جمع‌آوری شده توسط یک حسگر از طریق مسیری از حسگرهای مستقر شده بر روی دیرک‌های چراغ‌های دیگر هدایت می‌شود تا زمانی که به یک دروازه‌ای از اینترنت برسد. این نوع از معماری، چالش‌های جدیدی را برای سیستم‌های تشخیص نفوذ (IDSها) ایجاد می‌کند. آخرین ویژگی خاص مربوط به پروتکل‌های خاص شبکه است. شبکه‌های اینترنت اشیاء از پروتکل‌هایی استفاده می‌کنند که در شبکه‌های معمولی به کار گرفته نمی‌شوند، از قبیل IEEE 802.15.4، IPv6 بر روی شبکه محلی شخصی بی‌سیم[2] (6LoWPAN)، پروتکل مسیریابی IPv6 برای شبکه‌های کم توان و با اتلاف زیاد[3] (RPL) و پروتکل کاربرد محدود[4] (CoAP). پروتکل‌های مختلف باعث ایجاد آسیب‌پذیری‌های جدی شده و تقاضاهای جدیدی را از سیستم تشخیص نفوذ خواهند داشت.

[1] multihop
[2] IPv6 over Low-power Wireless Personal Area Network (6LoWPAN)
[3] IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL)
[4] Constrained Application Protocol (CoAP)

www.jozve.org

با توجه به اینکه توسعه‌ی سیستم‌های تشخیص نفوذ برای اینترنت اشیاء چالش بسیار مهمی را برای محققان امنیت اطلاعاتی ایجاد کرده است، ما به بررسی تشخیص نفوذ در حوزه‌ی اینترنت اشیاء می‌پردازیم. اهداف ما در این بررسی سه قسمت می‌باشند: ۱) یادگیری اینکه چگونه محققان به چالش‌هایی رسیدگی کرده‌اند که ویژگی‌های خاص اینترنت اشیاء برای توسعه‌ی IDS ایجاد می‌کنند؛ ۲) ارائه یک دسته‌بندی از IDSها برای اینترنت اشیاء مطابق با خصیصه‌های زیر: روش تشخیص، استراتژی استقرار IDS، تهدید امنیتی و استراتژی اعتبارسنجی؛ ۳) شناسایی مسائل باز در توسعه‌ی IDS برای اینترنت اشیاء جهت مشخص ساختن مسیرهای تحقیقاتی آینده. از آنجایی که بررسی مقالات مرتبط توسط ما نشان می‌دهد که پژوهش در این حوزه همچنان در مراحل ابتدایی قرار دارد، با این حال ما معتقدیم که مهمترین نوآوری این مقاله، ارائه‌ی بحث مفصلی در مورد مسیرهای تحقیقاتی آینده در سیستم‌های تشخیص نفوذ برای اینترنت اشیاء می‌باشد. ما در مورد مسائل باز مرتبط با عناوینی از قبیل انتخاب روش تشخیص، محدوده‌ی تشخیص حمله، مدیریت و هشدار امنیتی ترافیک، همبستگی هشدارها و بهبود استراتژی‌های اعتبارسنجی در آینده بیشتر بحث خواهیم نمود.

در ادامه این مقاله به صورت زیر سازماندهی شده است. بخش ۲ اصطلاحات مربوط به تشخیص نفوذ و اینترنت اشیاء را معرفی می‌کند. بخش ۳ به بحث در مورد مقالاتی می‌پردازد که به بررسی رویکردهای تشخیص نفوذ برای فناوری‌های مرتبط با اینترنت اشیاء از قبیل شبکه‌های متحرک ادهاک[1] (MANET)، شبکه‌های حسگر بی‌سیم، محاسبات ابری و سیستم‌های فیزیکی سایبری پرداخته‌اند. بخش ۴ دسته‌بندی پیشنهادی و تحلیلی از روش‌های تشخیص نفوذ موجود برای اینترنت اشیاء را ارائه می‌دهد. یکی از مهمترین نوآوری‌های این مقاله، بحث در مورد مسائل باز و فرصت‌های تحقیقاتی آینده در زمینه‌ی سیستم‌های تشخیص نفوذ در اینترنت اشیاء است که در بخش ۵ شرح داده شده‌اند. در نهایت، در بخش ۶ نیز از کلیات مباحث نتیجه‌گیری می‌کنیم.

[1] Mobile Ad hoc Networks (MANETs)

www.jozve.org

۱-۲. اصطلاحات مرتبط

این بخش به معرفی مفاهیم اصلی موجود در این مقاله در زمینه‌ی تشخیص نفوذ و اینترنت اشیاء می‌پردازد.

۱-۲-۱. تشخیص نفوذ

تشخیص نفوذ در واقع انجام اقداماتی جهت تشخیص نفوذگران به داخل سیستم‌های اطلاعاتی است. این اقدامات، که به عنوان نفوذ شناخته می‌شوند، با هدف دسترسی غیرمجاز به سیستم کامپیوتری صورت می‌گیرند. نفوذگران ممکن است کاربران داخلی یا خارجی باشند. نفوذگران داخلی در واقع کاربرانی در داخل شبکه با درجه‌های مختلف اجازه‌ی دسترسی هستند که تلاش می‌کنند درجه‌ی سطح دسترسی و امتیازات خود را برای سوءاستفاده از امتیازات غیرمجاز افزایش دهند. نفوذگران خارجی در واقع کاربرانی خارج از شبکه‌ی هدف هستند که تلاش می‌کنند تا دسترسی غیرمجازی به اطلاعات سیستم داشته باشند (Vacca، ۲۰۱۳؛ Patel و همکارانش، ۲۰۱۰).

یک سیستم تشخیص نفوذ معمولی شامل حسگرها، یک موتور تحلیل، و یک سیستم گزارش‌دهی است. حسگرها در مکان‌ها یا میزبان‌های مختلف شبکه مستقر می‌شوند. وظیفه‌ی این حسگرها جمع‌آوری داده‌های شبکه یا میزبان از قبیل آمارهای ترافیکی، سرآیند بسته‌ها[1]، درخواست‌های سرویس، فراخوان‌های[2] سیستم عامل، و تغییرات سیستم-فایل است. حسگرها داده‌های جمع‌آوری شده را به موتور تحلیل ارسال می‌کنند، که

[1] packet headers
[2] calls

www.jozve.org

مسئولیت بررسی داده‌های جمع‌آوری شده و تشخیص، نفوذهـای در حـال انجـام را دارد. وقتـی موتـور تحلیـل، نفوذی را تشخیص می‌دهد، سیستم گزارش‌دهی هشداری را برای مدیر شبکه تولید می‌کند.

سیستم‌های تشخیص نفوذ (IDSها) می‌توانند به صورت IDS مبتنی بر شبکه[1] (NIDS) و IDS مبتنی بر میزبان[2] (HIDS) دسته‌بندی شوند. IDS مبتنی بر شبکه (NIDS) به یک یا چندین بخش شبکه متصل شـده و ترافیک شبکه را برای کشف فعالیت‌های مخرب نظارت می‌کند. IDS مبتنی بر میزبان (HIDS) به یـک دسـتگاه کامپیوتر متصل شده و به اقدامات مخربی نظارت می‌کند که در داخل سیستم در حال انجـام هسـتند. بـرخلاف NIDS، HIDS نه تنها ترافیک شبکه را تحلیل می‌کند، بلکه همچنین فراخوان‌های سیستمی، اجرای فرآینـدها، تغییرات سیستم-فایل، ارتباطات بین فرآیندها، و گزارش‌های برنامه‌های کاربردی را نیز تحلیل می‌کند.

رویکردهای IDS ممکن است همچنین به صورت مبتنی بر امضـا، مبتنـی بـر ناهنجـاری، یـا مبتنـی بـر مشخصه نیز دسته‌بندی شوند. از آنجا که این دسته‌ها بخشی از طبقه‌بنـدی ارائـه شـده در ایـن مقالـه هسـتند، جزئیات بیشتری از آنها در بخش ۴ ارائه خواهد شد.

۱-۲-۲. اینترنت اشیاء

اینترنت اشیاء مفهومی است که تمام انواع برنامه‌هـای کـاربردی مختلـف را در کنـار یکـدیگر جمـع‌آوری می‌کند تا بر اساس همگرایی اشیاء هوشمند و اینترنت، ادغامی را بـین جهـان فیزیکـی و سـایبری ایجـاد کنـد. محدوده‌ی این برنامه‌های کاربردی ممکن است از یک دستگاه ساده در یک خانه‌ی هوشمند گرفته تا تجهیـزات پیچیده‌ای را در یک کارخانه‌ی صنعتی شامل شوند. اگر چه برنامه‌های کـاربردی اینترنـت اشـیاء اهـداف بسـیار متفاوتی دارند، ولی همه‌ی آنها مشخصات مشترکی را به اشتراک می‌گذارند. به طور کلی، عملیات اینترنت اشیاء

[1] Network-based IDS (NIDS)
[2] Host-based IDS (HIDS)

www.jozve.org

شامل سه مرحله‌ی مجزا است: مرحله‌ی جمع‌آوری، مرحله‌ی انتقال، و مرحله‌ی پردازش، مدیریت و مصرف (Borgia، ۲۰۱۴).

در مرحله‌ی جمع‌آوری، هدف اصلی جمع‌آوری داده‌هایی در مورد محیط فیزیکی است. وسایل و فناوری‌های حس کردن برای ارتباطات کوتاه مدت جهت دستیابی به این هدف ترکیب می‌شوند. وسایلی که در مرحله‌ی جمع‌آوری مورد استفاده قرار می‌گیرند، معمولا کوچک و با منابع محدود هستند. پروتکل‌ها و فناوری‌های ارتباطی که برای این مرحله طراحی می‌شوند، برای اجرا در شرایطی با نرخ‌های محدود داده‌ها و مسافت‌های کوتاه، همچنین با ظرفیت محدود حافظه و مصرف کم انرژی در نظر گرفته می‌شوند. با توجه به این مشخصات، شبکه‌های مربوط به مرحله‌ی جمع‌آوری اغلب با عنوان LLN[1] (شبکه‌های کم توان و با اتلاف زیاد) نامیده می‌شوند. راه‌حل‌هایی برای کنترل خطا، کنترل دسترسی رسانه، مسیریابی و آدرس‌دهی در LLNها ممکن است متفاوت از مواردی باشد که در اینترنت معمولی به کار گرفته می‌شوند.

مرحله‌ی انتقال سعی دارد تا داده‌های جمع‌آوری شده در حین مرحله‌ی جمع‌آوری را به برنامه‌های کاربردی و در نتیجه به کاربران انتقال دهد. در این مرحله، فناوری‌هایی از قبیل Ethernet، WiFi، ترکیب فیبر کواکسیال[2] (HFC) و خط مشترک دیجیتال[3] (DSL) با پروتکل‌های TCP/IP ترکیب می‌شوند تا شبکه‌ای از اتصالات اشیاء و کاربران را در مسافت‌های طولانی ایجاد نماید. دروازه‌ها برای ادغام پروتکل‌های LLN از مرحله‌ی جمع‌آوری با پروتکل‌های معمولی اینترنت از مرحله‌ی انتقال موردنیاز هستند.

در مرحله پردازش، مدیریت و بهره‌برداری، برنامه‌های کاربردی به پردازش داده‌های جمع‌آوری شده می‌پردازند تا اطلاعات مفیدی را در مورد محیط فیزیکی به دست آورند. این برنامه‌های کاربردی ممکن است بر اساس این اطلاعات تصمیم‌گیری کرده، و اشیاء فیزیکی را برای انجام عملیاتی در محیط فیزیکی کنترل کنند.

[1] Low power and Lossy Networks (LLN)
[2] Hybrid Fiber Coaxial (HFC)
[3] Digital Subscriber Line (DSL)

www.jozve.org

این مرحله همچنین شامل یک میان‌افزار است، که مسئولیت کمک به ادغام و ارتباط بین اشیاء فیزیکی مختلف و برنامه‌های کاربردی از بسترهای مختلف را برعهده دارد.

اتحادیه‌ها، کنسرسیوم‌ها، گروه‌های علاقمند ویژه، و سازمان‌های توسعه‌ی استاندارد مقداری زیادی از فناوری‌های ارتباطی را برای اینترنت اشیاء ارائه کرده‌اند، که ممکن است یک چالش بزرگ برای امنیت انتها-به-انتها در کاربردهای اینترنت اشیاء باشد (Meddeb، ۲۰۱۶). از محبوب‌ترین فناوری‌ها برای اینترنت اشیاء عبارتند از: IEEE 802.15.4، بلوتوث با انرژی کم[1] (BLE)، WirelessHART، Z-Wave، LoRaWAN، 6LoWPAN، RPL، CoAP، و MQTT[2] (انتقال مخابراتی صف پیام).

IEEE 802.15.4 استانداردی است که توسط موسسه مهندسان برق و الکترونیک[3] (IEEE) برای لایه‌های فیزیکی و کنترل دسترسی به رسانه در شبکه‌های شخصی بی‌سیم با سرعت کم ارائه شده است. وسایل با استفاده از استاندارد IEEE 802.15.4 می‌توانند با سرعت‌داده‌ها بین ۲۰ کیلوبیت‌برثانیه تا ۲۵۰ کیلوبیت‌برثانیه و محدوده‌ی انتقالی بین ۱۰ متر تا ۱۰۰ متر عمل کنند. کنترل دسترسی به رسانه از روش دسترسی چندگانه با قابلیت شنود سیگنال حامل/ پیشگیری از برخورد (CSMA/CD) استفاده می‌کند (استاندارد IEEE برای شبکه‌های محلی و شهری، بخش ۱۵۴، ۲۰۱۱).

کارگروه مهندسی اینترنت[4] (IEFT) استانداردهایی را برای کار بر روی IEEE 802.15.4 ارائه کرده و ادغام بین شبکه‌های LLN و اینترنت را آسانتر نموده است. استاندارد 6LoWPAN (Hui و Thubert، ۲۰۱۱) قصد دارد تا بسته‌ی IPv6 را با IEEE 802.15.4 تطبیق دهد، زیرا نسخه‌ی قبلی یک سرآیند[5] ۴۰ بایتی داشت و نسخه‌ی آخر نیز تنها اجازه‌ی ۱۲۷ بایت را در هر فریم می‌دهد که شامل سرآیند و اطلاعات بسته هستند. 6LoWPAN به قابلیت همکاری بین گره‌های IPv6 و LLN کمک می‌کند، ولی یک دروازه بین این دو شبکه

[1] Bluetooth Low Energy (BLE)
[2] Message Queue Telemetry Transport (MQTT)
[3] Institute of Electrical and Electronical Engineers (IEEE)
[4] Internet Engineering Task Force (IEFT)
[5] Header

www.jozve.org

همچنان لازم است. گروهی از IEFT که بر روی مسیریابی بر روی شبکه‌های کم توان و با اتلاف[1] (ROLL) کار می‌کنند، یک پروتکل مسیریابی را برای شبکه‌های LLN به نام RPL ارائه کرده‌اند (Winter و همکارانش، ۲۰۱۲). این پروتکل، توپولوژی شبکه حسگر را به صورت گراف‌های جهت‌دار بدون دور مقصدگرا[2] (DODAG) نمایش می‌دهد تا بهترین مسیر را با توجه به یک تابع هدف و برخی معیارها بیابد. این پروتکل از ترافیک نقطه-به-نقطه[3]، چندنقطه-به- نقطه[4] و نقطه-به-چندنقطه[5] پشتیبانی می‌کند.

جامعه‌ی اینترنت اشیاء پروتکل‌هایی را برای لایه‌ی کاربرد نیز ارائه کرده است. پروتکل‌های CoAP و MQTT از پرکاربردترین پروتکل‌های لایه کاربرد در اینترنت اشیاء هستند. گروهی از IEFT که بر روی محیط‌های محدود RESTful[6] (CoRE) کار می‌کنند، پیشنهاد کرده‌اند که CoAP یک پروتکل انتقال (مانند پروتکل انتقال ابَر متن- HTTP) برای شبکه‌های LLN باشد. CoAP اجازه‌ی تراکنش‌های درخواست/پاسخ را در شبکه‌های LLN می‌دهد، مشابه همان صورتی که در وب معمولی رخ می‌دهند، همچنین انتقال داده‌های جمع‌آوری شده را از دستگاه‌ها به کاربران ممکن می‌سازد (Shelby و همکارانش، ۲۰۱۴). MQTT یک پروتکل پیام بر اساس الگوی انتشار-اشتراک[7] است. OASIS[8] (سازمانی برای پیشرفت استانداردهای اطلاعات با ساختار)، یک کنسرسیوم بین‌المللی غیر-انتفاعی است که MQTT را در سال ۲۰۱۳ استاندارد کرده است. این پروتکل به صورت پروتکلی کم حجم و مناسب برای شبکه‌هایی با پیوندهای غیرمطمئن یا پیوندهایی با پهنای باند کم طراحی شده است. سه جزئی که در فرآیند انتشار-اشتراک MQTT نقش دارند، عبارتند از: مشترک، کارگزار، و ناشر. ناشر داده‌ها را به کارگزار ارسال می‌کند. کارگزار لیستی از مشترکینی را دارد که داده‌های مورد علاقه‌ی

[1] Routing over Low Power and Lossy Networks (ROLL)
[2] Destination Oriented Directed Acyclic Graphs (DoDAG)
[3] point-to-point
[4] multipoint-to-point
[5] point-to-multipoint
[6] Constrained RESTful Environments (CoRE)
[7] publish-subscribe
[8] Organization for the Advancement of Structured Information Standards (OASIS)

www.jozve.org

خود را که توسط ناشر ارسال شده‌اند، از کارگزار دریافت می‌کنند (Al-Fuqaha و همکـارانش، ۲۰۱۵؛ Banks و Gupta، ۲۰۱۴).

IEEE 802.15.4، 6LoWPAN، RPL، CoAP، و MQTT استانداردهایی هستند که بـرای رسـیدگی بـه لایه‌های خاصی از پشته‌ی پروتکلی شبکه‌های LLN طراحی شـده‌انـد. بـا ایـن حـال، اسـتانداردهای دیگـری از اینترنت اشیاء وجود دارد که معماری‌های یکپارچه‌ای را به صورت عمـودی مشـخص مـی‌کننـد، از قبیـل BLE، WirelessHART، Z-Wave، و LoRaWAN.

BLE توسط گروه علاقمند ویژه‌ی بلوتوث به عنوان یک تکامل از فناوری بلوتوث برای وسـایل کـم تـوان توسعه داده شده است. وسایل با استفاده از BLE می‌توانند با سرعت ۱ کیلوبیت‌برثانیه در باند ۲.۴ گیگاهرتز کار کنند. فاصله‌ی بین دو گره‌ی BLE حداکثر ۱۰۰ متر است. لایه‌های پایین‌تر در پشـته‌ی پروتکلـی BLE شـامل لایه‌ی فیزیکی و لایه‌ی پیوند است، که لایه‌ی فیزیکی مسئول انتقال بیت‌ها و ماژولاسـیون و لایـه‌ی پیونـد نیـز مسئول کنترل دسترسی به رسانه‌ی انتقال و برقراری اتصال است. هنگامی که لایه پیوند اتصالی را برقرار نمـود، وسایل ممکن است نقش فرمان‌دهنده[1] یا فرمان‌گیرنده[2] را داشته باشند. یک BLE piconet شامل مجموعه‌ای از وسایل فرمان‌گیرنده است که به یک دستگاه فرمان‌دهنده متصل شده‌اند. پروتکل کنترل و تطبیق منطقی پیوند (L2CAP) بر بالای لایه پیوند کار می‌کند. BLE L2CAP نسخه‌ی ساده شده‌ی بلوتوث L2CAP معمولی اسـت که عمدتا مسئولیت پخش کردن داده‌ها را بین لایه‌های بالاتر برعهده دارد. لایـه‌هـای بـالاتر شـامل مشخصـه‌ی ویژگی عمومی[3] (GATT) و مشخصه دسترسی عمـومی[4] (GAP) هسـتند. GATT اجـازه‌ی کشـف سـرویس و تبادل مشخصات را بین دو دستگاه می‌دهد. GAP نیز تعـدادی حالـت عملیـاتی را بـرای وسـایل BLE تعریـف می‌کند (Al-Fuqaha و همکارانش، ۲۰۱۵؛ Gomez و همکارانش، ۲۰۱۲).

[1] master
[2] salve
[3] Generic Attribute Profile (GATT)
[4] Generic Access Profile (GAP)

www.jozve.org

WirelessHART نتیجه‌ی تلاش‌های بنیاد ارتباطات HART در راستای تبدیل پروتکل مبدل بزرگراه قابل آدرس‌دهی از راه‌دور[1] (HART) به یک راه‌حل بی‌سیم می‌باشد. هر دو مورد HART و WirelessHART برای کنترل فرآیند صنعتی طراحی شده‌اند. WirelessHART بر طبق یک ساختار پنج لایه‌ای سازماندهی شده است: لایه‌ی فیزیکی، پیوند، شبکه، انتقال، و کاربردی. لایه‌ی فیزیکی مطابق با لایه‌ی فیزیکی در استاندارد IEEE 802.15.4 مشخص شده است. لایه‌ی پیوند نیز کنترل دسترسی به رسانه‌ی انتقال و اصلاح خطا را پیاده‌سازی می‌کند، که کنترل دسترسی به رسانه بر اساس روش تقسیم زمانی دسترسی چندگانه[2] (TDMA) است. لایه شبکه هسته‌ی اصلی پروتکل WirelessHART است و مسئولیت مسیریابی، کنترل توپولوژی، امنیت انتها-به-انتها و مدیریت نشست را بر عهده دارد. لایه‌ی شبکه در پروتکل WirelessHART از استقرار شبکه‌های مش خود-ترمیم[3] و خود-سازمان‌ده[4] پشتیبانی می‌کند. بر بالای لایه‌ی شبکه، لایه‌ی انتقال قرار دارد که قابلیت اطمینان انتها-به-انتها و کنترل جریان را فراهم می‌کند. در نهایت، لایه‌ی کاربردی بر برنامه‌های کاربردی مبتنی بر فرمان-پاسخ متکی است تا تبادل داده‌ها را میان وسایل و دروازه ممکن سازد (Song و همکارانش، ۲۰۰۸؛ Kim و همکارانش، ۲۰۰۸).

Z-Wave یک معماری پروتکل کم توان برای اتوماسیون منازل و کسب و کارهای کوچک است. این معماری توسط شرکت ZenSys توسعه داده شده، و توسط Z-Wave Alliance ارتقاء یافته است. وسایل Z-Wave در باند ۹۰۰ مگاهرتز کار می‌کنند. نرخ داده‌ها تا ۴۰ کیلوبیت‌برثانیه می‌رسد و حداکثر فاصله بین دو گره نیز حدود ۳۰ متر است. لایه‌ی کنترل دسترسی به رسانه در Z-Wave از روش CSMA/CD استفاده می‌کند و یک روش انتقال مجدد اختیاری برای قابلیت اطمینان دارد. یک شبکه Z-Wave دو نوع وسیله دارد: کنترل‌کننده‌ها و کنترل‌شونده‌ها[5]. کنترل‌کننده‌ها دستورات و درخواست‌هایی را به کنترل‌شونده‌ها ارسال

[1] Highway Addressable Remote Transducer (HART)
[2] Time Division Multiple Access (TDMA)
[3] self-healing
[4] self-organize
[5] slaves

www.jozve.org

می‌کنند، کنترل‌شونده‌ها نیز دستورات را اجرا نموده یا پاسخ‌ها را به کنترل‌کننده‌ها ارسال می‌کنند. مسیریابی در شبکه‌های Z-Wave توسط کنترل‌کننده‌ها انجام می‌شود که جدولی را به همراه اطلاعاتی در مورد توپولوژی کل شبکه نگه می‌دارند. وقتی یک کنترل‌کننده بسته‌ای را ارسال می‌کند، این بسته شامل اطلاعاتی در مورد مسیری است که باید برای بسته دنبال شود (Al-Fuqaha و همکارانش، ۲۰۱۵؛ Gomez و Paradells، ۲۰۱۰).

LoRaWAN یک فناوری توسعه داده شده توسط LoRa Alliance است که یک نهاد غیرانتفاعی می‌باشد. برخلاف فناوری‌هایی از قبیل IEEE 802.15.4، BLE، WirelessHART، و Z-Wave که هدف آنها عملیات در فواصل کوتاه است، LoRaWAN یک فناوری برای شبکه‌های گسترده‌ی کم توان[1] (LPWAN) می‌باشد. در شبکه‌های LoRaWAN، وسایل انتهایی[2] از طریق یک دروازه با یک سرور مرکزی شبکه ارتباط برقرار می‌کنند. وسایل انتهایی از طریق پیوندهای بی‌سیم تک گامی به طور مستقیم به دروازه‌ها متصل هستند، در حالی که دروازه‌ها از شبکه‌های IP معمولی برای اتصال به سرورهای مرکزی استفاده می‌کنند. یک وسیله‌ی انتهایی ممکن است داده‌ای را به چندین دروازه ارسال کند، و سرور شبکه مسئولیت حذف بسته‌های تکراری را دارد. نرخ داده‌ها در هر پایانه ۳ کیلو بیت بر ثانیه الی ۵۰ کیلو بیت بر ثانیه است. فاصله‌ی پوشش داده شده در مناطق شهری ممکن است ۲ کیلومتر الی ۵ کیلومتر باشد، در حالی که در مناطق روستایی و بیرون شهر این فاصله ۱۰ کیلومتر تا ۱۵ کیلومتر است (یک بررسی فنی از LoRa و LoRaWAN، ۲۰۱۵؛ Filho و همکارانش، ۲۰۱۶).

[1] Low Power Wide Area Networks (LPWANs)
[2] End devices

www.jozve.org

۱-۳. بررسی کارهای مرتبط

در طی سال‌های اخیر، مقالات مروری مختلفی بر روی سیستم‌های تشخیص نفوذ در فناوری‌های مرتبط با اینترنت اشیاء از قبیل شبکه‌های ادهاک متحرک (MANETs) (Mishra و همکارانش، ۲۰۱۴؛ Anantvalee و Jie، ۲۰۰۷؛ Kumar و Dutta، ۲۰۱۶)، شبکه‌های حسگر بی‌سیم (WSNs) (Farooqi و Khan، ۲۰۰۹؛ Abduvaliyev و همکارانش، ۲۰۱۳؛ Butun و همکارانش، ۲۰۱۴b)، محاسبات ابری (Modi و همکارانش، ۲۰۱۳)، و سیستم‌های سایبری فیزیکی (Mitchell و Chen، ۲۰۱۴) منتشر شده‌اند.

Mishra و همکارانش (۲۰۰۴) بیان کرده‌اند که استفاده از پژوهش‌های صورت گرفته بر روی شبکه‌های سیمی در شبکه‌های بی‌سیم به دلیل تفاوت‌های بنیادی معماری‌های این دو شبکه کار آسانی نیست، به ویژه اینکه در شبکه‌های بی‌سیم زیرساخت ثابتی نداریم. نویسندگان اظهار می‌دارند که نوع پاسخ به نفوذ در شبکه‌های ادهاک بی‌سیم به نوع نفوذ، پروتکل‌های شبکه و کاربردهای در حال استفاده و میزان اعتماد به شواهد بستگی دارد. برخی از پاسخ‌های احتمالی می‌تواند از جمله راه‌اندازی مجدد کانال‌های ارتباطی بین گره‌ها، شناسایی گره‌های در معرض خطر قرار گرفته و سازماندهی مجدد شبکه برای متوقف کردن گره‌های آسیب دیده و راه‌اندازی یک فرآیند درخواست احراز هویت مجدد از تمام گره‌های موجود در شبکه باشد. نویسندگان همچنین شرح مفصلی از هفت رویکرد IDS پیشنهاد شده برای شبکه‌های MANET را با توجه به روش‌های زیر ارائه داده‌اند: تشخیص ناهنجاری به صورت توزیع شده و تشخیص مبتنی بر عامل متحرک. در هر دو مورد، یک عامل IDS در هر گره‌ی متحرک اجرا می‌شود و جمع‌آوری داده‌های محلی و تشخیص محلی را انجام می‌دهد. تفاوت بین دو روش در تشخیص سراسری است: تشخیص ناهنجاری به صورت توزیع شده از اطلاعات گره‌های همسایه برای ایجاد یک موتور تشخیص مشارکتی استفاده می‌کند، در حالی که تشخیص مبتنی بر عامل متحرک از فناوری عامل‌های متحرک برای تشخیص نفوذ و پاسخ استفاده می‌کند.

www.jozve.org

Anantvalee و Jie (۲۰۰۷) مطالعه‌ای را در مورد زیرساخت شبکه برای IDS در شبکه‌های MANET انجام داده‌اند. نویسندگان سه معماری برای سیستم‌های تشخیص نفوذ در شبکه‌های MANET را شرح داده‌اند: سیستم‌های تشخیص نفوذ به صورت مشارکتی و توزیع شده (زیرساخت شبکه به صورت مسطح)، سیستم‌های تشخیص نفوذ به صورت سلسله‌مراتبی (زیرساخت شبکه به صورت چند لایه)، و عامل‌های متحرک برای سیستم‌های تشخیص نفوذ (زیرساخت شبکه به صورت چند لایه و مسطح). با توجه به ماهیت شبکه‌های MANET، نویسندگان گزارش داده‌اند که تقریبا تمام سیستم‌های تشخیص نفوذ بررسی شده به صورت توزیع شده سازماندهی شده‌اند و یک معماری مشارکتی دارند. این نویسندگان همچنین یک دسته‌بندی از روش‌های تشخیص گره‌های بدرفتار در شبکه‌های MANET را با توجه به معماری، نوع جمع‌آوری داده‌ها، توزیع داده‌ها، مشاهده، تشخیص بد رفتاری، مجازات گره‌های بدرفتار و کشف مسیر ارائه کرده‌اند.

Kumar و Dutta (۲۰۱۶) روش‌های تشخیص نفوذ ارائه شده برای شبکه‌های MANET را با تمرکز بر روی الگوریتم‌های تشخیص آنها بررسی نموده‌اند. نویسندگان یک دسته‌بندی درختی را برای روش‌های تشخیص نفوذ معرفی کرده‌اند که با توجه به ماهیت روش پردازشی استفاده شده در روش تشخیص صورت گرفته است. روش‌های تشخیص نفوذ به دسته‌های مبتنی بر آمار، مبتنی بر روش‌های اکتشافی، مبتنی بر قوانین، مبتنی بر حالت، مبتنی بر امضا، مبتنی بر اعتبار، مبتنی بر اطلاعات مسیریابی، مبتنی بر تقابل لایه‌ای و مبتنی بر نظریه‌ی گراف تقسیم می‌شوند. برای هر روش تشخیص نفوذی که مورد بررسی قرار گرفته است، نویسندگان دسته‌بندی دقیقی از سیستم با توجه به روش تشخیص (سوءرفتار، مبتنی بر ناهنجاری، مبتنی بر مشخصه یا ترکیبی)، معماری (مستقل، توزیع شده و مشارکتی، مبتنی بر عامل متحرک و سیستم تشخیص نفوذ سلسله‌مراتبی)، مدت زمان تشخیص (بی‌درنگ یا به صورت آفلاین)، پروتکل مسیریابی، نوع حمله‌های تشخیص داده شده، عملکرد، تاثیر تحرک، استحکام، انطاف‌پذیری، مقیاس‌پذیری، سرعت، و قابلیت اطمینان ارائه کرده‌اند. علاوه بر این، آنها چالش‌های تحقیقاتی را نیز بر شمرده و مسائل باز موجود در تشخیص نفوذ برای شبکه‌های MANET را نیز

www.jozve.org

مطرح کرده‌اند. هم رفتار نفوذی و هم رفتار خوب و بی‌خطر کاربران، سیستم‌ها، یا شبکه در طول زمان تغییر می‌کند. سیستم تشخیص نفوذ باید به صورت خود-مدیریت شونده[1] و خود-پیکربند[2] باشد تا به تغییرات مداوم محیط پویا رسیدگی کرده و با سرعت به تغییرات پویای منابع سخت‌افزاری و نرم‌افزاری شبکه پاسخ دهد.

Farooqi و Khan (۲۰۰۹) یک دسته‌بندی از سیستم‌های تشخیص نفوذ را برای شبکه‌های حسگر بی‌سیم از نظر نحوه‌ی استقرار عامل IDS در شبکه ارائه کرده‌اند: کاملا توزیع شده (عامل IDS در هر گره‌ی حسگر نصب می‌شود)، کاملا متمرکز (عامل IDS تنها در ایستگاه پایه نصب می‌شود)، و متمرکز-توزیع شده (عامل IDS در برخی از گره‌های ناظر نصب می‌شود). نویسندگان همچنین در مورد ارتباط بین موقعیت عامل IDS در شبکه‌های حسگر بی‌سیم و مصرف انرژی نیز بحث نموده‌اند. آنها به این نتیجه رسیده‌اند که رویکرد IDS متمرکز-توزیع شده برای شبکه‌های حسگر بی‌سیم از لحاظ مصرف توان و پیچیدگی توپولوژی شبکه مناسب‌تر است.

Abduvaliyev و همکارانش (۲۰۱۳) یک دسته‌بندی از سیستم‌های تشخیص نفوذ را برای شبکه‌های حسگر بی‌سیم با توجه به روش تشخیص: تشخیص سوءرفتار، تشخیص ناهنجاری، و تشخیص مبتنی بر مشخصه ارائه کرده‌اند. آنها همچنین شرح مفصلی از روش‌های IDS را با در نظر گرفتن ساختار شبکه‌های حسگر بی‌سیم ارائه کرده، و حوزه‌های حیاتی مختلفی را مطرح نموده‌اند که در حال حاضر توسعه نیافته‌اند. برخی از این حوزه‌ها شامل عدم پیاده‌سازی روش‌های IDS در دنیای واقعی برای شبکه‌های حسگر بی‌سیم و توسعه‌ی روش‌های IDS با در نظر گرفتن دیدگاه اینترنت اشیاء می‌باشند. آنها همچنین به این نتیجه رسیده‌اند، با این که طراحی سیستم‌های تشخیص نفوذ برای شبکه‌های حسگر بی‌سیم در سال‌های اخیر پیشرفت قابل توجهی داشته است، ولی همچنان مسائل تحقیقاتی متعددی (از قبیل معماری‌های IDS، تعادل بین دقت و مصرف منابع، ادغام بهتر روش‌های زیرساخت) وجود دارند که به توسعه‌ی بیشتری در این زمینه‌ها نیاز است.

[1] self-managed
[2] self-configured

www.jozve.org

Butun و همکارانش (۲۰۱۴b) به بررسی گسترده‌ای در مورد سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بی‌سیم پرداخته‌اند. آنها مروری کلی بر سیستم‌های تشخیص نفوذ ارائه شده برای شبکه‌های MANET داشته و کاربردپذیری آنها را در شبکه‌های حسگر بی‌سیم مورد بررسی قرار داده‌اند. بر طبق گفته‌ی نویسندگان، برخی از سیستم‌های تشخیص نفوذ به طور مستقیم در شبکه‌های حسگر بی‌سیم قابل استفاده هستند (دو رویکرد پیشنهادی)، برخی نیز با اصلاحات قابل ملاحظه‌ای قابل استفاده خواهند بود (هفت رویکرد پیشنهادی)، در حالی که باقی موارد نیز به علت الزامات خاص مورد نیاز برای طراحی شبکه‌های حسگر بی‌سیم قابل استفاده در این شبکه‌ها نیستند (هشت رویکرد پیشنهادی). نویسندگان همچنین مقایسه‌ای را بین سیستم‌های تشخیص نفوذ ارائه شده برای شبکه‌های حسگر بی‌سیم با توجه به معماری شبکه و روش تشخیص ارائه کرده‌اند. به علت نیاز به مصرف کم توان در شبکه‌های حسگر بی‌سیم، این مرجع در نهایت مصرف انرژی سیستم‌های تشخیص نفوذ را مطرح می‌کند.

Modi و همکارانش (۲۰۱۳) نفوذهای مختلفی را گزارش کرده‌اند که بر دسترس‌پذیری، محرمانگی، و یکپارچگی در محاسبات ابری تاثیر می‌گذارند. نویسندگان این مرجع، سیستم‌های تشخیص نفوذ استفاده شده در ابر را به سه دسته تقسیم کرده‌اند: فناوری سیستم تشخیص نفوذ (سیستم تشخیص نفوذ مبتنی بر میزبان[1] (HIDS)، سیستم تشخیص نفوذ مبتنی بر شبکه[2] (NIDS)، سیستم تشخیص نفوذ مبتنی بر هایپروایزر و سیستم تشخیص نفوذ توزیع شده[3] (DIDS))، روش تشخیص نفود و موقعیت‌یابی شبکه. آنها همچنین در مورد مزایا و معایب هر پروتکل بحث نموده و چالش‌هایی را شناسایی کرده‌اند تا محاسبات ابری را به صورت بستر قابل اعتمادی برای ارائه‌ی سرویس‌های اینترنت اشیاء در آورند. اکثر روش‌های تشخیص نفوذ ارائه شده برای ابر نمی‌توانند با حمله‌های تکرار شونده در این محیط مقابله کنند، حمله‌هایی از قبیل حمله‌ی افراد داخلی و حمله‌هایی که بر روش ماشین مجازی یا هایپروایزر انجام می‌شوند.

[1] Host-based intrusion detection system (HIDS)
[2] Network-based intrusion detection system (NIDS)
[3] Distributed intrusion detection system (DIDS)

www.jozve.org

بر طبق گفته‌های Mitchell و Chen (۲۰۱۴)، سیستم‌های فیزیکی-سایبری[1] (CPSs) به صورت سیستم‌های با مقیاس بزرگ، پراکنده از نظر جغرافیایی، یکپارچه، ناهمگن و حیاتی هستند که از حسگرها، محرک‌ها، و اجزای کنترلی و شبکه‌بندی[2] تشکیل شده‌اند. نویسندگان یک دسته‌بندی از سیستم‌های تشخیص نفوذ مدرن را برای سیستم‌های فیزیکی-سایبری بر اساس ابعاد طراحی ارائه کرده‌اند: روش تشخیص و مفاد بازرسی[3] (بر اساس میزبان یا بر اساس شبکه). در ابتدا، آنها تحلیل جامعی از تفاوت‌های موجود بین سیستم‌های تشخیص نفوذ معمولی و سیستم‌های تشخیص نفوذ ارائه شده برای سیستم‌های فیزیکی-سایبری ارائه کرده‌اند، که شامل نوع برخورد با نظارت بر فرآیند فیزیکی، حملات پیچیده، و فناوری‌های ارثی هستند. سپس، نویسندگان این مرجع به خلاصه‌سازی کارهای موجود در سیستم‌های تشخیص نفوذ ارائه شده برای سیستم‌های فیزیکی-سایبری از لحاظ کاربرد در سیستم‌های سایبری-فیزیکی، نوع حمله، ویژگی‌های بازرسی و کیفیت مجموعه‌دادگان پرداخته‌اند. این نویسندگان همچنین چالش‌های تحقیقاتی در این زمینه را بر شمرده و مسیرهای تحقیقاتی آینده را در زمینه‌ی سیستم‌های تشخیص نفوذ برای سیستم‌های فیزیکی-سایبری مطرح نموده‌اند.

اگر چه این مقالات عمدتا بر روی طراحی سیستم‌های تشخیص نفوذ برای عناصر مربوط به اینترنت اشیاء تمرکز دارند، ولی هیچ یک از آنها مطالعه‌ای بر روی روش‌های خاص سیستم‌های تشخیص نفوذ برای الگوی اینترنت اشیاء را انجام نداده‌اند. در این مقاله‌ی مروری، ما بر روی استراتژی‌های قرارگیری و روش‌های تشخیص در سیستم‌های تشخیص نفوذی بحث می‌کنیم که به طور خاص برای اینترنت اشیاء طراحی شده‌اند. ما همچنین تهدیدات رایج برای امنیت اینترنت اشیاء را ارائه کرده و در این مورد بحث می‌کنیم که سیستم‌های تشخیص نفوذ چگونه برای تشخیص این تهدیدات ممکن است مورد استفاده قرار بگیرند. علاوه بر این، ما مروری بر روی

[1] Cyber-Physical Systems (CPSs)
[2] networking
[3] audit material

www.jozve.org

انواع استراتژی‌های اعتبارسنجی به کار رفته در روش‌های تشخیص نفوذ برای اینترنـت اشـیاء داشـته و بـر روی مسائل باز تحقیقاتی و مسیرهای تحقیقاتی آینده بحث می‌کنیم.

www.jozve.org

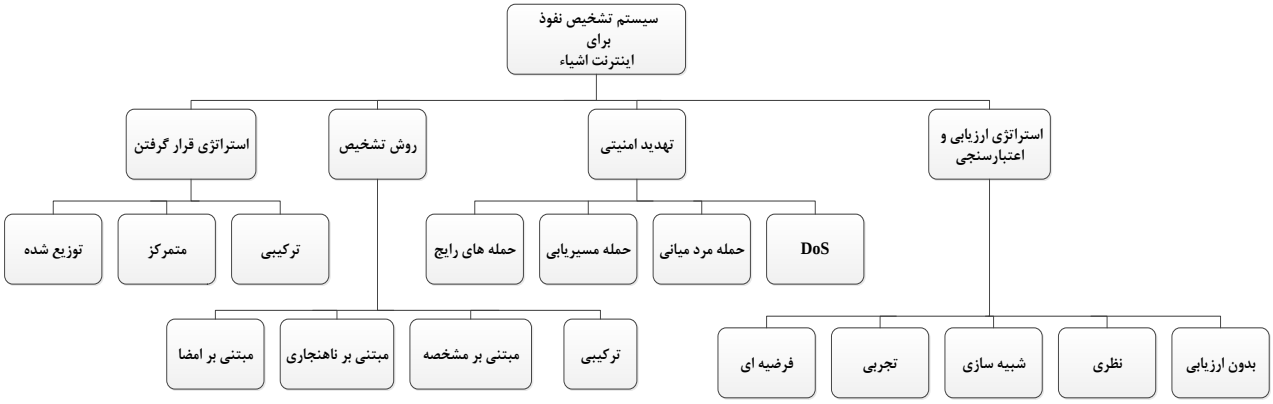
فصل دوم:

روش های تشخیص نفوذ در اینترنت اشیاء

www.jozve.org

۲-۱. تشخیص نفوذ در اینترنت اشیاء

در این بخش، ما به بررسی مفاهیم و مقالات مرتبط با تشخیص نفوذ در اینترنت اشیاء می‌پردازیم. هر مقاله با توجه به ویژگی‌های زیر دسته‌بندی شده است: استراتژی‌های قرار گرفتن IDS، روش تشخیص، تهدیدات امنیتی و استراتژی اعتبارسنجی. شکل ۱ دسته‌بندی پیشنهادی را برای تشخیص نفوذ در اینترنت اشیاء نشان داده و جدول ۱ نیز خلاصه‌ای از تلاش‌های انجام شده جهت طراحی تشخیص نفوذ سیستم برای اینترنت اشیاء را ارائه می‌دهد (علامت "–" برای یک ویژگی نامشخص به کار رفته است.).



شکل ۲-۱. دسته‌بندی سیستم‌های تشخیص نفوذ در اینترنت اشیاء.

www.jozve.org

جدول ۲-۱. خلاصه‌ای از سیستم‌های تشخیص نفوذ برای اینترنت اشیاء که در مقالات مختلف ارائه شده‌اند.

مراجع	استراتژی استقرار	روش تشخیص	تهدید امنیتی	استراتژی اعتبارسنجی
Cho و همکارانش (۲۰۰۹)	متمرکز	مبتنی بر ناهنجاری	حمله مرد میانی	شبیه‌سازی
Liu و همکارانش (۲۰۱۱)	-	مبتنی بر امضا	-	ارزیابی نشده است.
Le و همکارانش (۲۰۱۱)	ترکیبی	مبتنی بر مشخصه	حمله مسیریابی	ارزیابی نشده است.
Misra و همکارانش (۲۰۱۱)	-	مبتنی بر مشخصه	DoS	شبیه‌سازی
Kasinathan و همکارانش (۲۰۱۳a)	متمرکز	مبتنی بر امضا	DoS	تجربی
Wallgren و همکارانش (۲۰۱۳)	متمرکز	-	حمله مسیریابی	شبیه‌سازی
Reza و همکارانش (۲۰۱۳)	ترکیبی	ترکیبی	حمله مسیریابی	شبیه‌سازی
Gupta و همکارانش (۲۰۱۳)	-	مبتنی بر ناهنجاری	-	ارزیابی نشده است.
Kasinathan و همکارانش (۲۰۱۳b)	متمرکز	مبتنی بر امضا	-	مثال فرضیه‌ای
Amaral و همکارانش (۲۰۱۴)	ترکیبی	مبتنی بر مشخصه	-	تجربی
Oh و همکارانش (۲۰۱۴)	توزیع شده	مبتنی بر امضا	چندین حمله‌ی متداول (پایگاه‌داده‌های Snort و Clamav)	تجربی
Lee و همکارانش (۲۰۱۴)	توزیع شده	مبتنی بر ناهنجاری	DoS	شبیه‌سازی
Krimmling و Peter (۲۰۱۴)	-	ترکیبی	حمله مسیریابی و مرد میانی	شبیه‌سازی
Cervantes و همکارانش (۲۰۱۵)	توزیع شده	ترکیبی	حمله مسیریابی	شبیه‌سازی
Summerville و همکارانش (۲۰۱۵)	-	مبتنی بر ناهنجاری	حمله‌های رایج	تجربی
Thanigaivelan و همکارانش (۲۰۱۶)	ترکیبی	مبتنی بر ناهنجاری	-	ارزیابی نشده است.
Le و همکارانش (۲۰۱۶)	ترکیبی	مبتنی بر مشخصه	حمله مسیریابی	شبیه‌سازی
Pongle و Chavan (۲۰۱۵)	ترکیبی	مبتنی بر ناهنجاری	حمله مسیریابی	شبیه‌سازی

www.jozve.org

۲-۲. استراتژی‌های قرار گرفتن IDS

پیش از آغاز بحث در مورد استراتژی‌های استقرار سیستم‌های تشخیص نفوذ در شبکه‌های اینترنت اشیاء، لازم است که مروری بر معماری شبکه‌های اینترنت اشیاء و عناصر اصلی بخش‌های آن ارائه شود.

در سال‌های اخیر، محققان معماری‌های مختلفی را برای اینترنت اشیاء نشان داده‌اند (Bandyopadhyay و Sen، ۲۰۱۱؛ Khan و همکارانش، ۲۰۱۲؛ Han و همکارانش؛ ۲۰۱۳؛ ETSI، ۲۰۱۱)، که به شدت به مراحل جمع‌آوری، انتقال، و پردازش، مدیریت و بهره‌برداری وابسته هستند، مراحلی که در بخش ۲-۲ ارائه شده‌اند. اگر چه این روش‌های ارائه شده در برخی جنبه‌ها تفاوت دارند، ولی تمام این روش‌ها در سه دامنه‌ی گسترده سناریوهای اینترنت اشیاء را سازماندهی می‌کنند: دامنه‌ی فیزیکی، دامنه‌ی شبکه، و دامنه‌ی کاربردی. دامنه‌ی فیزیکی مربوط به مرحله‌ی جمع‌آوری است و شامل وسایلی می‌باشد که محیط فیزیکی را حس کرده و در آن فعالیت می‌کنند و اغلب یک LLN را تشکیل می‌دهند. دامنه‌ی شبکه که بر مرحله‌ی انتقال متکی است، راه‌حل‌ها و پروتکل‌های متداول شبکه را برای انتقال داده‌ها از محیط فیزیکی به برنامه‌های کاربردی و کاربران در کنار هم گردآوری می‌کند. یک مسیریاب مرزی لازم است که بین دامنه‌های شبکه و فیزیکی قرار بگیرد تا پروتکل‌های LLN موجود در لایه‌ی فیزیکی را با پروتکل‌های متداول در دامنه‌ی شبکه ادغام و یکپارچه نماید. در نهایت، دامنه‌ی کاربردی شامل واسطهایی است که به کاربران اجازه می‌دهد تا به اشیاء موجود در دامنه‌ی فیزیکی رسیدگی کنند.

در شبکه‌های اینترنت اشیاء، سیستم تشخیص نفوذ می‌تواند در مسیریاب مرزی، در یک یا چند میزبان اختصاصی، یا در هر شئ فیزیکی قرار بگیرد. مزیت قرار گرفتن سیستم تشخیص نفوذ در مسیریاب مرزی، تشخیص حملات نفوذی از اینترنت بر روی اشیاء موجود در دامنه‌ی فیزیکی است. با این حال، یک سیستم

www.jozve.org

تشخیص نفوذ در مسیریاب مرزی ممکن است سربار ارتباطی بین گره‌های LLN و مسیریاب مرزی ایجاد کند، چرا که سیستم تشخیص نفوذ به صورت مکرر از وضعیت شبکه پرس و جو می‌کند. قرار گرفتن سیستم تشخیص نفوذ در گره‌های LLN ممکن است سربار ارتباطی وابسته به نظارت شبکه را کاهش دهد، ولی منابع (پردازشی، ذخیره‌سازی، و انرژی) بیشتری از گره‌ها را نیاز دارد (Wallgren و همکارانش، ۲۰۱۳). این عمل ممکن است به علت محدودیت منابع در گره‌های LLN خود به یک مشکل تبدیل شود. توزیع عامل‌های تشخیص نفوذ در میان برخی از گره‌های اختصاصی نیز ممکن است یک راه‌حل برای نظارت کمتر ترافیک و حجم پردازشی بیشتر باشد. با این حال، این راه‌حل نیاز به سازماندهی شبکه به مناطق مختلف دارد که این مورد نیز ممکن است خود به یک چالش تبدیل شود.

بخش‌های زیر در ادامه سه استراتژی ممکن برای قرار گرفتن سیستم‌های تشخیص نفوذ و همچنین مزایا و معایب هر یک از آنها را شرح می‌دهد.

۲-۲-۱. قرار گرفتن IDS به صورت توزیع شده

در این استراتژی قرارگیری، سیستم‌های تشخیص نفوذ در هر شئ فیزیکی در LLN (شبکه‌های کم توان و با اتلاف زیاد) قرار داده می‌شوند. سیستم تشخیص نفوذ مستقر شده در هر گره باید بهینه باشد، چرا که این گره‌ها منابع محدودی دارند. برای رسیدگی به این مسئله، Oh و همکارانش (۲۰۱۴) و همچنین Lee و همکارانش (۲۰۱۴) سیستم‌های تشخیص نفوذ توزیع شده‌ی کم حجمی[1] (سبک وزنی) را ارائه کرده‌اند. Oh و همکارانش الگوریتم کم حجمی را برای تطبیق امضاهای حمله و بار[2] بسته‌ها تعریف نموده‌اند. آنها دو روش به نام‌های تغییر کمکی و تشخیص زودهنگام را پیشنهاد کرده‌اند که هدف اصلی آنها کاهش تعداد انطباق‌های مورد

[1] lightweight
[2] payload

www.jozve.org

نیاز برای تشخیص حمله است. آنها رویکرد خود را بـا الگـوریتم Wu-Manber (WM) مقایسـه نمـوده‌انـد، کـه الگوریتم WM یکی از سریعترین الگوریتم‌های انطباق الگو می‌باشد. طبق گفتـه‌ی نویسـندگان ایـن مرجـع، در حین اجرا بر روی یک بستر با منابع محدود، روش پیشنهادی آنها سریعتر از الگوریتم Wu-Manber اسـت. Lee و همکارانش نیز به نوبه‌ی خود یک روش کم حجم را پیشنهاد داده‌اند که مصرف انرژی گـره را بـرای تشـخیص نفوذگران نظارت می‌کند. نویسندگان این مرجع با تمرکز بر روی تنهـا یـک پـارامتر گـره، سـعی در بـه حـداقل رساندن منابع محاسباتی مورد نیاز برای تشخیص نفوذ را داشته‌اند.

در قرارگیری توزیع شده، گره‌ها ممکن است همچنین مسئولیت نظارت همسـایگان خـود را نیـز برعهـده داشته باشند. گره‌هایی که همسایگان خود را نظارت می‌کننـد بـا نـام نگهبـان (watchdog) نامیـده مـی‌شـوند. Cervantes و همکـارانش (۲۰۱۵) راه‌حلـی را بـه نـام INTI[1] (تشـخیص نفـوذ حمـلات Sinkhole بـر روی 6LoWPAN برای اینترنت اشیاء) ارائه کرده‌اند که برای تشخیص و کاهش حملات، مفاهیم اعتماد و اعتبار را با مفهوم نگهبان‌ها ترکیب نموده‌اند. در ابتدا، گره‌ها به صورت گره‌های رهبر، وابسته یا عضو دسته‌بندی شده و یک ساختار سلسله‌مراتبی را ایجاد می‌کنند. نقش هر گره می‌تواند در طول زمان با توجه به پیکربندی مجدد شبکه یا یک رویداد حمله تغییر کند. سپس، هر گره به وسیله‌ی ارزیابی ترافیک ورودی و خروجی گره‌ی مافوق خود بـه نظارت این گره می‌پردازد. وقتی یک گره حمله‌ای را تشخیص می‌دهد، این گره پیامی را جهت هشدار بـه دیگـر گره‌ها پخش می‌کند و مهاجم را نیز ایزوله می‌کند (جدا می‌کند). نویسـندگان در مـورد تـاثیر راه‌حـل خـود در گره‌های با ظرفیت کم بحث نکرده‌اند.

[1] Intrusion detection Sinkhole attacks on 6LoWPAN for Internet of ThIngs (INTI)

www.jozve.org

۲-۲-۲. قرار گرفتن IDS به صورت متمرکز

در قرار گرفتن IDS به صورت متمرکز، سیستم تشخیص نفوذ در یک جزء متمرکز قرار می‌گیرد، به عنوان مثال در یک مسیریاب مرزی یا یک میزبان اختصاصی مستقر می‌شود. تمام داده‌هایی که گره‌های LLN جمع‌آوری می‌کنند، از طریق مسیریاب مرزی به اینترنت انتقال می‌دهند و همچنین تمام درخواست‌های کاربران اینترنتی نیز از طریق مسیریاب مرزی به گره‌های LLN ارسال می‌شود. بنابراین، سیستم تشخیص نفوذ قرار گرفته در یک مسیریاب مرزی می‌تواند به تحلیل تمام ترافیک مبادله شده بین LLN و اینترنت بپردازد (Reza و همکارانش، ۲۰۱۳؛ Farooqi و Khan، ۲۰۰۹). با این حال، تحلیل ترافیکی که از مسیریاب مرزی عبور می‌کند، برای تشخیص حمله‌ها کافی نیست، حمله‌هایی که تنها گره‌های داخل LLN را شامل می‌شوند. سپس، محققان به طراحی سیستم‌های تشخیص نفوذی پرداختند که می‌توانند ترافیک مبادله شده بین گره‌های LLN را نظارت نمایند، بدون اینکه عملیات نظارت تاثیری بر عملکرد گره‌های کم ظرفیت داشته باشد. همچنین، IDS متمرکز ممکن است با نظارت بر گره‌ها در حین یک حمله مشکل داشته باشد، حمله‌ایی که بخشی از شبکه را در معرض خطر قرار می‌دهد.

Cho و همکارانش (۲۰۰۹) راه‌حلی را برای تحلیل بسته‌هایی ارائه داده‌اند که از مسیریاب مرزی بین دامنه‌ی فیزیکی و شبکه عبور می‌کنند. راه‌حل آنها بر روی حمله‌های بات‌نت تمرکز دارد و این امر علت انتخاب آنها را نشان می‌دهد که چرا تنها بر ترافیک مسیریاب مرزی نظارت می‌کنند. Kasinathan و همکارانش (۲۰۱۳a، ۲۰۱۳b) نیز از قرار گرفتن متمرکز سیستم تشخیص نفوذ استفاده کرده‌اند، ولی آنها محافظت از IDS را در برابر یک حمله‌ی DoS[1] (انکار سرویس) در نظر گرفته‌اند. از این رو، نویسندگان این مرجع تصمیم گرفتند تا موتور تحلیل IDS و سیستم گزارش‌دهی IDS را در یک میزبان اختصاصی قدرتمند قرار دهند. آنها

[1] Denial of Service (DoS)

www.jozve.org

حسگرهای IDS را در LLN قرار داده‌اند، حسگرهایی که مسئولیت نظارت بر ترافیک شبکه و ارسال این داده‌ها را به موتور تحلیل IDS دارند. میزبان اختصاصی IDS به صورت سیمی به حسگرهای IDS متصل شده است که این امر از انتقال داده‌های IDS و داده‌های شبکه‌های معمولی بر روی یک شبکه‌ی بی‌سیم یکسان جلوگیری می‌کند. بنابراین، اگر یک حمله‌ی DoS باعث کاهش کیفیت انتقال شبکه‌ی بی‌سیم شود، آنگاه داده‌های IDS تحت تاثیر این حمله قرار نخواهند گرفت.

Wallgren و همکارانش (۲۰۱۳) یک رویکرد متمرکز ارائه کرده‌اند که در آن سیستم تشخیص نفوذ در مسیریاب مرزی قرار گرفته است. هدف از این راه‌حل پیشنهادی، تشخیص حمله‌های داخل دامنه‌ی فیزیکی است. نویسندگان در این مرجع به جای نظارت بر ترافیک عبوری از مسیریاب مرزی، یک پروتکل ضربان قلب[1] را پیشنهاد داده‌اند. بر طبق این پروتکل پیشنهادی، مسیریاب مرزی در بازه‌های زمانی منظمی درخواست‌های اکوی ICMPv6 را به تمام گره‌های LLN ارسال می‌کند و منتظر پاسخ‌ها می‌ماند تا حمله‌ها یا مسائل دسترس‌پذیری را تشخیص دهد. اگر چه این راه‌حل باعث ایجاد ترافیک اضافی در شبکه می‌شود، ولی نویسندگان در آزمایش‌های خود نشان داده‌اند که گره‌های LLN برای اجرای الگوریتم ضربان قلب نیازی به تخصیص حافظه‌ی اضافی ندارند، و سربار انرژی نیز در این روش به حداقل کاهش یافته است.

۲-۲-۳. قرار گرفتن IDS به صورت ترکیبی

قرار گرفتن سیستم تشخیص نفوذ به صورت ترکیبی در واقع مفاهیم قرار گرفتن به صورت متمرکز و توزیع شده را ترکیب می‌کند تا از مزایای آنها بهره برده و از نقاط ضعف آنها پیشگیری کند.

اولین رویکرد برای قرار گرفتن ترکیبی، شبکه را به خوشه‌ها یا مناطقی تقسیم کرده و سازماندهی می‌کند، و فقط گره‌ی اصلی هر خوشه یک نمونه از سیستم تشخیص نفوذ را میزبانی می‌نماید. سپس، این گره

[1] heartbeat protocol

www.jozve.org

مسئول نظارت به دیگر گره‌های عضو خوشه‌ی خود می‌شود. در نگاه اول، این تعاریف مطابق روش ارائه شده توسط Cervantes و همکارانش (۲۰۱۵) دیدیه می‌شود که در بخش ۴-۱-۱ به عنوان مثالی برای قرار گرفتن توزیع شده ارائه شد. اگر چه رویکرد Cervantes و همکارانش شبکه‌ها را به خوشه‌هایی تقسیم کرده و برای هر خوشه نیز یک سرخوشه انتخاب می‌کند، و هر گره‌ای، چه سرخوشه باشد یا نباشد، می‌تواند بر همسایگان خود نظارت کند. ولی در رویکردهای ترکیبی، تنها گره‌های انتخاب شده‌ای که اغلب گره‌های قوی‌تر هستند، نمونه‌های IDS را میزبانی می‌کنند. از این رو، قرار گرفتن سیستم‌های تشخیص نفوذ به صورت ترکیبی ممکن است برای مصرف منابع بیشتری نسبت به قرار گرفتن IDSها به صورت توزیع شده طراحی شده باشند.

Amaral و همکارانش (۲۰۱۴) سیستم تشخیص نفوذی را برای اینترنت اشیاء با استفاده از این رویکرد ارائه کرده‌اند. گره‌های انتخاب شده در شبکه در این مرجع، یک سیستم تشخیص نفوذ را میزبانی می‌کنند. این گره‌های انتخاب شده (نظارت‌کنندگان[1]) سعی دارند تا نفوذ را به وسیله‌ی شنود بسته‌های رد و بدل شده در همسایگی خود شناسایی کند. یک نظارت کننده بر طبق مجموعه‌ای از قوانین در مورد به خطر افتادن یک گره تصمیم می‌گیرد. هر نظارت کننده یک مجموعه‌ی خاصی از قوانین دارد، زیرا هر جزء موجود در شبکه ممکن است یک رفتار متفاوتی داشته باشد. به عنوان مثال، یک مسیریاب مرزی معمولا پیام‌های بیشتری را نسبت به یک گره‌ی معمولی دریافت می‌کند. مزیت این رویکرد این است که اجازه‌ی ایجاد مجموعه قوانین متفاوتی را برای مناطق مختلف شبکه می‌دهد.

Le و همکارانش (۲۰۱۱) نیز رویکردی برای سازماندهی شبکه به مناطق مختلف ارائه کرده‌اند. آنها از قرار گرفتن ترکیبی برای ایجاد ستون فقراتی از گره‌های ناظر استفاده کرده‌اند. با حداقل تعداد گره‌های ناظری که کل شبکه را پوشش می‌دهند، یک گره‌ی ناظر به ارتباطات همسایگان خود گوش می‌دهد (شنود می‌کند) و مشخص می‌کند که یک گره در معرض خطر قرار دارد یا خیر. مزیت این راه‌حل این است که سربار ارتباطی

[1] watchdogs

www.jozve.org

تولید نمی‌کند، زیرا گره‌های ناظر تنها به انتقال‌های میان همسایگان خود گوش می‌دهند. در کار جدیدتری، Le و همکارانش (۲۰۱۶) شبکه را به خوشه‌های کوچکی با تعداد گره‌های مشابه تقسیم و سازماندهی می‌کنند. هر خوشه یک گره‌ی سرخوشه دارد، که ارتباط مستقیمی با تمام اعضای خوشه دارد. یک نمونه‌ی IDS در هر سرخوشه قرار می‌گیرد تا سرخوشه با استفاده از شنود ارتباطات اعضای خوشه بر آنها نظارت داشته باشد. اعضای خوشه باید اطلاعات مربوط به خود و دیگر همسایگان را سرخوشه گزارش دهند. اگر چه نویسندگان سرخوشه را به عنوان یک گره‌ی قوی‌تر در نظر گرفته‌اند، ولی آنها طراحی یک راه‌حل کم‌حجم و سبک[1] از IDS را انتخاب کرده‌اند.

در رویکرد دوم برای قرار گرفتن ترکیبی، ماژول‌های IDS هم در مسیریاب مرزی و هم در دیگر گره‌های شبکه قرار می‌گیرند. تفاوت اصلی این رویکرد با رویکرد اول، حضور یک جزء مرکزی است. ماژول‌های IDS در مسیریاب مرزی مسئول انجام وظایفی هستند که ظرفیت منابع بیشتری را می‌طلبند، درحالی که ماژول‌های IDS در گره‌های معمولی اغلب به صورت سبک و کم حجم می‌باشند. Reza و همکارانش (۲۰۱۳) سیستم تشخیص نفوذی را به نام SVELTE ارائه کرده‌اند. مسیریاب مرزی در این سیستم، ماژول‌های IDSایی را میزبانی می‌کند که نیاز به فرآیندهای پیچیده و بیشتری دارند مانند مسئولیت تشخیص نفوذها با استفاده از تحلیل داده‌های شبکه RPL. گره‌های شبکه مسئولیت انجام وظایف سبک‌تر مانند ارسال داده‌های شبکه RPL به مسیریاب مرزی و اطلاع‌رسانی مسیریاب مرزی در مورد ترافیک مخرب دریافت شده را بر عهده دارند.

در مرجع Pongle و Chavan (۲۰۱۵)، گره‌های شبکه مسئولیت تشخیص تغییرات در همسایگی خود و ارسال اطلاعاتی در مورد همسایگان خود به ماژول‌های متمرکز را بر عهده دارند، ماژول‌های متمرکز در مسیریاب مرزی مستقر شده‌اند. ماژول‌های مترکز، به نوبه‌ی خود، مسئولیت ذخیره و تحلیل این داده‌ها را برای تشخیص نفوذها و شناسایی حمله‌های ممکن بر عهده دارند. اگر چه تشریح این سیستم تشخیص نفوذ ممکن است یک

[1] lightweight

www.jozve.org

معماری را نشان دهد که به ترافیک شدیدی برای تشخیص نفوذ نیاز دارد، ولی نتایج نشان می‌دهند که سربار انرژی، سربار بسته، و مصرف حافظه برای محیطی با گره‌هایی با منابع محدود نیز مناسب است.

Thanigaivelan و همکارانش (۲۰۱۶) یک سیستم تشخیص نفوذی ارائه کرده‌اند که مسئولیت‌های مختلفی را به مسیریاب‌های مرزی و گره‌های شبکه اختصاص می‌دهد، و باعث می‌شود که آنها با هم همکاری کنند. ماژول سیستم تشخیص نفوذ واقع در گره به نظارت بر همسایگان گره پرداخته، و نفوذهای ممکن را تشخیص می‌دهد. وقتی رویدادی تشخیص داده می‌شود، آنگاه گره یک پیام هشدار را به ماژول سیستم تشخیص نفوذی ارسال می‌کند که بر روی مسیریاب مرزی واقع است. سپس، ماژول مسیریاب مرزی پیام‌های هشدار دریافت شده از گره‌های مختلف را به یکدیگر مرتبط نموده و با توجه به آنها در مورد نفوذ صورت گرفته تصمیم‌گیری می‌کند. با اینکه Thanigaivelan و همکارانش سیستم تشخیص نفوذ خود را به عنوان یک IDS توزیع شده دسته‌بندی نموده‌اند. ولی، نقش مرکزی مسیریاب مرزی در گرفتن تصمیم نهایی در مورد تشخیص نفوذ باعث می‌شود که این سیستم IDS پیشنهادی در واقع یکر رویکرد ترکیبی تلقی شود.

۲-۳. روش‌های تشخیص

روش‌های تشخیص نفوذ بسته به مکانیزم تشخیص استفاده شده در سیستم به چهار دسته تقسیم می‌شوند: مبتنی بر ناهنجاری، مبتنی بر امضا، مبتنی بر مشخصه، و روش ترکیبی.

www.jozve.org

۲-۳-۱. رویکردهای مبتنی بر امضا

در رویکردهای مبتنی بر امضا، IDSها وقتی حملات را تشخیص می‌دهند که رفتار سیستم یا شبکه با امضای حمله‌ای مطابقت داشته باشد که این امضاها در پایگاه‌داده‌های داخلی IDS ذخیره شده‌اند. اگر هر گونه فعالیت سیستم یا شبکه با امضاها / الگوهای ذخیره شده مطابقت داشته باشد، آنگاه هشداری فعال خواهد شد.

سیستم‌های تشخیص نفوذ مبتنی بر امضا در تشخیص تهدیدات شناخته شده بسیار دقیق و موثر هستند، و طرز کار آنها نیز جهت درک بسیار آسان است. با این حال، این رویکرد برای شناسایی حمله‌های جدید و انواع گوناگون حمله های شناخته شده ناکارآمد است، زیرا از آنجایی که سیستم تشخیص نفوذ امضای این گونه حمله‌ها را در پایگاه‌داده‌ی خود ندارد و به همین دلیل نمی‌تواند یک تطابق امضا برای رفتار سیستم با این حمله‌ها بیابد (Vacca، ۲۰۱۳؛ Liao و همکارانش، ۲۰۱۳).

در مرجع Liu و همکارانش (۲۰۱۱)، نویسندگان این مرجع یک سیستم تشخیص نفوذ مبتنی بر امضا را ارائه کرده‌اند که از روش‌های سیستم ایمنی مصنوعی استفاده می‌کند. تشخیص‌دهنده‌هایی که امضای حمله‌ها را دارند، به عنوان سلول‌های ایمنی مدل شده‌اند که قابلیت دسته‌بندی دیتاگرام‌ها را به عنوان سلول مخرب (عنصر غیر-خودی) یا سلول عادی (عنصر خودی) دارند. علاوه بر این، تشخیص‌دهنده‌ها می‌توانند برای سازگاری با شرایط جدید در محیط نظارت شده توسعه یابند. این مرجع در مورد استقرار رویکرد پیشنهادی خود بحث نکرده است، اینکه رویکرد آنها چگونه در شبکه‌های اینترنت اشیاء با گره‌های کم ظرفیت مستقر می‌شود. هزینه‌ی محاسباتی امضای حملات ذخیره شده و اجرای الگوریتم‌های یادگیری نیز احتمالا از مشکلات این رویکرد می‌باشند.

www.jozve.org

Kasinathan و همکارانش (۲۰۱۳a) یک سیستم تشخیص نفوذ مبتنی بر امضا را بـا چـارچوب شـبکه‌ای ادغام کرده‌اند که در پروژه‌ی ebbits [1]توسـعه داده شـده اسـت. هـدف اصـلی آنهـا تشـخیص حمـلات DoS در شبکه‌های مبتنی بر 6LoWPAN می‌باشد. برای پیاده‌سازی این سیستم تشخیص نفوذ، نویسندگان این مرجع از Suricata[2] که یک IDS مبتنی بر امضا است، در داخل شبکه‌های 6LoWPAN استفاده کرده‌انـد. ایـن سیسـتم تشخیص نفوذ پیشنهادی هشدارهایی را به یک مدیر حفاظت DoS ارسال می‌کند، که ایـن مـدیر بـرای بررسـی حمله به تحلیل اطلاعات اضافی از قبیل نرخ تداخل کانال و نرخ حذف بسته‌ها می‌پردازد. هدف از ایـن بررسـی، کاهش نرخ هشدار نادرست است. معماری پیشنهادی برای ممکن ساختن استقرار این IDS بر روی یک میزبـان اختصاصی لینوکس طراحی شده است تا از مسائل مربوط به ظرفیت کم گره‌ها جلوگیری کند. بـا ایـن حـال، در این مرجع به وضوح مشخص نیست که پایگاه‌داده‌ی امضاها چگونه به‌روزرسانی می‌شوند. همچنـین نویسـندگان این مرجع در نمونه‌ی دیگری، یعنی در مرجع Kasinathan و همکارانش (۲۰۱۳b) به ارائه‌ی یک رویکرد مبتنی بر امضا با توسعه‌ی رویکرد پیشنهادی قبلی خود در مرجع Kasinathan و همکارانش (۲۰۱۳a) پرداخته‌اند.

نویسندگان مرجع Oh و همکارانش (۲۰۱۴) سعی داشته‌اند تا هزینه‌ی محاسباتی مقایسه بین بار بسته‌ها و امضای حملات را کاهش دهند، چرا که گره‌های اینترنت اشیاء با ظرفیت کم ممکن اسـت چنـین عملیـاتی را پشتیبانی نکنند. روش پیشنهادی بر اساس یک الگوریتم تشخیص با چند الگو است. ایده‌ی این مرجـع در واقـع حذف بسیاری از عملیات غیرضروری با استفاده از مقادیر شیفت کمکی است. نویسندگان ایـن مرجـع الگـوریتم پیشنهادی خود را با استفاده از یک واحد محاسباتی Raspberry Pi که با حسـگر Omnivision 5647 ادغـام شده است، ارزیابی نموده‌اند. هدف اصلی این دستگاه در واقع ثبت تصاویر با استفاده از حسـگر جاسـازی شـده و انتقال این تصاویر به سرور مرکزی می‌باشد. سه الگوریتم با استفاده از مجموعه الگوهای نفوذ متعلق بـه Snort و

[1] http://www.ebbits-project.eu/
[2] http://suricata-ids.org/

www.jozve.org

ClamAV آزمایش شده‌اند. در سناریوی بهترین حالت، روش پیشنهادی به سرعتی تا ۲.۱۴ در مقایسه با الگوریتم معمولی تطبیق الگو و با توجه به محدودیت منابع دست یافته است.

۲-۳-۲. رویکردهای مبتنی بر ناهنجاری

سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری فعالیت‌های سیستم را در هر لحظه با پروفایل رفتار عادی سیستم مقایسه می‌کنند و هر گاه انحرافی از رفتار عادی را بیابد که از یک آستانه فراتر رفته است، آنگاه سیستم تشخیص نفوذ هشداری را تولید می‌نماید. این رویکرد برای تشخیص حملات جدید کارآمد است، به ویژه حملاتی که مرتبط با سوءاستفاده از منابع هستند. با این حال، هر گونه مشاهده‌ای که با یک رفتار عادی مطابقت نداشته باشد، به عنوان یک نفوذ در نظر گرفته می‌شود و یادگیری کل حوزه‌ی رفتار عادی سیستم کار ساده‌ای نیست. بدین ترتیب، این روش معمولا نرخ مثبت کاذب بالایی دارد (Mitchell و Chen، ۲۰۱۴؛ Debar، ۲۰۰۲؛ Scarfone و Mell، ۲۰۰۷).

محققان برای ایجاد نمایه‌ای از رفتار عادی معمولا از روش‌های آماری یا الگوریتم‌های یادگیری ماشین استفاده می‌کنند که این روش‌ها ممکن است برای گره‌های کم ظرفیت شبکه‌های اینترنت اشیاء بسیار سنگین باشد. بنابراین، رویکردهای مبتنی بر ناهنجاری ارائه شده برای شبکه‌های اینترنت اشیاء باید این ویژگی خاص را در نظر بگیرند.

در مرجع Cho و همکارانش (۲۰۰۹)، نویسندگان یک روش تشخیص بات‌نت‌ها را با استفاده از روش مبتنی بر ناهنجاری ارائه کرده‌اند. نویسندگان فرض کرده‌اند که بات‌نت‌ها باعث تغییرات غیرمنتظره‌ای در ترافیک گره‌های حسگر 6LoWPAN می‌شوند. راه‌حل پیشنهادی متوسط سه معیاری را محاسبه می‌کند که این سه

www.jozve.org

معیار در واقع نمایه‌ی رفتار عادی را ایجاد می‌کنند: مجموع قسمت[1] کنترل TCP، طول بسته، و تعداد اتصالات هر حسگر. سپس، سیستم بر ترافیک شبکه نظارت می‌کند و وقتی معیارها برای گره‌ای از مقدار متوسط محاسبه شده فراتر رود، آنگاه هشداری را تولید می‌کند.

Gupta و همکارانش (۲۰۱۳) یک معماری را برای یک سیستم تشخیص نفوذ بی‌سیم ارائه کرده‌اند. با توجه به معماری پیشنهادی، سیستم تشخیص نفوذ از الگوریتم‌های هوشمند محاسباتی برای ایجاد نمایه‌های رفتار عادی برای وسایل شبکه استفاده خواهد کرد. برای هر آدرس IP متفاوتی که به یک دستگاه تخصیص داده شده، یک نمایه‌ی رفتار عادی متفاوتی وجود خواهد داشت. نویسندگان امکان استقرار سیستم تشخیص نفوذ پیشنهادی را در شبکه‌هایی با وسایل کم ظرفیت در نظر نگرفته‌اند.

نویسندگان در مرجع Lee و همکارانش (۲۰۱۴) مصرف انرژی را به عنوان پارامتری برای تحلیل رفتار گره‌ها فرض کرده‌اند. آنها مدل‌هایی را برای مصرف عادی انرژی تحت روش‌های مسیریابی به صورت مش و در طی مسیر[2] تعریف کرده‌اند. سپس، هر گره مصرف انرژی خود را با سرعت نمونه‌برداری ۰.۵ ثانیه نظارت می‌کند. وقتی مصرف انرژی از یک مقدار مورد انتظار منحرف شود، آنگاه سیستم تشخیص نفوذ گره را به عنوان مخرب دسته‌بندی کرده و آن را از جدول مسیریابی در 6LoWPAN حذف می‌کند. نویسندگان این مرجع ادعا کرده‌اند که رویکرد پیشنهادی آنها سبک و کم‌حجم است، و به طور خاص برای شبکه‌های کم ظرفیت طراحی شده است. با این حال، آنها نتایج مربوط به نرخ مثبت کاذب را ارائه نکرده‌اند، که برای نتیجه‌گیری دقیق در مورد رویکرد ضروری است.

Summerville و همکارانش (۲۰۱۵) یک رویکرد تشخیص ناهنجاری بسته-عمیق را توسعه داده‌اند که هدف آن اجرا بر روی وسایل اینترنت اشیاء با منابع محدود است. نویسندگان این مرجع ادعا کرده‌اند که وسایل کوچک اینترنت اشیاء از پروتکل‌های اندک و نسبتا ساده‌ای استفاده می‌کنند، که این امر باعث می‌شود تا بارهای

[1] field
[2] route-over

www.jozve.org

شبکه‌ای[1] آنها بسیار مشابه باشد. بر اساس این ایده، آنها از روشی به نام انطباق الگوی بیتی برای انجام انتخاب ویژگی استفاده کرده‌اند. بارهای شبکه‌ای به عنوان دنباله‌ای از بایت‌ها در نظر گرفته می‌شود، و انتخاب ویژگی بر روی همپوشانی چندین بایت عمل می‌کند که n-grams نام دارد. یک انطباق بین یک الگوی بیتی و یک n-gram وقتی رخ می‌دهد که بیت‌های موجود در تمام موقعیت‌های هر دو دنباله با هم مطابقت داشته باشند. نویسندگان یک ارزیابی آزمایشی را با استفاده از دو دستگاه مجهز به اینترنت ارائه کرده‌اند و نرخ‌های مثبت کاذب برای چهار نوع حمله (انتشار کرم، تونل‌زنی، تزریق کد SQL، و حمله‌های پیمایش دایرکتوری[2]) بسیار پایین بود.

Thanigaivelan و همکارانش (۲۰۱۶) به طور خلاصه یک سیستم تشخیص ناهنجاری داخلی توزیع شده‌ای را برای اینترنت اشیاء معرفی کرده‌اند. اصل سیستم تشخیص نفوذ پیشنهادی جستجو برای یافتن هر گونه تفاوتی در شبکه به وسیله‌ی نظارت بر مشخصات گره‌های همسایه‌ای است که در مسافت یک گامی از هم قرار دارند، مشخصاتی از قبیل اندازه‌ی بسته و نرخ داده. طبق گفته نویسندگان، سیستم رفتارهای عادی را از اطلاعات نظارت شده به دست آورده و یادگیری می‌کند. با این حال، جزئیاتی در مورد روش استفاده شده برای ایجاد نمایه‌ی رفتار عادی ارائه نشده است. همچنین این امر نیز به وضوح مشخص نشده است که الگوریتم تشخیص بر روی گره‌های کم ظرفیت اینترنت اشیاء چگونه عمل خواهد نمود.

Pongle و Chavan (۲۰۱۵) یک سیستم تشخیص نفوذی را ارائه کرده‌اند که برای تشخیص حمله‌های wormhole (کرم‌چاله) در وسایل اینترنت اشیاء طراحی شده است. نویسندگان این مرجع فرض کرده‌اند که حمله‌ی wormhole همیشه نشانه‌هایی از خود را بر روی سیستم ایجاد می‌کند، به عنوان مثال، تعداد زیادی از بسته‌های کنترلی بین دو گره‌ی انتهایی تونل رد و بدل می‌شود، یا تعداد زیادی از همسایگان پس از یک حمله‌ی موفقیت‌آمیز شکل می گیرند. با استفاده از این منطق، نویسندگان سه الگوریتم را برای تشخیص چنین

[1] network payloads
[2] directory traversal

www.jozve.org

ناهنجاری‌هایی در شبکه ارائه کرده‌اند. با توجه به آزمایش‌های آنها، سیستم به نرخ مثبت واقعی ۹۴٪ در تشخیص wornhole و ۸۷٪ در تشخیص حمله و مهاجم دست یافته است. با این حال، هیچ جزئیاتی در مورد نرخ مثبت کاذب ارائه نشده است. نویسندگان این مرجع همچنین مطالعه‌ای بر روی مصرف توان و حافظه‌ی گره‌ها نیز انجام داده‌اند. ظاهرا، سیستم پیشنهادی برای وسایل اینترنت اشیاء مناسب است، زیرا مصرف توان و حافظه‌ی آن پایین است. از سوی دیگر، نتایج به دست آمده باید با دیگر مقالات مرتبط نیز مقایسه شود تا مبنایی بین آنها برقرار شود.

۲-۳-۳. رویکردهای مبتنی بر مشخصه

مشخصه در واقع مجموعه‌ای از قوانین و آستانه‌ها است که رفتار مورد انتظار را برای اجزای شبکه از قبیل گره‌ها، پروتکل‌ها، و جداول مسیریابی تعریف می‌کنند. رویکردهای مبتنی بر مشخصه، نفوذهایی را تشخیص می‌دهد که در آنها رفتار اجزای شبکه از مشخصه‌های تعریف شده انحراف یافته و تغییر داشته باشند. بنابراین، تشخیص مبتنی بر مشخصه اهداف مشابهی مانند تشخیص مبتنی بر ناهنجاری دارد: یعنی شناسایی انحرافات از رفتار عادی. با این حال، یکی از مهمترین تفاوت‌های موجود بین این دو روش به این صورت است که در رویکردهای مبتنی بر مشخصه، یک انسان متخصص باید به صورت دستی قوانین هر مشخصه را تعریف کند (Mitchell و Chen، ۲۰۱۴؛ Amaral و همکارانش، ۲۰۱۴؛ Butun و همکارانش، ۲۰۱۴a). مشخصات تعریف شده به صورت دستی معمولا نرخ مثبت کاذب کمتری را در مقایسه با تشخیص مبتنی بر ناهنجاری فراهم می‌کنند (Mitchell و Chen، ۲۰۱۴؛ Amaral و همکارانش، ۲۰۱۴؛ Butun و همکارانش، ۲۰۱۴a). علاوه بر این، سیستم‌های تشخیص مبتنی بر مشخصه نیازی به مرحله‌ی آموزش ندارند، زیرا آنها می‌توانند بلافاصله پس از تنظیم مشخصات شروع به کار کنند (Amaral و همکارانش، ۲۰۱۴). با این حال، تعریف مشخصات به صورت

www.jozve.org

دستی ممکن است با محیط‌های مختلف سازگاری نداشته باشد و همچنین تنظیم مشخصات وقت‌گیر و مستعد خطا است (Mitchell و Chen، ۲۰۱۴؛ Amaral و همکارانش، ۲۰۱۴؛ Butun و همکارانش، ۲۰۱۴a).

Misra و همکارانش (۲۰۱۱) رویکردی را برای محافظت از میان‌افزار اینترنت اشیاء از حملات DDoS[1] (انکار سرویس توزیع شده) ارائه کرده‌اند. برای تشخیص حملات، حداکثر ظرفیت هر لایه‌ی میان‌افزار مشخص می‌شود. وقتی که تعداد درخواست‌های رسیده به یک لایه از آستانه‌ی مشخصی فراتر رود، آنگاه سیستم هشداری را تولید می‌کند.

در مقاله‌ی Le و همکارانش (۲۰۱۱)، نویسندگان رویکرد مبتنی بر مشخصه‌ی دیگری را ارائه کرده‌اند، که بر روی تشخیص حملات RPL تمرکز دارد. آنها رفتار RPL را در یک ماشین حالت محدود مشخص می‌کنند، که برای نظارت بر شبکه و تشخیص رفتارهای مخرب مورد استفاده قرار می‌گیرد. این رویکرد در مقاله‌ی Le و همکارانش (۲۰۱۶) توسعه داده شده است، که نویسندگان در آن از فایل‌های ردیابی شبیه‌سازی (بستر Contiki-Cooja) برای تولید ماشین حالت محدود برای پروتکل RPL استفاده کرده‌اند. این پروفایل به مجموعه‌ای از قوانین تبدیل شده است که برای بررسی داده‌های نظارتی از گره‌های شبکه به کار گرفته می‌شوند. با توجه به آزمایشات آنها، نرخ‌های مثبت واقعی بسیار بالا بوده در برخی موارد به ۱۰۰٪ نیز می‌رسد و همچنین نرخ‌های مثبت کاذب بسیار پایین است و از ۰٪ تا ۶.۷۸٪ تغییر می‌کند. علاوه بر این، روش پیشنهادی در مقایسه با شبکه RPL معمولی، سربار انرژی ۶.۳٪ دارد.

Amaral و همکارانش (۲۰۱۴) یک سیستم تشخیص نفوذ مبتنی بر مشخصه ارائه کرده‌اند که به مدیر شبکه اجازه می‌دهد تا قوانین موردنیاز برای تشخیص حمله را ایجاد کند. هنگامی که این قوانین نقض شوند، آنگاه سیستم تشخیص نفوذ هشداری را به سیستم مدیریت رویداد[2] (EMS) ارسال می‌کند. EMS بر روی گره‌ای بدون محدودیت‌های منابع اجرا می‌شود تا هشدارهای رسیده از گره‌های مختلف شبکه را مرتبط نماید.

[1] Distributed Denial of Service (DDoS)
[2] Event Management System (EMS)

www.jozve.org

موفقیت رویکردهای Mirsa و همکارانش (۲۰۱۱) و Amaral و همکارانش (۲۰۱۴) به شدت به تخصص مدیر شبکه بستگی دارند، که یک ویژگی از روش مبتنی بر مشخصه است. تعریف مشخصات نادرست ممکن است باعث ایجاد مثبت‌های کاذب و منفی‌های کاذب بسیار زیاد شود، که خطر قابل توجهی را برای امنیت شبکه خواهد داشت.

۲-۳-۴. رویکردهای ترکیبی

رویکردهای ترکیبی از مفاهیم تشخیص مبتنی بر امضا، مبتنی بر مشخصه و مبتنی بر ناهنجاری استفاده می‌کنند تا مزایای این روش‌ها را به حداکثر رسانده و تاثیر معایب آنها را به حداقل برسانند.

SVELTE یک سیستم تشخیص نفوذ ترکیبی است که Raza و همکارانش در مرجع Raza (۲۰۱۳) ارائه کرده‌اند. هدف از این IDS ترکیبی، ارائه‌ی یک توازن بین هزینه‌ی ذخیره‌سازی در روش مبتنی بر امضا و هزینه‌ی محاسباتی در روش مبتنی بر ناهنجاری است. در مرجع Krimmling و Peter (۲۰۱۴)، نویسندگان تشخیص نفوذهای مبتنی بر امضا و ناهنجاری را مورد آزمایش قرار داده‌اند و این کار را با استفاده از چارچوب ارزیابی IDS پیشنهادی خود انجام داده‌اند. نتایج نشان می‌دهد که هر رویکرد در تشخیص برخی از انواع حملات شکست می‌خورد. به گفته‌ی نویسندگان این مرجع، ترکیبی از این رویکردها می‌تواند به طیف وسیعتری از حملات با یک سیستم IDS تنها رسیدگی کند. INTI IDS، توسط Cervantes و همکارانش (۲۰۱۵) برای تشخیص و جداسازی حملات sinkhole پیشنهاد شده است، و مفاهیم مبتنی بر ناهنجاری و مبتنی بر مشخصه را ترکیب می‌کند، از روش مبتنی بر ناهنجاری برای نظارت بر تغییرات بسته‌ها بین گره‌ها و از روش مبتنی بر مشخصه برای استخراج دو نوع از ارزیابی گره‌ها، یعنی اعتبار و اعتماد استفاده می‌کند. مقادیر بین صفر و یک متغیر هستند. وقتی مقادیر اعتبار یا اعتماد بالای ۰.۵ باشند، آنگاه گره به عنوان یک گره‌ی خوب در نظر گرفته

www.jozve.org

می‌شود. INTI ارزیابی شده و با SVELTE از نظر موثر بودن و کارایی جهت کاهش حملات sinkhole مورد مقایسه قرار گرفته است. نویسندگان یک سناریوی شبیه‌سازی را پیشنهاد کرده‌اند و نتایج این شبیه‌سازی نشان می‌دهد که INTI در یک سناریوی ثابت به نرخ تشخیص حمله‌ی sinkhole بالای ۹۲٪ و در یک سناریوی متحرک نیز به نرخ ۷۵٪ دست می‌یابد. علاوه بر این، INTI در هر دو سناریو نسبت به SVELTE، مثبت کاذب[1] و منفی کاذب[2] کمتری را از خود نشان داده است.

[1] False Positive
[2] False Negative

www.jozve.org

فصل سوم:

چالش های امنیتی اینترنت اشیا

www.jozve.org

۳-۱. چالش های امنیتی و انواع حملات در اینترنت اشیاء

از زمان پیدایش اینترنت اشیا و اذعان به تسهیلاتی که این فن آوری به همراه داشته و خواهد داشت اما شاهد دغدغه های گسترش یافته ای همچون مسایل امنیتی نیز بوده ایم، که سازندگان بدان اهمیت کمتری داده اند و تعاریف ضعیف امنیتی برای اینترنت اشیا شده است و آنچه مابین ۳۲ دسامبر ۲۰۱۳ تا ۶ ژانویه ۲۰۱۴ رخ داد این موضوع را ثابت می کند. قرار دادن پسوردهای ضعیف به صورت دیفالت Defult برای اینترنت اشیا و بعضا درج پسورد روی دفترچه راهنما و ضعف برنامه نویسی مناسب برای تغییر پسورد توسط کاربر و نوع پسورد، باعث شده تا هکرها به آسانی کنترل اینگونه ابزار را از راه دور به دست بگیرند. مشکلات ناشی شده از انتقال و پردازش های داده های ناخواسته، حملات سایبری موجب نگرانی های کاربران و مسائل قانونی شده است. اگر فعالیت روزانه افراد نظارت شده و آن ها تولید کننده خروجی های اطلاعاتی باشند، فعالیت های سیاسی، اقتصادی و اجتماعی تحت تاثیر قرار می گیرند. در صورت نقض امنیت، رخداد حمله و اختلال در عملکرد، مزایای IOT کمرنگ می شود. در آینده از نزدیک حجمی وسیع از اطلاعات توسط وسایل متصل و سیستم های مدیریتی دریافت و ارسال خواهد شد. به اعتقاد sopho در سال ۲۰۱۵ سوء استفاده از آسیب پذیری های نرم افزاری کاهش خواهد یافت. با توجه به کاهش تعداد آسیب پذیری های نرم افزاری، معدودی آسیب پذیری ها به شدت مورد استفاده قرار خواهد گرفت. اینترنت اشیاء، بزرگ ترین نگرانی امنیتی سال ۲۰۱۵ به نظر می رسد. در یکی از بررسی های اخیر واحد پژوهشی شرکت اچ پی نشان می دهد هر ابزار عادی متصل به اینترنت اشیا ۲۵ ضعف امنیتی دارد که رقم شگفت انگیزی است و ۷۰ درصد ابزارها دست کم یکی از چنین ضعف هایی را دارند. اینترنت اشیا با چالش های زیادی رو به رو است. از نظر مقیاس پذیری و برنامه های کاربردی IOT به تعداد زیادی از دستگاه ها نیاز دارد که پیاده سازی آن ها به دلیل محدودیت های زمان، حافظه و پردازش مشکل است. محدودیت آدرس های اینترنتی در نسخه ۴ پروتکل اینترنتی این سیستم هاروادار کرده حداکثر تا

www.jozve.org

حدود ۴ میلیارد آدرس را پشتیبانی کند که با توجه به حجم اتصال تا سال ۲۰۲۰ باید از امکانات پیشرفته تری استفاده کرد. (گوبی،۲۰۱۳).

در واقع می توان گفت برخلاف کامپیوترهای تجاری که چند دهه است به وسیله فایروال ها و سامانه های تشخیص نفوذ و بازدارنده (IDPS) محافظت می شوند، دستگاه های کنونی متصل به اینترنت از چنین تمهیداتی برخوردار نیستند. دانشگاه کلمبیا در راستای یکی از پژوهش های خود با حمله به سیستم های تجاری و نیز سامانه های نهفته موجود در دستگاه های مصرفی از جمله سامانه های سرگرمی خانگی، وب کم ها و اکسس پوینت های وای فای دریافت که تنها ۲/۴۶ درصد محصولات تجاری مشکل امنیتی دارند، در حالی که این مورد برای دستگاه های مصرفی ۴۱/۶۲ درصد بود. حتی در آن دسته از محصولات مصرفی که تمهیدات امنیتی دارند، در حالی که این مورد برای دستگاه های مصرفی ۴۱/۶۲ درصد بود. حتی در آن دسته از محصولات مصرفی که تمهیدات امنیتی دارند نیز امکانات بازدارنده یا فعال نشده اند یا گذرواژه پیش فرض یا ناکارآمد دارند .

بسیاری از تولید کنندگان این کالاها بیش تر به این می اندیشند که محصول خود را سریع تر وارد بازار کنند، امام به امنیت آن چندان توجهی ندارند. تولید کننده در برخی موارد دستگاه طراحی شده برای شبکه های خصوصی را به سادگی فقط به اینترنت متصل می کند و درون آن هیچ گونه تمهیدات امنیتی خاص را در نظر نمی گیرند. در بسیاری از این وسایل امکان دسترسی به تنظیمات امنیتی و سیستم عامل وجود ندارد. خیلی ساده می توانیم برنامه های امنیتی مورد نظرتان را روی کامپیوتر و یا اسمارت فون نصب کنیم. اما با یک گاز، یخچال و ... هوشمند که کیبورد و نمایشگر ندارد چگونه عمل کنیم؟

از چالش های دیگر امنیت lot ، سیستم عامل ها و نرم افزارهایی که باید به روز رسانی شوند. بیشترین منفعت آن آسودگی ما از بابت امنیت محصول است از سویی دیگر تولیدکنندگان محصولات هوشمند به سه دسته اند گروهی که تضمین می کنند محصولشان به روز رسانی می شود و گروه دیگر که این کار را زمان بر

www.jozve.org

دانسته و از آن صرف نظر می کنند. برخی دیگر از تولیدکنندگان، نه به روز رسانی را مد نظر می گیرند و نه مسائل امنیتی، با این حال قابلیت کنترل از راه دور محصول خود را بسیار مهم می دانند. در جمع بندی این بخش دغدغه های امنیتی اینترنت اشیا می توان موارد ذیل را ذکر کرد:

قوانین و مقررات امنیتی : در حال حاضر، قانون و مقررات امنیت، همچنان در مرکز توجهات قرار ندارد و هیچ استاندارد تکنولوژی ای در مورد IOT وجود ندارد. IOT مربوط به اطلاعات امن ملی، اسرار تجاری و حریم شخصی افراد می باشد. در نتیجه، کشور ما نیز به دیدگاه قانونی جهت توسعه IOT است. مقررات وقوانین به صورت بلا انکاری مورد نیاز است.

ساختار معماری: IOT در طول کل بازه زمانی، پایدار باقی می ماند و مکانیزم امنیت در هر لایه منطقی نمی‌تواند سیستم دفاع کامل را پیاده سازی کند، در نتیجه، این موضوع یک چالش بوده و خوزه های تحقیقاتی فراوانی جهت ایجاد ساختار امن با ترکیب کنترل و اطلاعات، مورد نیاز است.

مدیریت کلان: مدیریت اساسی، پایه مهمی از مکانیزم امن می باشد، این موضوع همواره یک موضوع تحقیقاتی داغ می باشد. این مورد همچنان مشکلترین جنبه امنیت رمزنگاری است. در حال حاضر، محققان راه حل ایده‌آل برای این موضوع را پیدا نکرده اند.. الگوریتم رمزنگاری سبک یا عملکرد بالاتر گره سنسور، همچنان اعمال نشده است. در نتیجه، شبکه سنسور مقیاس بزرگ همواره به صورت قابل اجرا باقی می ماند. مسائل امنیت شبکه بیشتر مورد توجه قرار گرفته و تبدیل به یک نکته مهم شده و مشکلاتی را در حوزه تحقیقات محیط شبکه ایجاد می کند.

نیازمندی ها برای کاربردهای نوظهور: با توسعه WSNها ، تشخیص فرکانس رادیویی (RFID)، تکنولوژی محاسبات فراگیرنده، تکنولوژی مخابرات شبکه، و تئوری کنترل بلادرنگ توزیع شده، CPS، یک شکل بروز پیدا کرده از IOT تبدیل به واقعیت شده است در این سیستم، امنیت بالا برای تضمین عملکرد

www.jozve.org

سیستم مورد نیاز است. ایجاد ساختارهای شبه امن نیز بسیار ضروری می باشد. مدیریت اساسی در یک شبکه سنسور مقیاس بزرگ واقعی نیز همواره از مسائل چالشی بوده و مقررات و قوانین این حوزه که مربوط به IOT است نیز جزو موضوعات چالشی می باشد.

استاندارد سازی: پاسی آئوری از شرکت Finnish و عثمان حق از Pachube با این نظریه موافق هستند و اعلام کردند ترجیح می دهند به جای آن که استانداردهای سخت گیرانه مانع پیشرفت شود، اجازه داده شود فناوری خود رشد کند. پاتریک و ترولد از شرکت سیسکو پس از آن اعلام کرد اینترنت اشیا بهتر است با استانداردهای باز ساخته شود. این منبع باز بودن عمل پذیری متقابل را به وجود می آورد. اما در نقطه مقابل محافظه کاران درباره این ایده تکاملی تدریجی به ما یادآوری می کنند بهتر است تامل کنیم چه کسی خواستار استانداردها است؟ موضوع به پاسخ گویی استانداردها باز می گردد. وبر پیشنهاد می کند استانداردها باید به صورتی ارائه شوند که چهارچوب های مدیریتی را به وجود آورند و اطلاعات را به سرعت در اختیار ما قرار دهند. پیاده سازی استانداردها پاسخ گویی آن ها را همراه خواهد داشت. بهبود پاسخ گویی با ایجاد چنین چهارچوبی بهبود امنیت اینترنت اشیا را به دنبال دارد.

حریم خصوصی: از مهمترین مسائل امنیتی که کل سیستم IOT در حال توسعه را مورد آزار قرار می دهد ناشی از مسائل امنیتی موجود در تکنولوژی های ست که در IOT برای باز بخش اطلاعات از یک دستگاه به دستگاه دیگر بکار گرفته می شوند. که همین مسئله حریم خصوصی افراد را تحت شعاع خود قرار می دهد(اکباتانی،۱۳۹۴).

www.jozve.org

۳-۲. مسائل امنیتی در شبکه های حسگر بیسیم (WSNS)

روابط سلسله مراتبی مسائل مختلف امنیتی که شبکه های حسگر بیسیم را تهدید می کند در شکل ۴ نشان داده شده است.

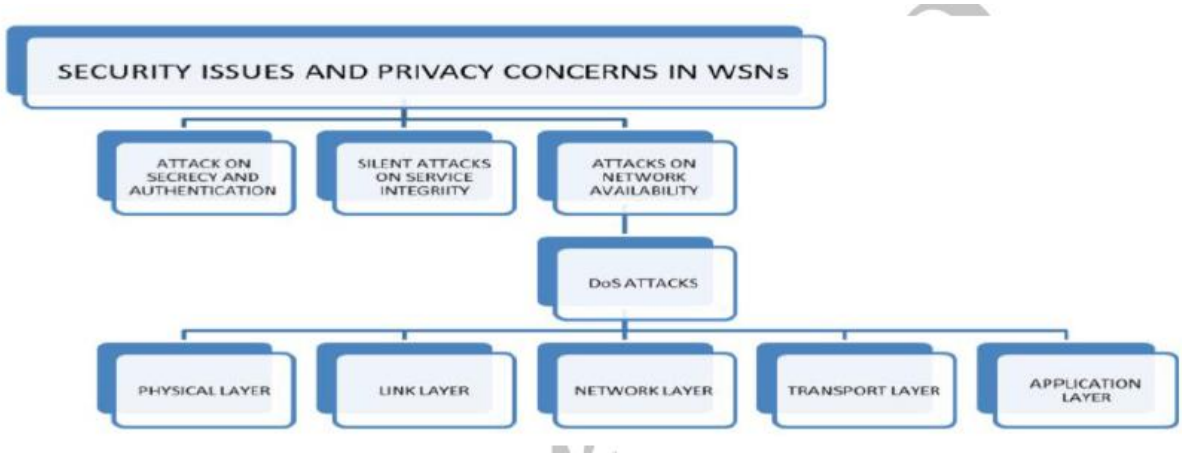
عملیات سرکوبگرایانه ای که میتوانند در شبکه های حسگر بیسیم اجرا شوند را میتوان به سه دسته تقسیم کرده :

- حملات بر محرمانگی و هویت

- حملات خاموش بر جامعیت سرویس

-حملات بر در دسترس بودن شبکه و انکار سرویر(Denial of service (DOS

حملاتی که رخ میدهد در این ۳ دسته قرار میگیرند. جلوگیری از دسترسی کاربران قانونی به اطلاعات توسط نفوذ گران شخص ثالث ناشناس میتواند در لایه های مختلف شبکه اتفاق بیافتد(بیهاش،۲۰۱۲).



شکل ۳-۱- روابط سلسله مراتبی امنیتی

www.jozve.org

۳-۳. حملات انگار سرویس بر لایه های IOT

۳-۳-۱. حمله Dos به لایه فیزیکی:

لایه فیزیکی شبکه های حسگر بیسیم انجـام عملیـات انتخـاب و تولیـد فرکـانس حامـل، مدولاسـیون و دمدولانه رمز گذاریه رمزگشایی و انتقال و دریافت داده را برعهده دارد. این لایه شبکه حسگر بی سیم اساسـا از طریق موارد زیر مورد حمله قرار میگیرد:

- Jamming: این نوع از حمله DOS, کانال ارتباطی بین گره ها را انفال مـی کنـد و بـدین ترتیـب از ارتباط آنها با یکدیگر جلوگیری بعمل می آورد .

- Node terrporing (دستکاری گره): دستکاری فیزیکی گره برای استخراج اطلاعات حسـاس بعنـوان دستکاری کره شناخته می شود راهکار : نوافق بر کلید حفاظت از داده حسگر و پیاده سازی رمزنگاری ساده

۳-۳-۲.حمله DOS به لایه اتصال

لاپه اتصال WSN، ارسال همزمان جریان داده های مختلف، تشخیص فرم دادن کنترل Mac و خطـا را بر عهده دارد. علاوه بر این قابلیت اطمینان نقطه به نقطه (point- point) و یا تقطه به چندین نقطه (point multiple point :) را تخمین می کند. حملات D05 که در این لایه اتفاق میافتد به شرح زیر است؛

www.jozve.org

-Collision (بر خورده) این نوع حمله D05 میتواند زمانی آغاز شود که دو گره بصورت همزمان بسته های داده را در یک کانال فرکانسی انتقال دهند برخورد بسته های داده به یکدیگر منجر به تغییرات کوچکی در بسته می شود. این امر موجب میگردد که در پایان دریافت، در شناسایی بسته یا ناسازگاری مواجه شویم که موجب دور انداختن پسته باده آسیب دیده و فرستادن دوباره آن خواهد شد(جی سن،۲۰۰۷) .

- Unfairnes همانطور که توضیح داده شده است، این حمله، یک حمله مبتنی بر تکرار برخورد (repeated Collision) است و میتواند بعنوان حملات مبتنی بر خستگی (exhaustion based attacks مطرح شود.

- Battery Exhaustion : این نوع از حمله D05، ترافیک بالای غیر معمولی را در یک کانال ایجاد می کند و بدین ترتیب قابلیت دسترسی پذیری را برای گره های دیگر بسیار محدود می سازد. چنین خرابکاری هایی در یک کانال از درخواست های بسیار زیاد درخواست ارسال و انتقال ها در طول کانال حاصل می شود(گوبی،۲۰۱۳).

۳-۳-۳.حمله DOS به لایه شبکه

کاربرد اصلی به شبکه مسیر بابی است، حملات DOS ویژه ای که در این لایه اتفاق می افتند عبارتند از؛

-Spoofing : باز پخش و هدایت نادرست ترافیک

-Hello flood attack: این حمله ترافیک بالایی را در کانال ها با فرستادن تعداد زیاد غفیر معمولی از پیامهای بی فایده (useless) صورت می دهد، در اینجا یک گره مخرب مجزا یک پیام بی فایده را ارسال می کند. سپس این پیام توسعد مهاجم برای ایجاد ترافیک بازپخش می شود.

www.jozve.org

- Moming : در حمله Homing, جستجو برای یافتن سرخوشه ها و مدیران کلیدی که توانای خاموش کردن کل شبکه را دارند. صورت می پذیرد.

-Selective forwarding : همانطور که از نام این حمله پیداست. در حمله ارسال انتخلی: یک گره که در معرض خطر قرار دارد. تنها چند گره انتخاب شده را بجای تمامی گروه ها میفرستند. این انتخاب گره ها بر اساس نیاز مندی مهاجم در رسیدن به اهداف خرابکارانه خود صورت می گیرد. بنابراین چنین گروه هایی بسته های داده را منتقل نمی کند.

- Sybil :در این حمله، مهاجم یک گوه مجزا را تکثیر می کند و آن را با هویت های چند گانه به دیگر گره ها نشان میدهد.

- Wormhole : این نوع از حمله DOS باعث جابجایی بیت های داده از جایگاه اصلی خود در شبکه می شوند. این جابجایی بسته داده از طریق تول رسی بیت های داده در طول یک تاخیر کوتاه از اتصال اتفاق می افتد.

Acknowledgement flooding: پیامهای تصدیق (Acknowledgement)، زمان هایی که شبکه های حسگر بیسیم الگوریتم های مسیر یابی را بکار می گیرند مورد نیاز هستند در این نوع از حمله DOS، یک گره مخرب پیامهای تحدیق جعلی را که اطلاعات نادرستی را به گره های مقصد همسایه میدهد. ارسال می کند.

- راهکار شناسایی مکانیزم های رمزنگاری - بالا بردن امنیت ارتباطات و تصدیق هویت

۳-۳-۴.حملات DOS در لایه انتقال

www.jozve.org

این لایه از معماری WSN، قابلیت اطمینان از انتقال داده ها را فراهم مـی سـازد و از ازدحـام ناشـی از ترافیک بالا در روترها جلوگیری می کند. حملات DOS در این لایه بشرح زیر است :

Flooding: به ازدحام عمدی در کانال های ارتباطی از طریق باز ارسال پیامهای غیر ضروری اشاره دارد :

Dw - synchronization در حملهDe - synchronization ، پیامهای جعلی در یک یا هردر نقبله ی انتهای (analpoint) تولید می شوند و از سـال مجـدد بسـته را بـرای اصـلاح خطـایی کـه موجـود نیسـت درخواست می کنند. این امـر موجـب از دسـت رفـتن انـرژی در یـک یـا هـر دو نقطـه انتهـایی بخـاطر انجـام دستورالعملهای جعلی می شود(روی و بیشباش ،۲۰۱۲).

۳-۳-۵.حملات D05 در لابه کاربرد

لابه کاربرد WSN، مسولیت مدیریت ترافیک را بر عهده دارد. این لایه همچنین بعنوان فراهم کننده نرم افزار برای برنامه ها کی کاربردی مختلف که ترجمه داده را به شکلی قابل فهم انجام میدهند، عمل می کند و یا در جمع آوری اطلاعات با فرستادن کوئری ها، کمک میکد(جی سن،۲۰۰۷). در این لایه یک حملـه مبتنـی بـر path (مسیر)، با تحریک گره های حسگر برای ایجاد یک ترافیک بزرگ در مسیر منتهی به ایسـتگاه پایـه آغـاز می شود.

راهکار : می توان با توافق بر کلید حفاظت از حریم خصوصی و تصدیق هویت از طرف مدیریت امنیت تـا حدود زیادی مقابله کرد(برونو بورگاز،۲۰۱۷).

۳-۴. اهمیت داده در اینترنت اشیاء :

www.jozve.org

داده ها واژه ای با اهمیت در اینترنت اشتباه می باشد. برای اینکه به اهمیت داده ها در اینترنت اشیا. پی ببریم عملکرد شرکت nest را بررسی میکنیم این شرکت در سال ۲۰۱۰ توسط گروهی از مهندسان سابق ایل ایمی شده و تلاش کرد ترموستات های عادی را به گیت های نیکی تبدیل کند که می تواند به اینترنت متصل شونده عملکرد این شرکت به اندازه ای خوب بود که یک شرکت خصوصی برقی به nest هزینه ای پرداخت کرد تا در رله دور دستگاه های تهویه مردم را خاموشی کند تا در روز های گرم سال، یعنی درست همان زمانی که هزینه برقی زیاد گران می شوده در کار کرد برق صرفه جویی شود چنین روشی رویه ای (واکش به در خواست) یا Demand response خوانده می شود و شبکه های هوشمند از مدت ها پیش آن را به عنوان راه کاری عالی به خدمت گرفته اند. اگر کارکرد برقی در زمان های اوج مصرف به اندازه کافی کاهش پیدا کننده شرکت های برق دیگر نیازی نخواهند داشت تیروگاه های ذخیره خود را که هزینه زیادی به آنها تحمل می کند به کار بیدازند(به طور خلاصه واکنش به درخواست، طرحی است برای صرفه جویی در کار کرد برقی هنگامی که مصرف برق افزایش می یابد.) واکنش به درخواست راه کار سودمندی است ترموستات های تولید شده توسط nest با استفاده از دو چیز التوانسته اند چنین راه کاری را عملی کنده پکی آگاه کردن کاربر از هزینه برقی که تا کنون به کار برده است و دیگری کنترل القاضای برف که هر دو رول از طریق جمع آوری داده های کاربر به دست می آید. کار واقعی ترموستات های nest گرد آوری داده ها است و این کار را از درون خانه ها آغاز می کند ترموستات های nest بتم آشکار سیار دارد و برای سنجش زعماء رطوبت هوا و نور محیط از حس گرهای ویژه ای بهره می برد. این دستگاه همچنین از الگوریتم هایی برخوردار است که عادت ها و ترجیح های ساکنان خانه را یاد می گیرند و میتوانند تنظیم های مربوط به سیستم گرمایشی وبرقی شهری را برنامه ریزی کند. برای ارائه داده های مربوط به آب و هوا از یک اتصال وای ای استفاده می شود و کاربران می توانید این سامانه را با گوشی با مرور گر وی کنترل کنند، باره ما تازه آغاز گر این ماجرا هستند و از اهمیت ویژه ای برخوردار هستند همان گونه که گوگل که اکنون با خرید ۳٫۲ میلیارد دلاری nest به شیوه ای ماهرانه از دانسته هایش در باره شما برای انتشار آگهی های ونبه سود می برد، او نیز با استفاده از توان مندی ها و داده هایی که گرد آوری می

www.jozve.org

کند، به شرکت های این حیطه سرویس های نوین می فروشند. در این فست علاوه بر این که اهمیت داده را بـا ذکر یک مقاله بررسی کردیم به این نتیجه خواهیم وحید که آیا از این داده ها بر علیه خود بـا اسـتفاده خواهـد شد؟ (عطاریان،۱۳۹۵)

۳-۵. نبود استاندارد واحد

اینترنت اشیا امروز دنیای متفاوتی دارد. وقتی که استانداردهای بنیادی اینترنت ایجاد شدند، افرادی کنترل این استانداردها را در دست داشتند که خواسته واقعی شان شکل گیری استانداردهای جهانی بود. استانداردهایی که به طور برابر در دسترس همه باشد. اما اینترنت امروزه در کنترل شرکت هایی است که هر کدام می خواهند از این استانداردها بهره بگیرند و با استفاده از آنها رقبا را شکست دهند و سود ببرند. همچنین، اینترنت در دست دولت هایی است که در اصل می خواهند بر همه چیز نظارت داشته باشند. در چنین وضعیتی دولت ها و شرکتها چگونه می خواهند بر سر دستیابی به استانداردهای جهانی به توافق برسند؟ در اینترنت اشیا استاندارد یعنی همه چیز هر دستگاه باید به دستگاه های دیگر اعلام کند که چه کاری را می خواهید انجام بدهد. بدون این استانداردها آنها نمی توانند هیچ یک از این کارها را انجام دهند. این واقعیت را هم به چالش اضافه کنید که معمولا تجهیزات متصل به iot بسیار گوناگون و متفاوت هستند. شرکت ها و سازمان های زیادی برای وضع استانداردهای مورد نیاز می کوشند که اتحادیه allseen ، کنسرسیوم اینترنت صنعتی، اتحادیه

کنسرسیوم اینترنت صنعتی،اتحادیه ipso و کنسر سیومopen interconnect جزء نهادهای اصلی در این باره هستند.دراین چشم انداز اینترنت اشیاء نقطه ای به چشم نمی خورد که بر سر یک سری استانداردهای جهانی به توافق برسند.(مرتضی یوسفی،۱۳۹۵)

www.jozve.org

۳-۶.چالش های اینترنت اشیا

۳-۶-۱.چالش حریم خصوصی

همان طور که در مورد لوازم بهداشتی و خدمات اضطراری ماشین ها ی هوشمند،دستگاه های اینترنت اشیا می تواند مقدار زیادی داده ها را در محل کاربران اینترنت اشیاء و حرکات ،شرایط بهداشتی،و تنظیمات خرید را انتقال دهند که همه این ها می تواند نگرانی های قابل توجهی برای حفظ حریم خصوصی فراهم کند.حفاظت از حرین خصوصی که اغلب بر دوش ارائه دهندگان در این سناریو ،به عنوان اطلاعات کلیدی تولید شده توسط اینترنت اشیا برای بهبود کیفیت زندگی مردم و کاهش هزینه های توسط ارائه دهندگان خدمات است .IOT قرار است به بهبود کیفیت زندگی مردم کمک کند .درحالی که اعتماد به نفس و پذیرش اینترنت اشیا و همچنین گسترش استفاده از سیستم خانه های هوشمند و دستگاه ها ی پوشیده ،نیاز اینترنت به حمایت از حریم خصوصی کاربران بستگی دارد.با توجه به(۲۰۱۴)TRUSTE اینترنت اشیا با شاخص حریم خصوصی فقط ۲۲درصد از کاربران توافق کردند که از مزایای دستگاه های هوشمند هیچ نگرانی در مورد حریم خصوصی ندارند.(آتزوری،۲۰۱۰)

۳-۶-۲.چالش امنیتی

www.jozve.org

به عنوان یک عدد در حال رشد از انواع دستگاه های متصل به شبکه اینترنت اشیا معرفی تعدیدهای امنیتی از اهمیت بالایی برخوردار است .اگر چه بهره وری شرکت ها و افزایش کیفیت زندگی مردم اینترنت اشیا را بهبود می بخشد اما اینترنت اشیا را نیز به سطوح حمله احتمالی برای هکرها و دیگر مجرمان اینترنتی تبدیل می کند.یک مطالعه اخیر توسط هیولت پاکارد(2014THP)نشان داد که 70% از دستگاه های اینترنت اشیا بیشتر مورد استفاده شامل آسیب های جدی هستند.دستگاه های اینترنت اشیا به علت عدم عدم رمزگذاری انتقال،رابط وب ناامن ،حفاظت ناکافی از نرم افزار،آسیب پذیرند.به طور متوسط،هر دستگاه شامل ۲۵ حفره و خطرات ناشی در شبکه خانگی هستند .دستگاه های موجود در اینترنت اشیا به طور معمول بدون انجام تکنیک های رمزنگاری داده ها استفاده کنید.

برخی از برنامه های اینترنت اشیا از زیرساخت های حساس و خدمات استراتژیک مانند شبکه های هوشمند و حفاظت از تاسیسات پشتیبانی می کنند.دیگر برنامه های کاربردی اینترنت اشیا به طور فزاینده مقدار زیادی از اطلاعات شخصی در مورد خانواده ،سلامت و وضعیت مالی تولید می کنند که شرکت قادر خواهد بود آن را به اهرمی برای کسب و کار خود تبدیل کنند.عدم امنیت و حریم خصوصی در تصویب اینترنت اشیا توسط شرکت ها و افراد مقاومت ایجاد خواهد کرد.چالش ها ی امنیتی ممکن است توسط آموزش به توسعه دهندگان و ترکیب راه حل های امنیتی (به عنوان مثال،سیستم پیشگیری از نفوذ ،فایروال)به محصولات و تشویق کاربران به استفاده از ویژگی های امنیتی اینترنت اشیا که در دستگاه های خود را ساخته شدده است،حل شود.(مرتضی یوسفی و همکاران،۱۳۹۵)

۳-۶-۳.چالش هرج و مرج

تکامل فناوری اینترنت اشیا (به عنوان مثال،چیپیست،سنسور ،فناوری بی سیم)بیش از حد شتاب است که بسیار سریع تر از چرخه نوآوری محصول مصرفی معمولی است.استندارد های هنوز در امنیت کافی ،مسائل

www.jozve.org

خصوصی،ارتباطات پیچیده و شمارکثیری از دستگاه های ضعیف تست نشده است.اگر به دقت طراحی نشوند،دستگاه های چند منظوره و برنامه های کابردی مشترک می تواند زندگی ما به هرج و مرج تبدیل کنند.در یک دنیای بی ارتباط یک خطای کوچک یا اشتباه می تواند فقط مربوط به همان بخش است.بااین حال ،در یک جهان بیش از حد انلاین یک خطا در یک بخش از یک سیستم می تواند باعث اختلال در سراسر سیستم شود.برنامه های کاربردی خانه های هوشمند و نظارت پزشکی و سیتم های کنترل از سنسور های پیوسته و دستگاه های ارتباطی و کنترلی تشکیل شده است.اگر یک سنسور از یک سیستم نظارت پزشکی یا سیستم های کنترلی دچار اختلال در عملکرد شوند،کنترل کننده ممکن یک سیگنال نادرست دریافت کند ،که ممکن است منجر به مرگ بیمار شد.تصور آن دشوار نیست که کیت خانه های هوشمند مانند ترموستات و... شکسته شود و یا توسط هکرها مورد حمله قرار گیرد که باعث ایجاد مشکلات ایمنی غیر منتظره می شود.یک دستگاه واحد ممکن است مشکل ناچیز ایجاد کند،اما برای سیستم به عنوان یک کل واکنش زنجیره ای از دیگر دستگاه های متصل می تواند تبدیل به مشکلی برزگ شود.برای جلوگیری از هرج و مرج در اینترنت اشیا جهان بیش از حد در ارتباط کسب و کارها نیاز به تلاش برای کاهش پیچیدگی سیتسم های متصل شده،افزایش امنیت و استاندارد برنامه های کاربردی و تضمین امنیت و حریم خصوصی کاربران در هر زمان و هر جا و در هر دستگاهی دارند. (آتزوری،۲۰۱۰)

۳-۷.مشخصه های بسیار مرتبط برای امن کردن اینترنت اشیا

کاملا واضح است که اکثرچیزهای مهم در IOT اعتبار سنجی دوجانبه و راهی برای امن کردن ارتباط با هر کدام از ((اشیا))هستند.جهت استفاده از مجموعه ای از اشیا باید نوعی اعتماد بین منابع اطلاعاتی و سینک ها به وجود بیاید.اعتماد جهت باور کردن اطلاعاتی که هر چیزی ارسال می کند،نیاز است.در هنگام ارتباط ما باید مطمئن باشیم که داده ها صحیح هستند،که ابتداء باید مطمئن شویم که ما در یک دستگاه

www.jozve.org

(۰درست)۹هستیم و داده های ارسال شده توسط این دستگاه در مسیر رسیدن به مقصد اغییری نکرده اند(یعنی اطمینان از یکپارچگی) به همین دلیل است که ما برروی اولین گام در فرایند نصب یک محیط IOTیعنی متصل کردن اشیا تمرکز کرده ایم.ما می خواهیم قادر به تضمین این باشیم که در حال صحبت با دستگاه درست هستیم لذا شما در حال ایجادیک زنجیره ی اعتماد هستید . (گوبی و همکاران ، ۲۰۱۳)

۳-۸.فایروال و سیاست های تحرک در اینترنت اشیاء

اینترنت اشیا برای ارائه یک شبکه که در آن جریان های اطلاعاتی به راحتی می توانند بین هر مجموعه انواع محصولات ،دستگاه ها ،کاربران و سیستم های اطلاعاتی ارتباط برقرار کنند در نظر گرفته شده است.این دیدگاه به دلیل توسعه پیوسته مفاهیم سیستم های جدید اطلاعاتی و فن آوری ها به واقعیت نزدیک می شود . بااین حال این واقعیت جدید نیاز به توجه ویژه در جنبه های خاصی از اینترنت اشیا مانند امنیت و تحرک است.اول افراد و شرکت ها امنیت دارایی های اطلاعاتی /داده ها را با استفاده از فایروال ها می خواهند،که به ناچار به یک درگیری و به چالش کشیده شدن بین امنیت داده ها ئ قابلیت استفاده می انجامد .دوم ، محصولات به طور فزاینده ای در حال تبدیل شدن در قالب تلفن همراه هستند،فعالیت های محیط هایی که در آن تماس با آنها به طور مستقیم با استفاده از آدرس IPشان می تواند مشکل باشد(به عنوان مثال محدودت های دسترسی).بنابراین در برخی از برنامه های اینترنت اشیا ممکن است فعال کردن ارتباطات دو طرفه از طریق هر نوع فایروال لازم باشد،به عنوان مثال،برای فعال کردن کنترل در زمان واقعی و تعمیر و نگهداری.

در اصطلاح اینترنت اشیا ئ سیستم های فیزیکی سایبری (CPS)،کاربران تلفن همراه و اشیاء به صورت پویا به کشف و تعامل با محاسبات ناهمگن،منابع فیزیکی و همچنین داده های مجازی و محیط ها قادر خواهند بود. این دیدگاه به دلیل افزایش روزانه مفاهیم و فن آوری ها مانند سخت افزار یا نرم افزار سنسور ،معنایی،ابری،مدل سازی داده ها،ذخیره سازی،استدلال، و غیره به واقعیت نزدیک می شود. میلیاردها دستگاه به

www.jozve.org

اینترنت متصل شده و پیش بینی شده که در سال ۲۰۲۰به حدود ۵۰-۱۰۰میلیارددستگاه برسد.استانداردسازی در نمونه اینترنت اشیا بسیار مهم است زیرا باعث افزایش قابلیت تبادل اطلاعات و توسعه پذیری می شود،اما هنوز هم یک نیاز واقعی برای نسل کافی و به طور کلی سطح نرم افزاری در استانداردهای پیام رسانی اینترنت اشیا وجود دارد.تفسیر اینترنت اشیا ارائه شده واقعی تر است ،جایی که اینترنت اشیا به این معنا که "یک سیستم اطلاعاتی عمومی برای دسترسی و هماهنگ سازی هر نوع اطلاعات محصول مرتبط ،به طور عمده از طریق اینترنت "استفاده شده است.در این تفسیر،تمرکز به کل چرخه عمر محصول داده می شود،که در آن محصول از طریق مناطق کسب وکارپیچیده و تبادل اطلاعات یکپارچه میان تمام سهامداران کالا و سیستم های درگیر است .طراحی چنین رابط هایی یک گام ضروری به منظور افزایش مدیریت چرخه عمر محصول(PLM) است،در حالی که امکان ایجاد درست یک اینترنت اشیا را ممکن سازد .بااین حال ،شرایط مناسب برای یک استاندارد مشترک تبادل داده ها بین سازمان هایی که رسیده اند و با حتی ارائه شده برای اینترنت اشیا ایجاد نشده است.گسترش تلفن های همراه و دستگاه های محاسبات فراگیر در طول دهه گذشته باعث ایجاد میزبان و تحرک خدمات در اینترنت شده که یک مسئله قابل توجه است.ارائه داده ها به یک میزبان تلفن همراه در سراسر تغییر آدرس شبکه بدون اخلال اتصالات موجود یک چالش اصلی باقی مانده است. .برای حل این مشکل مردم اقدامات پیشگیرانه را برای اطمینان از امنیت نحرمانه بودن و یکپارچگی دارایی های اطلاعاتی /داده ها بااستفاده از دیوار آتش و سیستم های پروکسی که به ناچار به یک درگیری برای به چالش کشیدن بین امنیت داده ها و قابلیت استفاده انجام می دهند امنیت برای انجام خدمات جدید چالش بیشتری ایجاد می کند،در حالی که قابلیت استفاده به منظور دستیابی به تایید کاربر از آن خدمات نیاز دارد. این اساسا درست است که در نظر گرفتن کل چرخه عمر محصول از اطلاعات مربوط به محصول یک منبع ارزشمند برای شرکت هاست ئ نباید توسط سازمان های دیگر دیده شود.در مظر گرفتن محیط ها با فایروال و ساسیت های تحرکی،اجازه دادن به اشتراک گذاری اطلاعات در مد p2pبا وجود حضور فایروالها،NANها،و یا سیستم های مشابه(به عموان مثال

www.jozve.org

هنگامی که برای توسعه کنترل زمان واقعی و یا پیش بینی خدمات تعمیر و نگهـداری در اینترنـت اشـیا)ممکن است مفید باشد.(اکباتانی،۱۳۹۴)

www.jozve.org

فصل چهارم:

نتیجه گیری

www.jozve.org

۴-۱. نتیجه‌گیری

اینترنت اشیاء با توجه به ظرفیت بالای آن در تبدیل اشیاء فیزیکی از حوزه‌های کاربردی مختلف به میزبان‌های اینترنت، انتظارات بالایی را از خود ایجاد کرده است. با این حال، مهاجمان نیز ممکن است از پتانسیل بزرگ اینترنت اشیاء به عنوان یک راه جدید برای به تهدید انداختن امنیت و حریم خصوصی کاربران استفاده کنند. بنابراین، راه‌حل‌های امنیتی برای اینترنت اشیاء باید توسعه داده شود. همانند شبکه‌های معمولی، سیستم‌های تشخیص نفوذ (IDS) برای اینترنت اشیاء نیز مهمترین ابزار امنیتی به حساب می‌آیند.

در این تحقیق، ما به مرور و بررسی تلاش‌های تحقیقاتی صورت گرفته در زمینه‌ی سیستم‌های تشخیص نفوذ برای اینترنت اشیاء پرداخته‌ایم. ما ۱۸ مقاله را انتخاب کرده‌ایم که روش‌های خاص IDS را برای اینترنت اشیاء ارائه نموده‌اند یا استراتژی‌های تشخیص مهاجم را برای اینترنت اشیاء توسعه داده‌اند که می‌تواند بخشی از یک IDS باشد. این مقاله‌ها بین سال‌های ۲۰۰۶ و ۲۰۱۶ منتشر شده‌اند. ما یک طبقه‌بندی از این مقالات ارائه کرده‌ایم که بر اساس ویژگی‌های زیر طبقه‌بندی شده‌اند: روش تشخیص، استراتژی استقرار IDS، تهدیدات امنیتی، و استراتژی ارزیابی و تایید. ما مشاهده نمودیم که تحقیقات در مورد روش‌های IDS برای اینترنت اشیاء همچنان در دوران ابتدایی قرار دارند. راه‌حل‌های ارائه شده طیف وسیعی از حملات و فناوری‌های اینترنت اشیاء را پوشش نمی‌دهند. علاوه بر این، مشخص نیست که کدام یک از روش‌های تشخیص و استراتژی‌های استقرار برای سیستم‌های اینترنت اشیاء مناسب هستند. در نهایت، استراتژی‌های ارزیابی و تایید نیز به خوبی تثبیت نشده‌اند.

www.jozve.org

۴-۲. پیشنهادات

به عنوان تحقیقات آینده، محققان ممکن است بر روی مسائل زیر تمرکز کنند:

- بررسی نقاط قوت و ضعف روش‌های مختلف تشخیص و استراتژی‌های متفاوت استقرار
- افزایش محدوده‌ی تشخیص حمله
- بررسی فناوری‌های بیشتری از اینترنت اشیاء
- بهبود استراتژی‌های ارزیابی و تایید
- بهبود امنیت مدیریت و هشدار ترافیک
- توسعه‌ی کاربردهای آینده از قبیل همبستگی هشدار و سیستم‌های مدیریت خودکار.

www.jozve.org

فهرست منابع و مآخذ

www.jozve.org

آیه عطاریان،۱۳۹۵ ،پاردایم امنیت در پلت فرم اینترنت اشیا، ششمین همایش پژوهش های نوین در علوم و فناوری

غلامحسین اکباتانی فرد،سیده حورا فخر موسوی،مجید مظفری،۱۳۹۴، تامین امنیت در اینترنت اشیا با ارایه روشی استاندارد در مورد فایروال و سیاست های تحرک ، دومین کنفرانس بین المللی وسومین همایش ملی کاربرد فناوری های نوین در علوم مهندسی

مرتضی یوسفی، عباداله زهره وندی ، ۱۳۹۵،اینترنت اشیاء، برنامه های کاربردی و چالش های توسعه ،کنفرانس بین المللی مهندسی کامپیوتر و فناوری اطلاعات

Atzori, L., Lera, A. and Morabito, G. (2010),“ The Internet of Things: A Survey,” Computer Networks, 54(15): pp. 2787–2805

Bruno Bogaz Zarpelão, , Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de ,2017,A survey of intrusion detection in Internet of Things, Journal of Network and Computer Applications.

Gubbi, A., Buyya, T., Marusic, S. and Palaniswami M. (2013),“ Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, **29** : pp. 1645–1660.

J. Sen, “A Survey on Wireless Sensor networkSecurity”, International Journal of CommunicationsNetwork and Information Security, vol. 1, no. 2, (2009)August, pp. 59-82.

M. Sharifnejad, M. Shari, M. Ghiasabadi and S.Beheshti, “A Survey on Wireless Sensor NetworksSecurity”, SETIT, (2007,)

Roy, Bibhash, SumanBanik, ParthiDey, SugataSanyaland NabenduChaki, "Ant colony based routing formobile ad-hoc networks towards improved quality ofservices." Journal of Emerging Trends in Computingand Information Sciences 3.1 (2012): 10-14.

www.jozve.org