مجله‌ی علمی پژوهش در علوم رایانه، شماره ۳۰، تابستان ۱۴۰۲، ص ۴۳- ۲۵

ISSN: 2745-3673
http://www.Rcsj.ir

مجله علمی پژوهش در علوم رایانه (سال هشتم)
شماره ۳۰ / تابستان ۱۴۰۲ / ص ۴۳- ۲۵

مروری بر عملکرد سیستم های تشخیص نفوذ در اینترنت اشیاء

مهرناز مودی
گروه برق و کامپیوتر، دانشکده فنی و مهندسی، دانشگاه تربت حیدریه.

نام نویسنده مسئول:
مهرناز مودی

تاریخ دریافت: ۱۴۰۲/۰۴/۱۴
تاریخ پذیرش: ۱۴۰۲/۰۶/۲۱

چکیده

با رشد روزافزون فناوری اطلاعات و استفاده گسترده از شبکه های کامپیوتری، امنیت شبکه به عنوان یکی از مباحث بسیار مهم و چالش برانگیز این حوزه مطرح است. نفوذ در شبکه های کامپیوتری با انگیزه های مختلف مالی، سیاسی، نظامی و یا برای نشان دادن ضعف امنیتی موجود در برنامه های کاربردی، ضعف امنیتی در طراحی شبکه و پروتکل های آن صورت می گیرد. سیستم های تشخیص نفوذ ابزارهای امنیتی هستند که برای تامین امنیت ارتباطات در سیستم های اطلاعاتی مورد استفاده قرار می گیرند. سیستم های تشخیص نفوذ براساس روش مورد استفاده برای تشخیص نفوذ به دو دسته مبتنی بر امضا و مبتنی بر ناهنجاری تقسیم می شوند. از طرفی اینترنت اشیاء، فناوری نوظهوری است که اینترنت و اشیای هوشمند فیزیکی را ادغام می کند، اشیایی که به دامنه‌های گسترده ای از قبیل خانه‌ها و شهرهای هوشمند، فرآیندهای صنعتی و نظامی، نظارت بر بهداشت و سلامت انسانها، کسب وکار و کشاورزی تعلق دارد. فناوری اینترنت اشیا، حضور وسایل متصل به اینترنت را در فعالیتهای روزانه ما عمیق تر می کند و مزایای زیادی را در کیفیت زندگی به همراه دارد و از طرفی چالش های مرتبط با مسائل امنیتی نیز ایجاد کرده است. براین اساس، راه حل های امنیتی برای اینترنت اشیا باید توسعه داده شود. همانند سایر شبکه ها، سیستم های تشخیص نفوذ برای اینترنت اشیاء نیز، مهمترین ابزار امنیتی به حساب می آید. در پژوهش حاضر استراتژی‌های قرارگرفتن سیستم های تشخیص نفوذ در اینترنت اشیاء و روش های تشخیص نفوذ در اینترنت اشیاء مورد بررسی قرار گرفته است.

واژگان کلیدی: تشخیص نفوذ، اینترنت اشیاء، شبکه، امنیت، الگوریتم هوشمند.

مجله‌ی علمی پژوهش در علوم رایانه، شماره ۳۰، تابستان ۱۴۰۲، ص ۴۳- ۲۵

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه ای بر سیستم های تشخیص نفوذ

نفوذ را می توان به عنوان اقداماتی که تلاش می کند جامعیت، محرمانگی و دسترس پذیری منبع ها را به خطر اندازد تعریف کرد. نفوذ حاصل یک تهاجم عمدی و بدخواهانه روی مجموعه‌ای از آسیب‌پذیری‌های سیستم است که در بهترین شرایط، باعث بروز دسترسی‌های غیرمجاز و در بدترین حالت باعث خرابی یا رفتارهای غیرقابل پیش‌بینی در سیستم می‌شود[1]. تشخیص نفوذ، فرآیند نظارت و تجزیه و تحلیل وقایع در یک سیستم کامپیوتری یا شبکه، به منظور تشخیص فعالیت‌های غیرعادی است. هدف از تشخیص نفوذ، بررسی پیاده سازی و سیاست امنیتی یک سازمان است. اساسا برای مشاهده این که آیا سازمان، معیارهای امنیتی که در سیاست امنیتی مشخص کرده است را به درستی پیاده‌سازی کرده یا نه استفاده می‌شود. [2,3]

سیستم تشخیص نفوذ چیست؟

سیستم‌های تشخیص نفوذ (IDS[1]) که به منظور تشخیص فعالیت های غیرعادی مورد استفاده قرار می‌گیرند، در سال‌های اخیر مورد توجه بسیاری از محققین قرار گرفته است و مدلهای مختلفی به منظور شناسایی و جلوگیری از حملات و برقراری امنیت ارائه و طراحی شده اند. یک سیستم تشخیص نفوذ کلیه فعالیت های موجود بر روی شبکه را تجزیه و تحلیل کرده و با استفاده از اطلاعات موجود بر روی پایگاه داده خود تعیین می کند که فعالیت انجام شده مجاز یا غیر مجاز است و همچنین تعیین می کند که آیا این فعالیت می‌تواند آسیبی به شبکه شما وارد کند یا خیر و در نهایت به شما در مورد این گونه فعالیتها اطلاع رسانی می‌کند. این اطلاع رسانی معمولا از طریق ارسال هشدار به مدیر سیستم انجام می شود. یک IDS در حقیقت یک نوع اسنیفر بسته[2] محسوب می‌شود بطوری که کلیه بسته های ارسالی و دریافتی در شبکه را دریافت کرده و آن ها را تجزیه و تحلیل می کند، این سیستم توانایی فعالیت با انواع پروتکل های ارتباطی در شبکه به ویژه توانایی فعالیت با پروتکلTCP/ IP را داراست [4, 5].اجزای سامانه های تشخیص نفوذ به شرح زیر می باشد.

- **حسگر یا عامل:** جزئی از سیستم که به جستجوی ترافیک شبکه می پردازد. این اصطلاح گاهی اشاره به سیستم های تشخیص نفوذ مبتنی بر میزبان دارد.
- **سرور مدیریت:** واحد مرکزی سامانه‌های تشخیص نفوذ است که داده را از حسگر سیستم و قسمت های مختلف سیستم دریافت می‌کند. بعضی از سرورهای مدیریت می‌توانند بر روی داده های دریافتی، تحلیل های انجام دهند و به این ترتیب وقوع رویدادهایی را در شبکه پویش کنند. برقراری رابطه میان داده های دریافت شده از سمت حسگرهای مختلف، مثل مسیرهای یکسانی که در سنسورهای مختلف، رویدادهایی ایجاد کرده اند منجر به کشف همبستگی بین رخدادهای در جریان، در کل بستر شبکه می شود.
- **سرور پایگاه داده:** سرور پایگاه داده وظیفه ثبت تمامی رخدادها و هشدارهای دریافت شده توسط حسگرها یا سرور مدیریت را بر عهده دارد. سرور پایگاه داده در بیشتر سیستم‌های تشخیص نفوذ استفاده می شود.
- **واسط کاربری:** واسط کاربری (کنسول[3]) برنامه‌ای است که روی یک کامپیوتر نصب شده و واسط کاربران و یا مدیر سیستم می شود. مدیر سیستم می تواند از طریق آن به پیکربندی قسمت‌های مختلف سیستم، حسگرها، بروزرسانی نرم افزار و یا ایجاد تغییرات نرم‌افزار بپردازد. همچنین امکان مشاهده رخدادهای ثبت شده و نیز پویش وضعیت فعلی و رخدادهای در جریان امکان پذیر است.
- **طعمه مجازی:** بسیاری از سیستم ها برای یافتن اقدامات جدید و نفوذی که ممکن است الگوهای ناشناخته داشته باشند، از تکنیک طعمه مجازی استفاده می‌کنند. این تکنیک یکی از میزبانهای شبکه است که هیچگونه سرویسی را ارائه نمی دهد و تنها کاربر آن مدیر طعمه مجازی است. به همین خاطر هیچگونه دسترسی از داخل یا خارج شبکه به آن نباید

[1] Intrusion Detection System
[2] Sniffer-Packet
[3] Console

ISSN: 2745-3673
http://www.Rcsj.ir

وجود داشته باشد. در نتیجه هرگونه دسترسی به آن می تواند به عنوان یک اقدام مشکوک شناسایی شده و منبع این دسترسی و IP مربوطه، شناسایی می شود و برای بررسی آن اقدامات لازم صورت می گیرد [6].

انواع سیستم‌های تشخیص نفوذ

سیستم‌های تشخیص نفوذ براساس مکان قرارگیری در سیستم شبکه و دامنه فعالیت به دو گروه سیستم‌های تشخیص نفوذ مبتنی بر میزبان و سیستم‌های تشخیص نفوذ مبتنی بر شبکه طبقه بندی می شوند. معمولا برای دستیابی به حداکثر کارایی و امنیت، این سیستم های تشخیص نفوذ به صورت ترکیبی نیز مورد استفاده قرار می‌گیرند که با نام سیستم های تشخیص نفوذ توزیع شده شناخته می شوند.

- **سیستم های تشخیص نفوذ مبتنی بر میزبان** (Host-Based): برنامه هایی هستند که بر روی یک سیستم نصب می شوند و ترافیک یا رویدادها را بر اساس لیستی از امضاهای شناخته شده برای آن سیستم عامل، فیلتر می کنند. این سیستم ها می توانند حملات و تهدیداتی مانند دسترسی به فایلها، اسبهای تراوا و ... را روی کامپیوتر میزبان تشخیص دهند. از این گونه سیستم ها به دلیل ایجاد بار کاری زیاد بر رویCPU، معمولا کمتر استفاده می شود. نرم افزار مربوط به اینگونه سیستم تشخیص نفوذ به صورت تک به تک بر روی تمام سیستم ها نصب می شود و بصورت مجزا فعالیت می کنند. این سیستم ها فقط بسته های ورودی و خروجی به یک کامپیوتر را بررسی و نظارت کرده و هنگام تشخیص نفوذ و یا فعالیت مشکوک به مدیر شبکه و یا کاربر کامپیوتر هشدار می دهند.

امتیاز مهم این سیستم ها توانایی سازماندهی مناسب تصمیمات برای هر میزبان به صورت اختصاصی و منحصر به فرد است. به عنوان مثال لازم نیست روی میزبانی که سرویسDNS[4]را اجرا نمی‌کند قوانین چندگانه‌ای که برای تشخیص سوء استفاده از DNS طراحی شده اند مورد بررسی قرار داده شوند، در نتیجه با کاهش قوانین مربوطه کارایی افزایش پیدا می کند و استفاده از پردازنده برای هر میزبان کاهش پیدا می کند. همچنین سیستم‌های تشخیص نفوذ مبتنی بر میزبان اطلاعات مشخصی در مورد اینکه نفوذ از کجا و توسط چه کسی و چه موقع اتفاق افتاده است را فراهم می‌کنند. در این سیستم ها احتمال هشدار نادرست کم است.

از معایب سیستم های تشخیص نفوذ مبتنی بر میزبان، میتوان به سازگاری کم بین سیستم عامل و نرم افزارهای چندگانه اشاره کرد. اغلب این سیستم ها برای یک سیستم عامل نوشته می شوند. همچنین این سیستم ها برخی از حملاتی را که در لایه های پایین شبکه انجام می شوند، شناسایی نمی کنند.

- **سیستم های تشخیص نفوذ مبتنی بر شبکه** (Network-Based): سیستم‌های تشخیص نفوذ مبتنی بر شبکه نظارت و تجزیه و تحلیل ترافیک سراسر شبکه، به منظور شناسایی تهدیدات را به عهده دارند. این سیستم ها فعالیت های مخربی مانند حملات انکار سرویس(DOS[5])، اسکن پورت و... را در تمام شبکه شناسایی می کنند. سیستم‌های تشخیص نفوذ مبتنی بر شبکه به صورت سخت افزار یا نرم افزارهایی هستند که برای پویش ترافیک عبوری در کل شبکه و کامپیوترهای موجود در شبکه در مکان یا مکان های خاصی از شبکه قرار داده می شوند و ترافیک شبکه را مورد تحلیل قرار می دهند، هنگامی که حمله یا رفتار غیرعادی تشخیص داده شود، یک پیغام هشدار برای مدیر شبکه ارسال می شود.

سیستم های تشخیص نفوذ مبتنی بر شبکه به دلیل اینکه در لایه شبکه عمل می کنند، به سیستم عامل وابستگی ندارند. این سیستم ها ترافیک شبکه را به ازای هر بسته عبوری از شبکه در زمان واقعی و به صورت بلادرنگ یا نزدیک به آن به منظور شناسایی الگوهای نفوذ مورد بررسی قرار می دهند.

[4] Domain Name System
[5] Denial of Service

ISSN: 2745-3673
http://www.Rcsj.ir

یکی از چالش‌هایی که سیستم های تشخیص نفوذ مبتنی بر شبکه با آن روبرو هستند این است که این سیستم ها بایتها، بسته ها و جریان را برای تشخیص نفوذ بررسی می‌کنند، به همین دلیل در شبکه های با سرعت بالا، نظارت بر تمام بسته ها غیر ممکن است. این سیستم ها قادر به جمع‌آوری داده ها با سرعت بالا نیستند و در شبکه هایی با سرعت بالای100 Mbps دچار مشکل می شوند و بسیاری از بسته های عبوری را از دست می دهند. همچنین حمله های با ارتباط رمزنگاری شده رو به افزایش است و محتوای بسته های رمزنگاری شده برای سیستم تشخیص نفوذ غیر قابل دسترسی است که برای رفع این مشکل تحلیل جریانهای شبکه به جای تحلیل هر بسته بهترین گزینه جهت نظارت و تحلیل است [3, 7, 8] .

ساختار و همبندی اجزای سیستم تشخیص نفوذ

اجزای سیستم های تشخیص نفوذ می توانند از طریق شبکه مجزا با هم ارتباط پیدا کنند. همچنین این امکان وجود دارد که بر روی بستر شبکه اصلی، ارتباط اجزای سیستم برقرار شود. در روش اول یک شبکه کامل مجزا و جدا از شبکه اصلی به نام شبکه مدیریت برای ارتباط ایجاد می شود، بنابراین حسگرهای به کار رفته در سیستم نیاز به واسط شبکه جداگانه ای برای ارتباط با شبکه مدیریت دارند، ولی بخش های دیگر سیستم مثل سرور پایگاه داده و سرور تحلیل، تنها به شبکه مدیریت اتصال دارند. از مزایای این طرح این است که سیستم تشخیص نفوذ از دید مهاجمین پنهان می ماند و امنیت آن در مقابله با انواع حملات حفظ می‌شود. در مقابل هزینه اضافی نصب و ایجاد ارتباطات برای ایجاد شبکه لازم می باشد. در مواردی که ایجاد شبکه فیزیکی مجزا امکان‌پذیر نباشد، استفاده از شبکه های مجازی بر روی بستر شبکه اصلی مرسوم می باشد، تا امنیت ارتباطات تامین گردد. با این حال این روش در مقایسه با روش قبل، امنیت و کارایی کمتری دارد. برای مثال در حملات سیستم تشخیص نفوذ می تواند به خود قربانی حمله شود و امکان برقراری ارتباطات و کارکرد مناسب مختل شود [9].

عملکرد امنیتی سیستم های تشخیص نفوذ

این سیستم ها می توانند عملکردهای امنیتی و شناسایی مختلفی را داشته باشند که خروجی آن ها را برای واحد مدیریت داخلی شبکه کاربرد دارد. این قابلیت ها را می‌توان در سه دسته قابلیت های شناسایی شبکه، پویش و ثبت رخدادها و فعالیت های مرتبط با بازدارندگی از بروز حملات و آسیب های ممکن دسته بندی نمود. قابلیت های شناسایی شامل بررسی و شناسایی میزبان های فعال در شبکه، فعالیت های آن، پروتکل های ارتباطی مورد استفاده، نرم افزارهای مورد استفاده و دیگر خصوصیات عمومی شبکه است. سیستم های تشخیص نفوذ کارکرد گسترده‌ای در پویش و ثبت انواع رخدادهای شبکه دارند. این رخدادهای ثبت شده می‌توانند برای بررسی صحت هشدارهای صادر شده و بررسی ارتباط میان رخدادهای به وقوع پیوسته مورد استفاده قرار گیرند. در مورد هر کدام از رویدادها، زمان وقوع، نوع رخداد، درجه اهمیت آن و نیز اقدام بازدارنده صورت گرفته (در صورت وجود) در پایگاه داده ثبت می شود. این وقایع ثبت شده، هم به صورت محلی و هم به صورت متمرکز در سرور مرکزی ذخیره می‌شوند تا امنیت آن‌ها حفظ شود. زمان ثبت رویدادهای مختلف از جانب اجزای مختلف شبکه باید بر اساس یک ساعت مرکزی هماهنگ باشند. برای ایجاد این هماهنگی میتوان از پروتکلی مانند پروتکل زمانبندی شبکه ای یا هر روش خاص دیگری استفاده کرد که در نهایت تمام وقایع بر اساس برچسب‌های زمانی هماهنگ شده ثبت شوند.

مهمترین قابلیت ابزارهای تشخیص نفوذ، همان تشخیص حملات و اقدامات مخرب می‌باشد. برای این کار از روش-های مختلف تشخیص نفوذ استفاده می شود. عمده ابزارهای تشخیص نفوذ از ترکیبی از روش های سیستم های تشخیص نفوذ به منظور تشخیص انواع حملات استفاده می کنند، تا به دقت و بازدهی مورد نظر دست یابند. تکنولوژی های مختلف ابزارهای IDS قابلیت های مختلفی را برای فاز تنظیم و نصب سیستم و نیز سفارشی کردن آن ارائه می دهند. هر چه قابلیت های سیستم در موقع نصب و سفارشی کردن بیشتر و بهتر باشد، سیستم نصب شده به پیکربندی اولیه، عملکرد بهتری را می تواند ارائه دهد. به این دلیل، هنگام انتخاب ابزار تشخیص نفوذ مناسب، این قابلیت ها باید دقیق مورد بررسی قرار گیرد. از جمله این قابلیت ها می توان به این موارد اشاره کرد:

ISSN: 2745-3673
http://www.Rcsj.ir

- **حدود آستانه:** فاصله کمیت های مربوط به حالت عادی از حالت غیرعادی سیستم را مشخص می کند. این کمیت ها به طور مثال می توانند تعداد تلاش های مجاز یک مشتری برای ورود به سیستم در مدت ۶۰ ثانیه اخیر باشد که اگر از حدی تجاوز کند، مشکوک است.
- **لیست های سیاه و سفید:** لیست سیاه شامل انواع موجودیتهای متفاوتی است که بنا به سابقه سیستم، مرتبط با فعالیت های مخرب تشخیص داده شده اند. این موجودیت ها می توانند شامل مشتری های خاص، آدرسIP، شماره درگاه TCP یاUDP، اسامی کاربری، اسامی فایل و... باشند. لیست های سیاه این امکان را فراهم می آورند تا با استفاده از تجربه گذشته سیستم و سابقه اقدامات مخرب کشف شده توسط سیستم، عوامل آنها را شناسایی کنیم و در دسترسی های بعدی در مورد آنها سیاست های خاصی را اعمال کنیم. بسیاری از ابزارهای تشخیص نفوذ امکان ایجاد لیست سیاه را به صورت پویا فراهم می کنند. لیست های سفید به لیست عواملی گفته می شوند که برعکس لیست سیاه، به سیستم به عنوان فعالیت های خوشخیم شناسانده می شوند.
- **تنظیمات هشداردهی:** بسیاری از ابزارهای تشخیص نفوذ این امکان را دارند که روی نحوه هشداردهی آن‌ها تنظیمات خاصی صورت گیرد، از جمله:

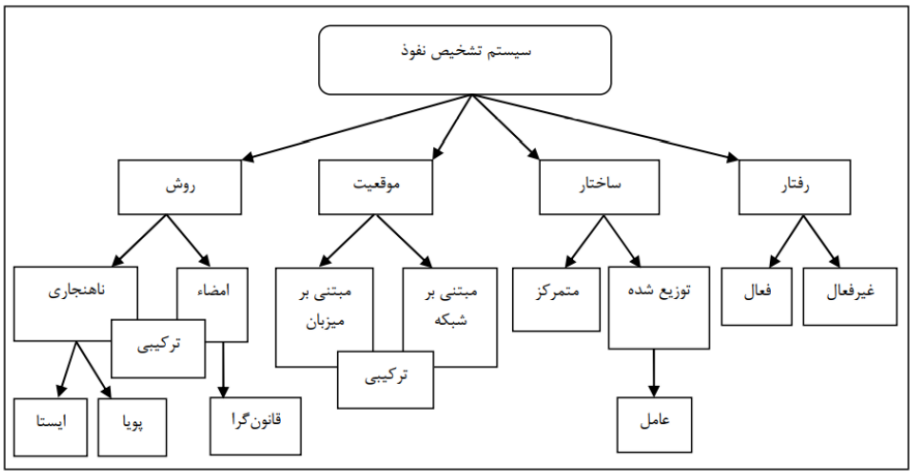
۱. هشدار کل خاموش شود.
۲. به هر کدام از انواع هشدارهای تولید شده درجه اولویت برای بررسی داده شود.
۳. مشخص کردن اینکه چه اطلاعاتی باید ذخیره شوند.
٤. از چه روشی برای هشداردهی استفاده شود (برای مثال از ایمیل برای اطلاع به مدیر سیستم استفاده شود) و هشدارهای تولید شده از طریق چه واسطی به واحد مدیریت شبکه منتقل شوند، تا بر اساس سیاست های امنیتی و پیشگیرانه پاسخی برای مقابله با آن فعالیت ایجاد شود.
٥. در مورد فعالیت های متعدد منجر به ایجاد هشدار تصمیم گرفته شود به صورتی که از ایجاد تعداد زیاد هشدارها جلوگیری شود. بسیاری از حمله کننده ها می توانند با مشغول کردن سیستم به تعداد زیادی هشدار، از این مساله سود برند و در لا به لای هشدارهای بی مورد کار اصلی خود را انجام دهند.

- **مشاهده کدهای خاص برنامه:** بعضی از ابزارهای تشخیص نفوذ امکان دیدن بعضی کد های مربوط به تشخیص نفوذ را برای مدیر سیستم فراهم می کنند. این مساله کمک می کند تا دلیل بعضی هشدار ها مشخص شود و بتوان فهمید هشدارهای داده شده در وضعیتهای خاص چقدر اهمیت دارند و آیا بی مورد هستند یا نه. همچنین این امکان هست تا کد بر اساس ویژگی های خاص شبکه تغییر کند. البته این اقدام باید شناخت کامل از ابزار و برنامه نویسی آن صورت گیرد تا عملکرد ابزار دچار مشکل نشود. مدیران شبکه باید در دوره های زمانی منظم به شرایط بارگزاری و پیکربندی سیستم توجه کنند، همچنین ممکن است نیاز باشد تنظیمات هشدار سیستم بر اساس شرایط گوناگون تنظیم مجدد شود، زیرا شرایط سیستم به مرور زمان تغییر می کند [10, 11].

طبقه بندی روشهای سیستم های تشخیص نفوذ

طبقه بندی سیستم های تشخیص نفوذ، که در تصویر (۱) نشان داده شده است، خانوادهٔ سیستم های تشخیص نفوذ را با توجه به خصوصیات آن‌ها تعریف می کند. روش‌های تشخیص نفوذ را می توان به دو روش مبتنی بر امضاء و مبتنی بر ناهنجاری تقسیم کرد. روش های تشخیص، هسته و پایه اصلی فناوری های تشخیص نفوذ هستند.

ISSN: 2745-3673
http://www.Rcsj.ir



تصویر (۱): طبقه بندی سیستمهای تشخیص نفوذ

تشخیص مبتنی بر امضاء: در این روش که همانند کاری است که یک آنتی ویروس انجام می دهد، IDS دارای یک پایگاه داده است که در آن نوع و روش فعالیت برخی از حملات مشخص شده اند، به محض اینکه IDS ترافیکی را تشخیص دهد، آن را با اطلاعات پایگاه داده مربوطه مقایسه کرده و در صورت بروز تطابق اعلام هشدار می کند. سیستم های تشخیص نفوذ مبتنی بر امضاء به عنوان سیستم های تشخیص نفوذ مبتنی بر دانش نیز شناخته می شوند. این سیستم ها اشاره به یک پایگاه داده از حملات قبلی، امضاءها و آسیب پذیری های سیستم دارند. معنی کلمه امضاء وقتی که درباره سیستم های تشخیص نفوذ صحبت می شود، به عنوان یک مدرک ثبت شده از یک نفوذ یا یک حمله است. هر نفوذ یک اثر انگشت یا ردپا به جای می گذارد که این اثر انگشت یا ردپا، امضاء یا الگو نامیده می شود و می تواند جهت شناسایی حملات مشابه در آینده مورد استفاده قرار گیرد.

این سیستم ها یک پایگاه داده که شامل تعدادی امضاء از حملات شناخته شده است را آماده می کنند. داده های ممیزی جمع‌آوری شده توسط سیستم تشخیص نفوذ با محتوای پایگاه داده مقایسه شده و اگر با آن انطباق داشته باشد، یک هشدار صادر می شود. رخدادهایی که با مدل حملات تطابق نداشته باشند، به عنوان بخشی از فعالیت های قانونی در نظر گرفته می شوند. این روش برای حملات شناخته شده بسیار مؤثر است و تعداد کمی هشدار غلط تولید می کند. با این حال، این روش قادر نیست حملات جدید را تشخیص دهد. هنگامی که الگو حملات کمی تغییر داده شود، این روش نسخه های تغییریافته از حملات قدیمی را تشخیص نمی دهد. بنابراین، این روش تنها در تشخیص حملات از پیش شناخته شده، مؤثر است.

- **مزایا سیستم های تشخیص نفوذ مبتنی بر امضاء**

۱) هشدارهای اشتباه کمی دارند.
۲) ساده بودن روش تشخیص حملات.
۳) توانایی در تشخیص مؤثر تمامی الگوهای شناخته شده حملات.
۴) تحلیل های انجام شده، عمیق و مفصل است و موجب می شود فهم مشکل و اقدامات پیش گیرانه توسط مدیر امنیتی ساده تر شود.

- **معایب سیستم های تشخیص نفوذ مبتنی بر امضاء**

۱) ناتوانی در تشخیص حملات ناشناخته و جدید که نمونه امضائی برای آن ها تولید نشده است.
۲) ناتوانی در برابر حملاتی که از چند مرحله تشکیل شده اند و مبتنی بر یک سری رخدادهای متوالی هستند.
۳) الگوهای نفوذ باید مرتب به روز شوند.

ISSN: 2745-3673
http://www.Rcsj.ir

۴) در سرعت های بالا، کارا و قابل اجرا نیستند، زیرا باید تمامی بسته های اطلاعاتی را از لحاظ تطابق با تمامی الگوهای حمله مقایسه کنند.

تشخیص مبتنی بر ناهنجاری: در این نوع از انواع IDS سیستم با توجه به رفتاری که در شبکه عادی وجود دارد و ترافیکی که در اثر یک عمل غیرعادی ایجاد شده است و با توجه به بررسی های خود و مقایسه ترافیک طبیعی و غیرعادی، تصمیم می گیرد که در مورد این نوع ترافیک هشدار دهد. در سیستم های تشخیص نفوذ مبتنی بر ناهنجاری، نمایه های طبیعی (یا رفتارهای طبیعی) در سیستم نگهداری می شوند. سپس سیستم، داده های گرفته شده را با این نمایه ها مقایسه کرده و رفتار هر فعالیتی که از این نمایه ها انحراف داشته باشد را به عنوان یک نفوذ تلقی می کند و با اطلاع رسانی به مدیر امنیتی سیستم یا اتخاذ یک پاسخ مناسب در برابر آن اقدام می کند. برای تشخیص حملات جدید و همچنین مهاجمان داخلی ۲ مرحله باید دنبال شود:

– شناسایی رفتارهای نرمال و پیدا کردن قوانین ویژه برای آن ها (توصیف رفتار عادی به وسیله یادگیری خودکار)
– ایجاد نمایه هایی از رفتارهای عادی سیستم، شبکه، کاربران و گروه های کاربری

با بررسی ترافیک ورودی، رفتارهایی که از این نمایه ها پیروی می کنند، جزء رفتارهای عادی به حساب می آیند و فعالیتهایی که انحراف بیش از حد از مقادیر تعریف شده برای این نمایه ها دارند، به عنوان رفتارهای ناهنجار و تلاش های نفوذ شمرده می شوند. مهمترین روش های تشخیص ناهنجاری عبارتند از: تشخیص ناهنجاری آماری، تشخیص مبتنی بر داده کاوی، تشخیص مبتنی بر دانش و تشخیص مبتنی بر یادگیری ماشین.

- **مزایا سیستم های تشخیص نفوذ مبتنی بر ناهنجاری**

۱) قادر به تشخیص حملات جدید که تا به حال رخ نداده اند، هستند.
۲) این سیستم ها وابستگی کمی به مکانیزم های مربوط به سیستم عامل دارند.
۳) از آنجایی که الگوهای رفتارهای هنجار می توانند برای هر سیستم تشخیص نفوذ منحصر به فرد باشند، سیستم تشخیص نفوذ در برابر حملات نفوذ مقاوم تر است.
۴) سیستم های تشخیص ناهنجاری می توانند اطلاعاتی تولید کنند که در تعریف امضاء برای سیستم های تشخیص مبتنی بر امضاء مورد استفاده قرار گیرد.

- **معایب سیستم های تشخیص نفوذ مبتنی بر ناهنجاری**

۱) انتخاب یک مجموعه مناسب از پارامترها و ویژگی های سیستم، برای اندازه گیری و تشخیص حملات براساس آنها، مشکل و نیازمند تجربه زیادی است.
۲) دارای نرخ بالای هشدارهای غلط هستند؛ زیرا در مرحله یادگیری، پوشش دقیق تمام جنبه‌های رفتار یک سیستم امکانپذیر نیست. همچنین رفتار یک سیستم ممکن است با گذشت زمان تغییر کند.
۳) نگهداری فایل های نمایه، سربار قابل توجهی برای سیستم عامل دارد. همچنین بیشتر اوقات نیاز به مجموعه آموزشی برای ایجاد نمایه های طبیعی است.
۴) در مواردی که دامنه عملکرد سیستم وسیع باشد و رفتار عادی به مرور زمان تغییر کند، ایجاد نمایه رفتار عادی سیستم، کاری دشوار و زمان گیر خواهد بود [2].

معماری سیستم های تشخیص نفوذ

معماری سیستم‌های تشخیص نفوذ خیلی متنوع و گوناگون است. محققین به منظور جمع‌آوری داده‌ها، تحلیل و پاسخگویی در کل حیطه متمرکز، نامتمرکز، تعاملی و مستقل اجزایی کلیدی را برای این سیستم ها پیاده سازی کرده اند. در حال حاضر سیستم های تشخیص نفوذ، در گسترده ای از سیستم های مبتنی بر میزبان شخصی، که جمع آوری و تحلیل کلیه

ISSN: 2745-3673
http://www.Rcsj.ir

داده ها در آنها به صورت محلی صورت می گیرد، تا سیستم های مبتنی بر شبکه یا حتی سیستم های تعاملی توزیع شده بین چندین سازمان، که جمع آوری داده و تحلیل و پاسخگویی را هم به صورت محلی و هم توزیع شده انجام می دهند، قرار دارند. اگرچه این سیستم ها نیازمندی های متفاوتی دارند، اما به لحاظ عملکرد از یکسری اجزا تشکیل شده اند که به شرح زیر است:

حسگر: این جزء نقش نظارت بر ترافیک تحت پوشش را دارد و می تواند به صورت متمرکز و یا توزیع شده در شبکه قرار گیرد و وظیفه آن جمع آوری داده های لازم برای موتور یک سیستم تشخیص نفوذ می باشد. این داده ها بسته به نوع سیستم تشخیص نفوذ و روش بکار رفته در موتور آن می تواند کلیه بسته های ارسالی، بخشی از آن ها و یا حتی بخشی از محتوای آن ها باشد.

صف پیام: اطلاعات جمع آوری شده توسط حسگرها از طرق یک کانال ارتباطی به واقعه نگار ارسال می شود. این کانال بسته به ساختار حسگرها و معماری سیستم تشخیص نفوذ ممکن است بستر شبکه، یا یک لایه برنامه کاربردی باشد. در هر صورت به دلیل حجم بالای اطلاعات ارسالی از حسگرها نیاز به یک بافر واسط جهت ذخیره سازی موقت آنها و تحویل به واقعه نگار در زمان مناسب می باشد. صف پیام نقش این بافر را ایفا می کند.

واقعه نگار: این جزء نیز بسته به معماری سیستم تشخیص نفوذ ممکن است اصلا وجود نداشته باشد. اما در اکثر روش ها این جزء یک بخش ضروری از معماری به شمار آمده و وظیفه آن نگهداری کلیه اطلاعات جمع آوری شده توسط حسگرها در ساختار مناسب و قابل استفاده توسط تحلیلگر می باشد. ساختار این جزء نیز بسته به تکنیک استفاده شده در تحلیلگر متفاوت بوده و ممکن است فایل، پایگاه داده باشد.

تحلیلگر: شاید بتوان تحلیلگر را اصلی ترین جزء سیستم تشخیص نفوذ به شمار آورد. زیرا که پردازش و تحلیل داده ها به منظور تشخیص نفوذهای احتمالی در این جزء صورت می پذیرد. بسته به نوع رویکرد بکار گرفته شده در سیستم تشخیص نفوذ، مکانسیم ها (تکنیک ها) مختلفی برای پردازش داده ها به خدمت گرفته می شوند.

واکنشگر: بعد از تشخیص نفوذ توسط تحلیگر، نوبت به این جزء جهت انجام اقدام مناسب میباشد. بسته به نوع سیستم تشخیص نفوذ (فعال یا غیرفعال) این اقدام می تواند متفاوت باشد. در سیستم های فعال که در رده سیستم جلوگیری از نفوذها دسته بندی می شوند، با قطع ارتباط در مقابل نفوذ تشخیص داده شده عکس العمل نشان می دهند. اما در سیستم های غیرفعال صرفا به اعلان هشدار کفایت می کند [12].

ابزارهای خودکار تست نفوذ

نتایج تحقیقاتی که در زمینه ابزارهای تست نفوذ در سال ۲۰۰۶ انجام شده است، ده ابزار زیر را به عنوان بهترین ابزارهای تست نفوذ معرفی کرده اند.

Nessus: این نرم افزار اسکن آسیب پذیری شبکه است که بیش از ۱۱۰۰۰ پلاگین دارد. این نرم افزار، دارای بررسی های امنیتی محلی (Local) و راه دور، معماری کلاینت/سرور با رابط گرافیکی GTK، و زبان اسکریپتی برای نوشتن پلاگین های مورد دلخواه است.

GFI LANgaurd: این یک اسکنر تجاری برای امنیت شبکه برای سیستم عامل ویندوز است. این نرم افزار، شبکه‌هایIP را اسکن میکند تا ماشین های در حال اجرا را شناسایی کند. این نرم افزار می تواند سیستم عامل کامپیوتر ها، برنامه های در حال اجرای سیستم ها، سرویس پک نصب شده بر روی سیستم عامل، patch های نصب نشده و ... را کشف کند.

Retina: یک اسکنر تجاری آسیب پذیر است. همانندNessus ، این برنامه نیز تمام سیستم های یک شبکه را اسکن می کند و تمام آسیب پذیری های کشف شده را گزارش می دهد.

Core Impact: محصولی برای خودکارسازی فرآیند تست نفوذ است که به عنوان قدرتمندترین ابزار اکسپلویت مطرح می شود (بسیار گران است). این محصول دارای پایگاه داده بسیار بزرگ و آپدیت است.

ISSN: 2745-3673
http://www.Rcsj.ir

ISS Internet Scanner: یک ابزار ارزیابی آسیب پذیری در سطح اپلیکیشن است. اسکنر اینترنت می تواند بیش از ۱۳۰۰ نوع دستگاه شبکه ها از قبیل کامپیوترهای رومیزی، سرورها، روترها، سوئیچ ها، فایروال ها، دستگاه های امنیتی و ... را شناسایی کند.

X-Scan: یک اسکنر شبکه است که به صورت چند نخی عملیات اسکن آسیب پذیری را انجام می دهد. این ابزار می تواند نوع سرویس ها، نوع سیستم عامل های راه دور و نسخه آنها، و نام کاربری و پسوردهای ضعیف را کشف کند.

SARA: ابزار ارزیابی آسیب پذیری است که از اسکنر SATAN مشتق شده است. آپدیت های آن دو بار در ماه منتشر می شود.

QualysGuard: یک اسکنر آسیب پذیری تحت وب است. کاربران می توانند از طریق اینترفیس وب به آن وصل شوند. این ابزار، بیش از ۵۰۰۰ آسیب پذیری را چک می کند.

SAINT: ابزاری تجاری برای ارزیابی آسیب پذیری است.

MBSA: محصول مایکروسافت است که با دیگر محصولات مایکروسافت سازگاری دارد. به طور متوسط هر هفته، ۳ میلیون کامپیوتر را اسکن می کند.

علاوه بر این لیست، شما باید با ابزارهای دیگر اکسپلویت آشنا باشید:

Metasploit Framework: نرم افزاری اپن سورس (Open Source) برای ایجاد، تست، و استفاده از اکسپلویت است.

Canvas: ابزار تجاری استفاده از آسیب پذیری است که شامل بیش از ۱۵۰ اکسپلویت است [3] .

تشخیص نفوذ در اینترنت اشیاء

مقدمه ای بر اینترنت اشیاء

اینترنت اشیاء (IoT[6]) فناوری است که هر شی یا دستگاهی را در هر نقطه از هر مسیر یا شبکه به هم متصل می کند. تمام اشیاء متصل باید در اکوسیستم اینترنت اشیاء، با استفاده از شناسه منحصر به فرد آدرس دهی شوند.اینترنت اشیاء می تواند در زمینه های مختلف مانند شهرهای هوشمند، خانه های هوشمند، حمل و نقل، کشاورزی، مراقبت های بهداشتی و غیره استفاده شود. علاوه بر این، طبق اطلاعات اخیرGartner، در فناوری IoT لازم است به ازای هر انسان حدود ۶ دستگاه با یکدیگر ارتباط برقرار کنند [13].بر اساس گزارش های سازمان تهدیدهای امنیتی اینترنت (ISTR[7]) ۲ دقیقه برای حمله به هر دستگاهIoT لازم است. همچنین از سال ۲۰۱۶ تا ۲۰۱۷ در حدود ۶۰۰ درصد حمله به دستگاه های IoT افزایش یافته است. این در حالی است که گزارش های Gmalto، نشان می‌دهد که تقریبا نیمی از شرکت های پیشرو در حوزه IoT نمی توانند نفوذ به دستگاه های IoT خود را تشخیص دهند.

بسیاری از سازمان‌ها به عنوان بخشی از تحولات دیجیتال خود، IoT را در بر می‌گیرند. در این راستا، شرکت ها تعداد زیادی از دستگاه های IoT را به شبکه های شرکتی خود متصل می کنند. این دستگاه ها با سایر دارایی های ارزشمند فناوری اطلاعات ارتباط برقرار می کنند و گاهی اوقات اطلاعات حساسی را کنترل می کنند. بنابراین مهم است که شرکت ها اقداماتی را برای ایمن سازی دستگاه های IoT خود انجام دهند. متاسفانه، برقراری امنیت IoT آسان به نظر نمی رسد زیرا دستگاه های هوشمند متعدد و متنوع یک اکوسیستم چند منظورهIoT، که به پیچیدگی محیط IT به طور کلی افزوده است ایجاد کرده است. چنین پیچیدگی موجب ایجاد خطر دیجیتالی می شود، زیرا مهاجمان تعداد بیشتری از دستگاه ها را برای هدف قرار دادن دارند و از روابط این دستگاه ها سوء استفاده می کنند. علاوه بر این، محصولات هوشمند اطلاعات مشابه ای را اداره نمی کنند. برخی دستگاه ها ممکن است اقدامات امنیتی کمتری نسبت به دیگر دستگاه ها را انجام دهند، به همین دلیل امنیت اطلاعات، سازمان ها را مورد تهدید قرار داده است و سازمان ها به وضوح احساس محافظت از میزان رو به رشد داده ها را که جمع آوری و ذخیره

[6] Internet of Things
[7] International Society for Third-Sector Research

ISSN: 2745-3673
http://www.Rcsj.ir

کرده اند، احساس می کنند. لذا آن ها با سرمایه گذاری در امنیت می خواهند این مشکل را حل کنند به طوری که هزینه ها در حوزه امنیت دستگاه هایIoT توسط شرکت ها در سال ۲۰۱۷ از ۱۱.۷ درصد به ۱۳.۱۵ درصد در سال ۲۰۱۸ افزایش یافته است.

بازار دستگاه های IoT شناخته شده است و نقش آنها در زندگی روزمره به طور چشمگیری افزایش یافته است. اما مجرمان سایبری نیز فرصت های مالی را در نظر گرفته و در نتیجه حملات خود را چند برابر می کنند و خطر برای مصرف کنندگانی که ابزارهای IoT خود را دوست دارند، این است که تهدیدات می توانند به طور غیرمنتظره ای به آن ها ضربه بزند و دستگاه های ظاهرا بی‌ضرر را به دستگاه های قدرتمند برای فعالیت غیرقانونی تبدیل کند. این امر می‌تواند استفاده از آنها درحملات DDoS[8]، یا فعالیت بات نت ها باشد. با توجه به این که، ارتباطات بیشتر به نوعی معادل افزایش تهدیدات و سخت تر شدن حفظ حریم خصوصی و امنیت IoT است. سه چالش اصلی برای IoT معرفی شده است. اولین چالش، ناهمگونی شبکه است. دوم،IoT معماری بسیار گسترده ای را به خصوص در برنامه های کاربردی مانند شهرهای هوشمند و شبکه های هوشمند اتخاذ می کند. سوم IoT پروتکل های جدیدی برای رسیدگی به مسائل خاص مربوط به محدودیت قدرت و محاسبات حسگرهای شبکه معرفی می کند [14].

شبکه های نرم افزار محور

شبکه های نرم افزار محور (SDN[9]) یک نمونه از شبکه های جدیدی هستند که انعطاف پذیری، قابلیت مقیاس پذیری و امنیت را بهبود می بخشد که می تواند تا حدی چالشهای موجود را در IoT حل کند. در واقع شبکه هایSDN صفحه کنترل و انتقال را از هم جدا می کنند. صفحه انتقال برای سوئیچ جریان داده ها است. همچنین صفحه کنترل یک قسمت جدیدی در شبکه، که کنترلر نامیده می‌شود را معرفی می کند و صفحه انتقال شامل دستگاه های سخت افزاری مانند سوئیچ ها، روترها، فایروال ها و سیستم‌های تشخیص نفوذ (IDS) است. این دستگاه ها هیچ پردازشی برای پر کردن جدول صفحه انتقال نیاز ندارند و منطق شبکه به طور مستقل به کنترلر منتقل شده است. کنترلر خدماتی مانند وضعیت شبکه و اطلاعات توپولوژی آن را ارائه می دهد و برای جابجایی اطلاعات از کنترلر به صفحه انتقال و برعکس از پروتکلی به نام OpenFlow استفاده می شود. با این وجود امنیت در SDN همچنان یکی از اصلی ترین نگرانی ها است [15,16].

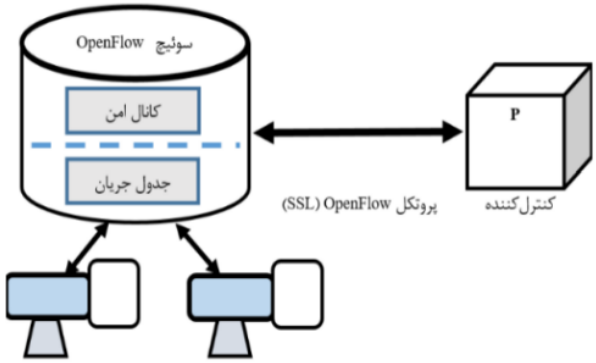
با توجه به اینکه SDN برای بهبود چالش های IoT از قبیل انعطاف پذیری و یا مقیا س پذیری به آن اضافه شده است اما از طرفی نگرانی هایی که در امنیت SDN وجود داشت، به نگرانی های امنیتی در IoT افزوده شده و لذا نگرانی در امنیتIoT SDN بیشتر از پیش شده است. SDN بخاطر کنترلر مرکزی، دید کلی شبکه را فراهم می کند و این فرایند مدیریت و اجرای سیاست‌ها را آسان می‌کند و همچنین خطاها را در زمان پیکربندی و تغییر سیاست‌های شبکه کاهش می دهد و قابلیت همکاری را افزایش می دهد. مثل چندین شبکه در صنایع مختلف می توانند در یک شبکه یکپارچه و قابل اطمینان قرار گیرند. تهدیدات امنیتی، چالشی حیاتی در شبکه‌های معمولی هستند و این تهدیدها در شبکه هایSDN تشدید می‌شوند. در واقع مزایای این مدل از شبکه با تهدیدهای اضافی همراه است که در شبکه های سنتی امکان پذیر نبوده اند. برطبق بررسی های امنیتی که بر روی پروتکل OpenFlow صورت گرفته، مشخص شده است که حملات مختلفی بر روی این پروتکل صورت گرفته است. برای مثال، جداول جریان و دستگاه های کنترل کانال بین دستگاه ها و کنترلر می تواند تحت تاثیر حملات انکار سرویس قرار گیرد. کانال ارتباطی بین کنترلر و سوئیچ با یک اتصال TCP با پروتکل رمزنگاری TCP برای امن کردن کانال ارتباطی شروع می شود و بدون یک روش رمزگذاری، ارتباط بین کنترلر و دستگاه های انتقال در معرض حملات مرد میانی است [17].

به علت رشد فناوری بی‌سیم ناهمگن، شبکه های فاقد زیرساخت مبتنی بر شبکه نرم افزار محور نیز انعطاف پذیری، پویایی، مقیاس پذیری و فرصت هایی را برای حل مسائل امنیتی فراهم می کنند. شبکه نرم افزارمحور ضمن ارائه و معرفی برنامه ریزی، کنترل متمرکز، تجزیه و تحلیل ترافیک و بهبود امنیت، مجازی سازی و هوشمندی را در شبکه ایجاد می کند. با توجه به اینکه

[8] Distributed Denial of Service
[9] Software Defined Networking

ISSN: 2745-3673
http://www.Rcsj.ir

به کارگیری یک راه حل کنترل متمرکز با سطح تمرکز زدایی، خرابکاری و تأخیر در محیط های فاقد زیرساخت ناسازگار است، کاربرد آن با چالش هایی رو به رو است. اساس کار شبکه نرم افزارمحور بر جداسازی هوش شبکه (کنترل) از پوسته (انتقال اطلاعات) است. این قبیل شبکه ها پس از انتشار جاوا توسط سان مایکروسیستمز در سال ۱۹۹۵ رایج شدند. در شبکه های بالا کنترل کنندۀ متمرکز کل شبکه را هدایت کرده و برنامه ریزی سبب پویایی شبکه، شخصی سازی و تعریف کاربری های جدید بر اساس نیاز هر سازمان می شود [15,16]. نحوۀ عملکرد پروتکل OpenFlow برقراری ارتباط امن بین سوئیچ و کنترل کننده است. شبکه OpenFlow می تواند متشکل از چندین شبکه فیزیکی مجهز به دستگاه های حمل و نقل مانند روتر و سوئیچ باشد. سوئیچ OpenFlow شامل سه بخش جداول جریان، کانال ارتباطی امن و پروتکل OpenFlow است که در تصویر (۲) نشان داده شده است. سطح کنترل به عنوان کنترل کنندۀ پروتکل فوق عمل و کنترل کننده عملیات به روزرسانی، افزودن یا حذف ورودی های جریان را به وسیله قوانین از پیش تعریف شده اجرا می کند. [18, 19]



تصویر (۲): اجزاء سوئیچ (OpenFlow)

ویژگی ها و مزایای شبکه نرم افزار محور

شبکه نرم افزارمحور به عنوان روشی انعطاف پذیر جهت کنترل شبکه به صورت نظام‌مند ظاهر شده است. بستر بالا از پروتکل OpenFlow جهت برقراری ارتباط امن بین سطوح داده و کنترل بهره می برد. وجود برخی ویژگی های فوق العاده در شبکه نرم افزار محور باعث حل بسیاری از مشکلات امنیتی فعلی شده است. شبکه نرم افزار محور دارای ویژگی های مهمی از قبیل قابلیت برنامه ریزی، چابکی و پویایی، کنترل و مدیریت متمرکز، تجزیه و تحلیل ترافیک، به روزرسانی پویای قوانین حمل و نقل، بهینه سازی منابع و حفظ امنیت است. همچنین شبکه بالا دارای مزایایی نسبت به شبکه های مرسوم مانند استقرار آسان تر، ارائه خدمات جدید، کاهش هزینه مدیریتی و عملیاتی فناوری های ناهمگن، عملیات مؤثر زیرساخت های چند فروشنده، افزایش مداوم و شفاف عملیات و سرویس دهی، بهبود امنیت در شبکه، افزایش قابلیت برنامه ریزی عناصر شبکه در پلتفرم بیسیم توزیع شده و ممانعت از درگیرکردن تجهیزات است .برقراری امنیت یک چالش بزرگ در شبکه های مبتنی بر شبکه نرم افزار محور و به طورکلی در شبکه های موردی سیار با قابلیت بالا است [20]. یکی از روش های رایج بهبود امنیت، به کارگیری معماری های مختلف شبکه نرم افزار محور است که در ادامه آن را تشریح می کنیم.

انواع معماری کنترل کننده در شبکه نرم افزار محور

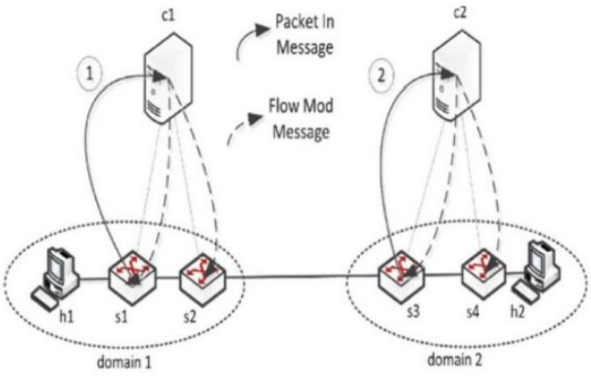
با توجه به عدم وجود استاندارد اجرایی برای استفاده از معماری های مختلف شبکه نرم افزار محور در طراحی شبکه ، مشتریان نسخه های متفاوتی را از کنترل کننده شبکه نرم افزار محور برای رفع نیاز خود استفاده می کنند. انواع معماری شبکه نرم افزار محور از لحاظ ساختار کنترل کننده شامل کنترل کننده های متمرکز واحد و چندگانه (معماری سلسله مراتبی، معماری توزیع شده کامل با دیدگاه محلی و جهانی) است. در ادامه این ساختارها را تشریح می کنیم.

- **استفاده از یک کنترل کننده متمرکز (کنترل کننده متمرکز واحد):** کنترل کننده شبکه نرم افزار محور واحد، بخشی از شبکه با عنوان دامنه را کنترل کرده و اطلاعات محدودی از شبکه دارد. دامنه مجموعه ای از تمام سوییچ

ISSN: 2745-3673
http://www.Rcsj.ir

هایی است که به طور مستقیم به یک کنترل کننده متصل شده و همهٔ میزبان ها به این سوئیچها متصل هستند. برای مثال در تصویر (۳)c1 به صورت مجزا به عنوان کنترل کننده متمرکز واحد، فقط قادر به دیدن s2 و s1 و h1 است. حمله منع سرویس و منع سرویس توزیع شده می تواند در کنترل کننده با ساختار بالا رخ دهد که تنها نقطه شکست است [18, 21].

- **استفاده از کنترل کننده های چندگانه (سلسله مراتبی و توزیع شده):** به کارگیری کنترل کننده های متعدد می تواند ضمن افزایش میزان اعتماد و تحمل شکست، مشکل شکست نقطه ای را برطرف کرده و در صورت شکست یک کنترل کننده، امکان تداوم در کنترل شبکه را میسر سازد. همچنین با ساختار بالا کنترل کننده ها برای تدوام در کنترل شبکه با همدیگر همکاری کرده و اطلاعات را مبادله می‌کنند. درضمن استفاده از ساختار بالا که از کنترل کننده های زیادی بهره می‌گیرد، سربار را افزایش می دهد. تصویر (۳) ساختار شبکه نرم افزار محور با کنترل کننده های چندگانه را نشان می دهد.



تصویر (۳) : کنترل کننده های چندگانه با دامنه های مختلف و قابلیت مسیریابی مستقل بسته ها

معماری کنترل کننده چندگانه می تواند با استفاده از دو طرح کنترل کننده چندگانهٔ سلسله مراتبی و چندگانهٔ توزیع شده کامل (مسطح) با دیدگاه محلی و جهانی طراحی و اجرا شود[18] .

ساختار کنترل کنندهٔ چندگانه سلسله مراتبی

مدل سلسله مراتبی به عنوان یک معماری عمودی است و در ساختار بالا کنترل کننده ریشه (اصلی) هماهنگی های لازم را بین کنترل کننده های محلی ایجاد کرده و آنها را مدیریت می کند. در این ساختار کنترل کنندهٔ ریشه به پایگاه داده جهانی دسترسی داشته و کنترل کننده های محلی قبل از اینکه بتوانند هر عملیات بین دامنه را اجرا کنند، می بایست اطلاعات شبکه را از کنترل کننده ریشه درخواست کند. در این مدل کنترل کنندهٔ ریشه به عنوان یک سرور و کنترل‌کننده‌های محلی به عنوان مشتری عمل می کنند. همچنین هیچ یک از کنترل کننده های محلی خوشه اتصال برنامه نویسی کاربردی شرقی - غربی با سایرین نداشته و فقط با کنترل کنندهٔ ریشه متمرکز ارتباط دارند . در تصویر (۴) کنترل کننده MC[10] به عنوان ریشه (اصلی) و SC1[11] و SC2 کنترل کننده های محلی (ثانویه) هستند.

[10] Main Controller
[11] Secondary Controller

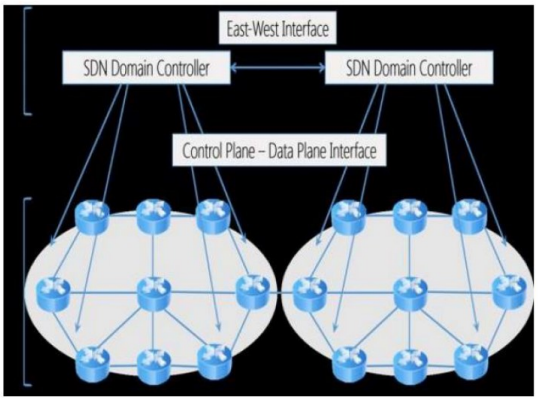
ISSN: 2745-3673
http://www.Rcsj.ir

تصویر (۴) : ساختار کنترل کننده های سلسله مراتبی

لازمه برقراری ارتباط و پاسخ به درخواستها این است که هر SC توسط MC تأیید شود. فرایند برقراری ارتباط در دو مرحله ادامه می یابد. در مرحله نخست، یک SC درخواست خود را برای مدیر ارائه کرده و در مرحله دوم، MC با دسترسی به پایگاه داده، مجوز یا رد دسترسی SC درخواست کننده را صادر می کند. در این ساختار کنترل کنندۀ ریشه، وضعیت شبکه جهانی و کنترل کننده های محلی، فقط حالت شبکه محلی خود را حفظ می کنند؛ بنابراین در ساختار بالا کنترل کنندۀ ریشه با مدیریت بر کنترل کننده های محلی، اتصال و هماهنگی بین خوشه را فراهم می کند.

ساختار کنترل کنندۀ توزیع شدۀ کامل (مسطح[۱۲])

کنترل کننده با ساختار توزیع شده کامل یا مسطح، برنامه کاربردی - کنترلی واقع در چند سرور موجود در شبکه را به منظور جمع آوری اطلاعات اجرا می کند. همچنین یک رابط برنامه نویسی برای پیاده‌سازی ویژگی‌های مدیریتی مانند مسیریابی و کنترل دسترسی ارائه می کند. تصویر (۵) نمونه ای از ساختار شبکه نرم افزار محور مجهز به کنترل کنندۀ توزیع شدۀ کامل (با دیدگاه محلی و جهانی) را نشان می دهد. کنترل کنندۀ چندگانۀ توزیع شده کامل با دیدگاه محلی، نشان دهندۀ وضعیت فعلی شبکه در یک دامنه است که به صورت محلی در کنترل کننده ذخیره می شود. این حالت به کنترل کننده کمک کرده تا از هر رویداد مانند پیوستن یا ترک میزبان و اتصال به بالا یا پایین آگاه باشد؛ اما کنترل کنندۀ چندگانۀ به منظور به روزشدن، دسترسی به اطلاعات بیشتر و ساختن یک وضعیت شبکه جهانی (دیدگاه جهانی) باید بخشهایی از وضعیت شبکه محلی خود را به کنترل کننده های دیگر توزیع کند؛ بنابراین برخی از اطلاعات از قبیل حالت شبکه محلی ایستا و پویا، فهرست برنامه های نصب شده و دستگاه های متصل در کنترل کننده مبادله می شود [18].



تصویر (۵): ساختار کنترل کننده توزیع شده کامل

[12] Flat

ISSN: 2745-3673
http://www.Rcsj.ir

تشخیص نفوذ در اینترنت اشیاء

در این بخش، به بررسی مفاهیم و تحقیقات مرتبط با تشخیص نفوذ در اینترنت اشیاء بر اساس چهار ویژگی استراتژی های قرار گرفتنIDS ، روش تشخیص، تهدیدات امنیتی و استراتژی اعتبارسنجی پرداخته شده است.

استراتژی های قرار گرفتن IDS

در سالهای اخیر، محققان معماری های مختلفی را برای اینترنت اشیاء نشان داده اند، که به شدت به مراحل جمع آوری، انتقال، و پردازش، مدیریت و بهره برداری وابسته هستند. اگر چه این روش های ارائه شده در برخی جنبه ها تفاوت دارند، ولی تمام این روش ها در سه دامنه ی گسترده سناریوهای اینترنت اشیاء را سازماندهی می کنند: دامنه ی فیزیکی، دامنه ی شبکه، و دامنه ی کاربردی. دامنه ی فیزیکی مربوط به مرحله جمع آوری است و شامل وسایلی می باشد که محیط فیزیکی را حس کرده و در آن فعالیت می کنند و اغلب یک LLN[13] را تشکیل می دهند. دامنه شبکه که بر مرحله انتقال متکی است، راه حل ها و پروتکل های متداول شبکه را برای انتقال داده ها از محیط فیزیکی به برنامه های کاربردی و کاربران در کنار هم گردآوری می‌کند. یک مسیریاب مرزی لازم است که بین دامنه های شبکه و فیزیکی قرار بگیرد تا پروتکل های LLN موجود در لایه ی فیزیکی را با پروتکل های متداول در دامنه شبکه ادغام و یکپارچه نماید. در نهایت، دامنه کاربردی شامل واسط هایی است که به کاربران اجازه می دهد تا به اشیاء موجود در دامنه فیزیکی رسیدگی کنند.

در شبکه های اینترنت اشیاء، سیستم تشخیص نفوذ می تواند 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. در ادامه سه استراتژی ممکن برای قرار گرفتن سیستم های تشخیص نفوذ را شرح می دهد.

- **قرار گرفتن IDS به صورت توزیع شده :** در این استراتژی قرارگیری، سیستم‌های تشخیص نفوذ در هر شئ فیزیکی درLLN (شبکه های کم توان و با اتلاف زیاد) قرار داده می شوند. سیستم تشخیص نفوذ مستقر شده در هر گره باید بهینه باشد، چرا که این گره ها منابع محدودی دارند. در قرارگیری توزیع شده، گره‌ها ممکن است همچنین مسئولیت نظارت همسایگان خود را نیز بر عهده داشته باشند. گره هایی که همسایگان خود را نظارت می کنند با نام نگهبان[14] نامیده می شوند.
- **قرار گرفتن IDS به صورت متمرکز :** در قرار گرفتن IDS به صورت متمرکز، سیستم تشخیص نفوذ در یک جزء متمرکز قرار می گیرد، به عنوان مثال در یک مسیریاب مرزی یا یک میزبان اختصاصی مستقر می شود. 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 می تواند به تحلیل تمام ترافیک مبادله شده بین LLN و اینترنت بپردازد. با این حال، تحلیل ترافیکی که از مسیریاب مرزی عبور می کند، برای تشخیص حمله ها کافی نیست، حمله-هایی که تنها گره‌های داخل LLN را شامل می شوند. سپس، محققان به طراحی سیستم های تشخیص نفوذی پرداختند که می توانند ترافیک مبادله شده بین گره های LLN را نظارت نمایند، بدون اینکه عملیات نظارت تاثیری بر عملکرد گره های کم ظرفیت داشته باشد. همچنین، IDS متمرکز ممکن است با نظارت بر گره ها در حین یک حمله مشکل داشته باشد، حمله ایی که بخشی از شبکه را در معرض خطر قرار می دهد .
- **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 می کند تا از مزایای آنها بهره برده و از نقاط ضعف آنها پیشگیری کند. اولین رویکرد برای قرار گرفتن ترکیبی، شبکه را به خوشه ها یا مناطقی تقسیم کرده و سازماندهی می کند، و

[13] Low Power and Lossy Networks
[14] Watchdog

ISSN: 2745-3673
http://www.Rcsj.ir

فقط گره ی اصلی هر خوشه یک نمونه از سیستم تشخیص نفوذ را میزبانی می نماید. سپس، این گره مسئول نظارت به دیگر گره های عضو خوشه ی خود می شود.

روش های تشخیص

روش های تشخیص نفوذ بسته به مکانیزم تشخیص استفاده شده در سیستم به چهار دسته تقسیم می شوند:

a)رویکردهای مبتنی بر امضا

در رویکردهای مبتنی بر امضا، IDS ها وقتی حملات را تشخیص می دهند که رفتار سیستم یا شبکه با امضای حمله ای مطابقت داشته باشد که این امضاها در پایگاه داده های داخلی IDS ذخیره شده اند. اگر هر گونه فعالیت سیستم یا شبکه با امضاها / الگوهای ذخیره شده مطابقت داشته باشد، آنگاه هشداری فعال خواهد شد.

b)رویکردهای مبتنی بر ناهنجاری

سیستم های تشخیص نفوذ مبتنی بر ناهنجاری فعالیت های سیستم را در هر لحظه با پروفایل رفتار عادی سیستم مقایسه می کنند 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.

c)رویکردهای مبتنی بر مشخصه

مشخصه در واقع مجموعه ای از قوانین و آستانه ها است که رفتار مورد انتظار را برای اجزای شبکه از قبیل گره ها، پروتکل ها، و جداول مسیریابی تعریف می کنند. رویکردهای مبتنی بر مشخصه، نفوذهایی را تشخیص می دهد که در آنها رفتار اجزای شبکه از مشخصه های 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 مهم ترین تفاوت های 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.

d)رویکردهای ترکیبی

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

تهدیدات امنیتی

IoT می تواند تحت تأثیر گونه های مختلف تهدیدهای امنیتی از جمله موارد زیر قرار گیرد:

- کرم های معمولی که از ICT به IoT جهش کرده اند: بطور کلی محدود به اشیایی است که در حال اجرا روی سیستم عامل مصرف کننده است مثل ویندوز، لینوکس و . ...
- حملات با اسکریپ ها و یا دیگر اهداف مقیم دوربین تحت وب IoT محافظت نشده، سرقت محتوا، شکستن سیستم های کنترل خانه.
- جرایم سازمان یافته: دسترسی به مالکیت معنوی، خرابکاری و جاسوسی.

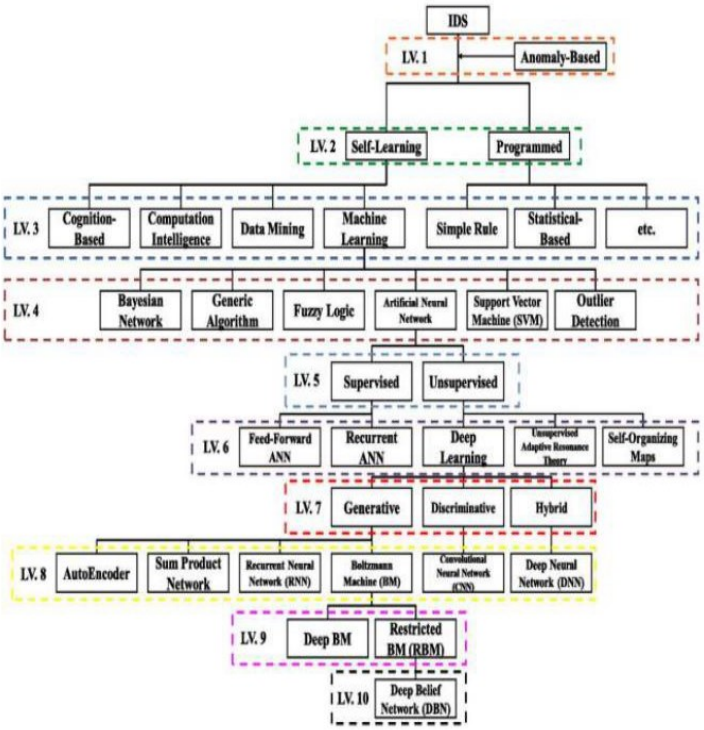
استراتژی اعتبارسنجی

اعتبارسنجی و ارزیابی شامل بررسی این مورد است که آیا مدل ساخته شده با دقت رضایت بخشی در راستای اهداف مطالعه رفتار می کند یا خیر. روش های اعتبارسنجی بسیاری وجود دارند، و این روش ها ممکن است به وسیله ی دو منبع اطلاعاتی از هم تفکیک داده شوند: کارشناسان و داده ها. در حالی که استفاده از کارشناسان یک مدل اعتبارسنجی ذهنی و اغلب کیفی را فراهم می کند، استفاده از داده ها ممکن است یک مدل اعتبارسنجی کمی و هدفمندتری را ارائه دهد [22, 23] .

ISSN: 2745-3673
http://www.Rcsj.ir

الگوریتم‌های هوشمند

در سالهای اخیر الگوریتم های هوشمند در جاهای مختلفی مورد استفاده قرار گرفته اند به عنوان مثال پیشرفت های اخیر در یادگیری ماشین ML[15] این تکنیک را قابل انعطاف تر در کاربردها و سناریوهای مختلف کرده است، بدیهی است، همانطور که ما منتظر اتوماتیک کردن جنبه‌های بیشتری از زندگیمان هستیم، از اتوماسیون خانگی تا وسایل نقلیه مستقل، تکنیک های ML تبدیل به یک جنبه مهم در سیستم های مختلف می‌شود که در تصمیم گیری ها، تجزیه و تحلیل و اتوماسیون کمک می‌کند. پژوهش های متعددی، جهت استفاده از الگوریتم‌های هوشمند در سیستم های تشخیص نفوذ در شبکه های مختلف صورت گرفته است و نتایج آنها حاکی از این است که این الگوریتم ها با توجه به شرایط، سخت افزارهای محاسباتی مناسب به موفقیت قابل توجه ای رسیده اند. همچنین دسته‌بندی‌های مختلفی برای شناسایی ناهنجاریها در IDS ممکن است. در تصویر (۶) روش های مختلف برای طبقه بندی نشان داده شده است.



تصویر (۶): دسته بندی روش های تشخیص ناهنجاری

همانطور که قبل توضیح داده شد، مهمترین واژه در اینجا طبقه‌بندی است و تعریف طبقه‌بندی باید مورد بررسی قرار گیرد. برای طبقه بندی در اولین قدم باید داده های خام را که به صورت مجموعه‌ای از داده‌ها هستند، بدست آورد و این مجموعه داده ها توسط یکی از سه استراتژی مهم کاهش ابعاد، خوشه بندی و نمونه برداری کاهش یابد. استفاده از یک الگوریتم خوب برای طبقه‌بندی بسیار مهم است. برای طبقه بندی، دو مجموعه داده به نام های مجموعه داده آموزشی و مجموعه داده آزمایشی مورد نیاز است. هدف از مجموعه داده های آموزشی استفاده از آن در آموزش الگوریتم طبقه‌بندی است و مجموعه داده های آزمایشی برای تست عملکرد طبقه بندی استفاده می شود. همچنین یک مجموعه داده مهم دیگر به منظور تنظیم پارامترها وجود دارد که به عنوان مجموعه داده اعتبارسنجی نامیده می شود. یکی از چیزهایی که باید در نظر داشت این است که هر دو مجموعه داده آموزشی و اعتبارسنجی تنها مجموعه داده هایی هستند که باید برای آموزش الگوریتم در طبقه بندی استفاده شوند. با توجه به این موضوع که طبقه بندی به یادگیری مرتبط است، در واقع افزایش دقت در طبقه بندی بخاطر افزایش دقت یادگیری میباشد. لذا انتخاب یک الگوریتم کارآمد، شناخته شده و قدرتمند برای یادگیری الگوهای طبقه های مختلف از اهمیت بسیاری برخوردار

[15] Machine Learning

ISSN: 2745-3673
http://www.Rcsj.ir

است. همچنین الگوریتم های یادگیری در سه دسته، یادگیری با نظارت، یادگیری بدون نظارت و یادگیری نیمه نظارتی، شناخته می شوند.

- **یادگیری با نظارت:** یادگیری با نظارت که به طبقه بندی پیشگویانه یا مستقیم شناخته می شود. در این یادگیری، داده های که به درستی طبقه‌بندی شده را گرفته و سپس یک الگوریتم یادگیری نظارت شده با استفاده از این داده ها آموزش دیده تا برای پیش بینی در مرحله بعدی مورد استفاده قرار گیرد. بنابراین، این روش زمانی مناسب است که یک مقدار از داده ها با برچسب مشخصی وجود داشته باشد. الگوریتم های شناخته شده در روش یادگیری با نظارت شامل ماشین های پشتیبان بردار، شبکه عصبی مصنوعی، رگرسیون لجستیک، جنگل های تصادفی، درخت تصمیم و غیره هستند.
- **یادگیری بدون نظارت:** یادگیری بدون نظارت به خوشه بندی توصیفی یا غیرمستقیم شناخته می شود. در واقع اگر یادگیری بر روی داده های بدون برچسب و برای یافتن الگوهای پنهان در این داده ها انجام شود، یادگیری بدون نظارت خواهد بود. الگوریتم های شناخته شده یادگیری بدون نظارت عبارت از خوشه بندی، نقشه خود سازمانده، یادگیری عمیق و غیر هستند.
- **یادگیری نیمه نظارتی:** یادگیری نیمه نظارتی یک نسخه ترکیبی از یادگیری با نظارت و یادگیری بدون نظارت است، به طوری که برای یادگیری از داده های برچسب دار و بدون برچسب باید استفاده شود[24] .

نتیجه گیری

در دنیای امروز که سیستم های کامپیوتری و شبکه ها بسیار گسترش یافته اند ، طبیعی است که سودجویان زیادی ظاهر می شوند که با هدف های گوناگون حملاتی را به سیستم های کامپیوتری و شبکه ها صورت دهند. بنابراین باید راههای حملات سودجویان را تا حد ممکن مسدود کرد. سیستم های تشخیص نفوذ به این منظور پدید آمدند. راه های مختلفی برای تشخیص نفوذ وجود دارد که هر کدام کاربردی متفاوت دارند و استفاده از ترکیب این روش ها کمک می کند تا با حملات مقابله کرد. برای استفاده از سامانه های تشخیص نفوذ ابتدا باید اجزای سیستم های تشخیص نفوذ که عبارت اند از حسگر یا عامل، سرور مدیریت، سرور پایگاه داده، واسط کاربری و طعمه مجازی را به خوبی شناخت و در سیستم مورد نظر شناسایی کرد.وقتی اجزای سامانه تشخیص نفوذ در سیستم شناسایی شد باید انتخاب کرد که از چه سیستم تشخیص نفوذی باید استفاده نمود. سیستم های تشخیص نفوذ به ۲ دسته مبتنی بر میزبان و مبتنی بر شبکه تقسیم می شوند. سیستم های تشخیص نفوذ مبتنی بر میزبان نرم افزارهایی هستند که بر روی سیستم عامل اجرا شده و دسترسی به سیستم را محدود می کنند و سیستم های تشخیص نفوذ مبتنی بر شبکه، نظارت و تجزیه و تحلیل ترافیک سراسر شبکه ، به منظور شناسایی تهدیدات را به عهده دارند.

پس از آنکه با تشخیص نفوذ به طور کامل آشنا شدیم، صحبت از یک فناوری نوظهور به میان می آید با نام اینترنت اشیاء. اینترنت اشیاء به زبان ساده یعنی ارتباط حسگرها و دستگاه با شبکه اینترنت که از طریق این ارتباط و تعامل بین لوازم متصل به شبکه و کاربران دارای دسترسی مجاز به این شبکه، امکان مشاهده و کنترل لوازم متصل به شبکه برای کاربران آن فراهم می شود. از این رو شبکه های نرم افزار محور یک نمونه از شبکه های جدیدی هستند که انعطاف پذیری، قابلیت مقیاس پذیری و امنیت را بهبود می بخشند که می تواند تا حدی چالش های موجود در اینترنت اشیاء را حل کند. شبکه نرم افزارمحور ضمن ارائه و معرفی برنامه ریزی، کنترل متمرکز، تجزیه و تحلیل ترافیک و بهبود امنیت، مجازی سازی و هوشمندی را در شبکه ایجاد می کند. بنابراین می توان از شبکه های نرم افزار محور در سیستم های تشخیص نفوذ استفاده کرد و همچنین گزینه مناسبی برای برقرار کردن امنیت در اینترنت اشیاء است.از سیستم های تشخیص نفوذ در اینترنت اشیاء به صورت توزیع شده، متمرکز و ترکیبی می توان استفاده کرد.استراتژی قرارگرفتن سیستم های تشخیص نفوذ در اینترنت اشیاء به صورت توزیع شده به این صورت است که سیستم تشخیص نفوذ در هر شئ فیزیکی در شبکه‌های کم‌توان و با اتلاف زیاد قرار داده می شوند. در استراتژی متمرکز، سیستم تشخیص نفوذ در یک جزء متمرکز قرار می گیرد و در استراتژی ترکیبی در واقع مفاهیم قرار گرفتن به صورت متمرکز و توزیع شده ترکیب می شوند.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] Gómez, J., Gil, C., Baños, R. *et al.* A Pareto-based multi-objective evolutionary algorithm for automatic rule generation in network intrusion detection systems. *Soft Comput* 17, 255–263 (2013).

[۲] بجانی، صادق و حسنی آهنگر، محمدرضا، اخضمی، مصطفی، ۱۳۹۲ نقش سیستمهای تشخیص نفوذ در امنیت سرویس‌های وب، فصلنامه علمی - ترویجی پدافند غیرعامل.

[۳] عمادی استرآبادی، سید مهدی و لیثی بهرمانی، شهره، ۱۳۹۴، امنیت و نفوذپذیری در شبکه های کامپیوتری، انتشارات فدک ایساتیس.

[۴] نصیری، محمد، معرفی سیستم های تشخیص نفوذ و انواع آن به زبان بسیار ساده، با اقتباس از https://firewall.tosinso.com/fa/articles/20/IDS.

[۵] ماروسی، علی و ذباح، ایمان و عطائی خباز، حسین، ۱۳۹۹، تشخیص نفوذ در شبکه با استفاده از ترکیب های عصبی مصنوعی به صورت سلسله مراتبی، نشریه علمی پدافند الکترونیکی و سایبری.

[۶] قدوسی محصل، محمدعلی و اسماعیلی، مهدی، ۱۳۹۵، بررسی تکنولوژی های سیستمهای تشخیص نفوذ، سومین کنفرانس ملی برق و کامپیوتر سیستمهای توزیع شده و شبکه های هوشمند.

[7] Jaiganesh, V., S. Mangayarkarasi and P. Sumathi. “Intrusion Detection Systems: A Survey and Analysis of Classification Techniques.” (2013).

[8] P. V. Amoli and T. Hämäläinen, "A real time unsupervised NIDS for detecting unknown and encrypted network attacks in high speed network," *2013 IEEE International Workshop on Measurements & Networking (M&N)*, Naples, Italy, 2013, pp. 149-154.

[9] S. Abbasghorbani and R. Tavoli, "Survey on sequential pattern mining algorithms," *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, Tehran, Iran, 2015, pp. 1153-1164.

[10] T. T. Aye, "Web log cleaning for mining of web usage patterns," *2011 3rd International Conference on Computer Research and Development*, Shanghai, China, 2011, pp. 490-494.

[11] Chau, D. H. P., Nachenberg, C., Wilhelm, J., Wright, A., & Faloutsos, C. (2011, April). Polonium: Tera-scale graph mining and inference for malware detection. In *Proceedings of the 2011 SIAM International Conference on Data Mining* (pp. 131-142). Society for Industrial and Applied Mathematics.

[۱۲] صابری، فروغ و احمدی، غلام رضا، ۱۳۹۸، مقایسه روش های شناسایی سیستمهای تشخیص نفوذ، سومین کنفرانس ملی فناوری های نوین در مهندسی برق و کامپیوتر.

[13] Islam, M. J., Mahin, M., Roy, S., Debnath, B. C., & Khatun, A. (2019, February). Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities. In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)* (pp. 1-6). IEEE.

[14] Jing, Q., Vasilakos, A.V., Wan, J. *et al.* Security of the Internet of Things: perspectives and challenges. *Wireless Netw* 20, 2481–2501 (2014).

[15] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., ... & Turner, J. (2008). OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review*, *38*(2), 69-74.

[16] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28.

[17] Dawoud, A., Shahristani, S., & Raun, C. (2018). Deep learning and software-defined networks: Towards secure IoT architecture. *Internet of Things*, *3*, 82-89.

[18] Alqallaf, M., & Wang, B. (2015, June). Software defined collaborative secure ad hoc wireless networks. In *2015 International Conference on Collaboration Technologies and Systems (CTS)* (pp. 196-203). IEEE.

[19] Oktian, Y. E., Lee, S., Lee, H., & Lam, J. (2017). Distributed SDN controller system: A survey on design choice. *computer networks*, *121*, 100-111.

ISSN: 2745-3673
http://www.Rcsj.ir

[20] Reddy, V. K., & Sreenivasulu, D. (2016). Software-defined networking with ddos attacks in cloud computing. *International Journal of innovative Technologies (IJIT)*, *4*(19), 3779-3783.

[21] Ayesh aImran, "SDN Controllers Security Issues", University of Jyväskylä, MS Thesis document in Web Intelligence and Service Engineering, November 2017.

[۲۲] سیادت، سیده صفیه و انگورج غفاری، محسن و مدنی، محمدرضوان، ۱۴۰۱ روشی جهت تشخیص نفوذ در اینترنت اشیاء با استفاده از نظریه بازی ها، نشریه علمی پدافند الکترونیکی و سایبری.

[۲۳] غیوری ثالث، مجید و سلیمی، علی، ۱۴۰۰ مدلی برای تشخیص نفوذ در اینترنت اشیاء با استفاده از بازی شراکت، فصلنامه علمی - پژوهشی فرماندهی و کنترل.

[۲۴] رئیسی، ذکریا و ادیب نیا، فضل اهلل و مصطفوی، سید اکبر، ۱۴۰۰، مروری بر سیستمهای تشخیص نفوذ در شبکه های LOT-SDN مبتنی بر الگوریتم های هوشمند، بیستمین کنفرانس ملی دانشجویی مهندسی برق ایران.