مقایسه و ارزیابی سیستم های تشخیص نفوذ در شبکه های موردی سیار

وحیده بابائیان[1]، مجید کرامتی مقدم

1-عضو هیأت علمی دانشگاه صنعتی بیرجند، دانشکده مهندسی کامپیوتر و صنایع، بیرجند

2- کارشناس دانشگاه صنعتی بیرجند، دانشکده مهندسی کامپیوتر و صنایع، بیرجند
babaiyan@birjandut.ac.ir

خلاصه

شبکه‌های موردی سیار نوع خاصی از شبکه‌های بی‌سیم هستند که هیچگونه زیرساخت ثابتی برای کنترل شبکه ندارند. در این شبکه‌ها گره‌ها می توانند به هر جا که می‌خواهند نقل مکان کنند و بدین لحاظ توپولوژی شبکه مرتب درحال تغییر است. هر گره هم به عنوان میزبان و هم به عنوان مسیریاب عمل می کند. این نوع شبکه‌ها درجهٔ آسیب پذیری بالایی در مقابل حملات و نفوذهای سوء استفاده کننده‌ها دارد. از این رو امنیت در این گونه شبکه‌ها مخاطرات بسیاری دارد و استفاده از سیستم‌های تشخیص نفوذ اهمیت بالایی در رفع این مسائل دارد. در این مقاله به بررسی روش‌های ارائه شده اخیر در این زمینه می‌پردازیم و آن‌ها را بر اساس متریک‌های متفاوت مورد مقایسه قرار می‌دهیم.

کلمات کلیدی: شبکه های موردی سیار، تشخیص نفوذ، امنیت

1. مقدمه

در دنیای امروزی، کامپیوتر و شبکه‌های کامپیوتری متصل به اینترنت نقش بسزایی در ارتباطات و انتقال اطلاعات دارند. در این بین افراد سودجو با دسترسی به اطلاعات مهم مراکز خاص یا اطلاعات افراد دیگر و با هدف اعمال نفوذ و یا حتی به هم ریختن نظم سیستم‌ها، عمل تعرض به سیستم‌های کامپیوتری را در پیش گرفته‌اند. از آنجا که از نظر تکنیکی ایجاد سیستم‌های کامپیوتری بدون نقاط ضعف و شکست امنیتی عملاً غیرممکن است، تشخیص نفوذ در سیستم های کامپیوتری با اهمیت خاصی انجام می‌شود. برای ایجاد امنیت کامل در یک سیستم کامپیوتری، علاوه بر دیواره‌آتش و دیگر تجهیزات جلوگیری از نفوذ، سیستم‌های دیگری به نام سیستم‌های تشخیص نفوذ مورد نیاز می‌باشند تا بتوانند در صورتی که نفوذگر از دیواره‌ی آتش، آنتی ویروس و دیگر تجهیزات امنیتی عبور کرد و وارد سیستم شد، آن را تشخیص داده و چاره‌ای برای مقابله با آن بیاندیشند. یک نفوذ در واقع فعالیت یا عملی است که توسط آن محرمانگی، صحت و تمامیت و یا دسترسی پذیری به منابع دچار اختلال و یا تعرض می‌شود. سیستم های تشخیص نفوذ یا IDS[1] ها در حال حاضر جزء اصلی ترین و کاملترین قسمت‌های یک سیستم پایش یا مانیتورینگ شبکه می‌باشند. تشخیص نفوذ در واقع قسمتی از یک سیستم حفاظتی است[1].

تشخیص نفوذ فرآیندی است که در آن رویدادها و رخدادهای یک سیستم یا شبکه پایش شده و بر اساس این پایش ها وقوع نفوذ به آن شبکه یا سیستم تشخیص داده می شود. شبکه‌های موردی سیار از یک مجموعه از نودهای خودمختار و سیار تشکیل شده است؛ لذا به دلیل همین سیار بودن نود، سیستم‌های تشخیص نفوذ پیشنهاد شده برای شبکه‌های متعارف و سیمی، که در نقاط استراتژیک همچون سوئیچ ها و مسیریاب ها قرار می گیرند، مناسب و قابل استفاده در MANET[2] نیستند. بنابراین باید یک سری تغییراتی روی مشخصات IDS های شبکه‌های سیمی اعمال شود تا قابل استفاده و مناسب برای شبکه‌های MANETگردد. یکی از مسائل نگران کننده در مورد شبکه‌های موردی سیار (MANETs) این است که در آن گره‌های متحرک خود را درون شبکه، بدون کمک هیچ زیرساخت از پیش تعریف شده‌ای سازماندهی کنند. برای به دست آوردن سطح قابل قبولی از امنیت در چندین زمینه، راه حل‌های امنیتی سنتی باید با یک مکانیزم تشخیص نفوذ همراه شوند[2]. نفوذ به مجموعه اقدامات غیر قانونی که یکپارچگی، محرمانگی یا دسترسی یک منبع را به خطر می اندازد اطلاق می شود[3] . نفوذ در شبکه به دسته های زیر تقسیم می شوند[4]:

ورود غیر قانونی: ورود غیرقانونی هنگامی روی می دهد که یک بیگانه به شناسه کاربر و کلمه رمز معتبر دسترسی پیدا می کند.

حملات ایفای نقش: هنگامی روی می دهد که نفوذی سیستم را متقاعد کند که وی یک کاربر مجاز با امتیاز بالا است.

رخنه به سیستم کنترل امنیت: نفوذگر تلاش می کند تا جنبه های امنیتی سیستم از قبیل کلمات رمز را اصلاح کند.

[1] Intrusion Detection System
[2] Mobile Ad hoc Networks

نشت: اطلاعات به خارج از سیستم انتقال داده می شوند.

جلوگیری از سرویس: منابع برای سایر کاربران غیر قابل دسترسی می شوند.

استفاده های خرابکارانه: این دسته از نفوذها شامل حملات متفاوتی از قبیل حذف فایل ها، سوء استفاده از منابع و غیره هستند.

برای نفوذ به سیستم ها و شبکه های کامپیوتری معمولاً از راه های مختلفی استفاده می شود. استفاده از عیوب نرم افزاری به عنوان اولین راه نفوذ به شبکه معرفی می گردد. در این روش‌ها نفوذی‌ها معمولاً به منظور ورود غیر قانونی به سیستم‌ها و شبکه‌های کامپیوتری، از عیوب نرم‌افزاری موجود در برنامه‌ها کاربردی متقاضی و سرویس گر، سیستم عامل، و پشته شبکه سوءاستفاده می کنند. متأسفانه در تولید نرم‌افزار به روش‌های غیر رسمی نمی‌توان تمامی خطاهای موجود در نرم‌افزارها را تشخیص داد و تنها از طریق تولید نرم‌افزار به روش‌های رسمی است که می توان این کار را انجام داد. اما با توجه به اینکه تولید نرم‌افزار با استفاده از روش‌های رسمی، سخت، زمانبر و پرهزینه است، شرکت‌های تولیدکنندهٔ نرم‌افزار استقبالی از روش‌های رسمی برای تولید نرم افزارها نمی کنند. در نتیجه با این واقعیت روبرو می‌شویم که در نرم‌افزارها همیشه نقاط ضعفی وجود دارد. راه دیگر در نفوذ به شبکه ها استفاده از نقاط ضعف طراحی می‌باشد. حتی اگر پیاده سازی یک نرم افزار کاملاً درست و مطابق با طراحی باشد، باز هم ممکن است در خود طراحی نقاط ضعفی وجود داشته باشد که منجر به نفوذ شود.

2. روش‌های تشخیص نفوذ

با افزایش روز افزون شبکه‌های کامپیوتری، تلاش برای جلوگیری و کشف نفوذ در شبکه ها امری ضروری است. تشخیص نفوذ عبارت است از فرایند شناسایی و پاسخ به فعالیت‌های مخرب که به شکل هدفمند منابع شبکه را مورد حمله قرار می‌دهد. سیستم تشخیص نفوذ با استفاده از روش‌های تحلیلی به کشف حملات می‌پردازد و منابع حمله را شناسایی می کنند و هشدارهای لازم برای مدیران ارسال می کنند[5] . سیستم‌های تشخیص نفوذ می‌توانند به صورت سخت افزاری یا نرم افزاری پیاده‌سازی شوند. یکی از مزایای این سیستم ها توانایی مستندکردن نفوذ یا تهدید تشخیص داده شده است در نتیجه جدیدترین الگوهای حمله برای عموم قابل شناسایی خواهد بود [6]. در واقع هدف سیستم تشخیص نفوذ جلوگیری از حمله نیست بلکه کشف و شناسایی حملات و تشخیص اشکالات امنیتی در شبکه های کامپیوتری و اعلام آن به مدیر سیستم است.

به منظور مقابله با نفوذگران به سیستم ها و شبکه های کامپیوتری، روش های متعددی تحت عنوان روش‌های تشخیص نفوذ ایجاد گردیده است که عمل نظارت بر وقایع اتفاق افتاده در یک سیستم یا شبکه‌ی کامپیوتری را بر عهده دارد. روش‌های تشخیص مورد استفاده در سیستم‌های تشخیص نفوذ به دو دسته تقسیم می‌شوند: روش تشخیص رفتار غیرعادی و روش تشخیص مبتنی بر امضاء.

روش تشخیص رفتار غیر عادی: در روش تشخیص رفتار غیرعادی، یک نما از رفتار عادی ایجاد می‌شود. یک ناهنجاری ممکن است نشان دهنده‌ی یک نفوذ باشد. برای تشخیص رفتار غیرعادی، باید رفتارهای عادی را شناسایی کرده و الگوها و قواعد خاصی برای آن ها پیدا کرد. رفتارهایی که از این الگوها پیروی می کنند، عادی بوده و رویدادهایی که انحرافی بیش از حد معمول آماری از این الگوها دارند، به عنوان رفتار غیرعادی تشخیص داده می‌شود. نفوذهای غیرعادی برای تشخیص بسیار سخت هستند، چون هیچگونه الگوی ثابتی برای نظارت وجود ندارد. معمولاً رویدادی که بسیار بیشتر یا کمتر از دو استاندارد انحراف از آمار عادی به وقوع می پیوندد، غیرعادی فرض می شود. به عنوان مثال اگر کاربری به جای یک یا دو بار ورود و خروج عادی به سیستم در طول روز، بیست بار این کار را انجام دهد، و یا کامپیوتری که در ساعت ۲:۰۰ بعد از نیمه شب مورد استفاده قرار گرفته در حالی که قرار نبوده کامپیوتر فوق پس از ساعت اداری روشن باشد. هر یک از این موارد می‌تواند به عنوان یک رفتار غیر عادی در نظر گرفته شود[7]. تکنیک ها و معیارهایی که در تشخیص رفتار غیرعادی به کار می‌روند، عبارتند از: تشخیص سطح آستانه، معیارهای آماری، معیارهای قانون گرا و....

در تشخیص سطح آستانه تعداد ورود و خروج به / از سیستم و یا زمان استفاده از سیستم، از مشخصه‌های رفتار سیستم و یا استفاده کننده است که می توان با شمارش آن به رفتار غیرعادی سیستم پی برد و آن را ناشی از یک نفوذ دانست. معیارهای آماری در نوع پارامتریک، مشخصات جمع شده براساس یک الگوی خاص در نظر گرفته می شود و در حالت غیر پارامتریک بر اساس مقادیری که به تجربه حاصل شده است مقایسه صورت می گیرد. از IDS های معروف که از رهگیری آماری برای تشخیص نفوذ رفتار غیرعادی استفاده می کنند، می توان NIDS را نام برد. معیارهای قانون گرا شبیه به معیارهای آماری غیرپارامتریک است، به‌طوری که داده‌ی مشاهده شده براساس الگوهای استفاده شده‌ی مشخصی به طور قابل قبول تعریف می‌شود. اما با الگوهایی که به عنوان قانون مشخص شده فرق دارد و به صورت شمارش نیست. روش‌های خوشه‌بندی، شبکه‌های عصبی، الگوریتم‌های ژنتیک و مدل‌های سیستم ایمنی به عنوان سایر معیارها در سیستمتشخیص نفوذ استفاده می‌شوند. دو معیار اول یعنی تشخیص سطح آستانه و معیارهای آماری در IDSهای تجاری استفاده می‌شوند. متاسفانه تشخیص دهندگان نفوذهای غیرعادی و IDSهایی از این نوع، باعث ایجاد تعداد زیادی هشدار نادرست می‌شوند و آن هم به خاطر این است که الگوهای رفتاری از جانب استفاده کنندگان و سیستم بسیار متفاوت است. در عوض محققان ادعا می کنند برخلاف روش‌های تشخیص مبتنی بر امضاء (که حتماً باید با الگوهای حملات قبلی منطبق باشند)، روش‌های تشخیص رفتار غیرعادی، قادر به کشف انواع حملات جدید هستند.

تعدادی از IDSهای تجاری از انواع تشخیص دهندگان رفتار غیرعادی هستند و اغلب IDS ها از این نوع بیشتردرکارهایی‌چون پویش پورت استفاده می‌شوند.با این وجود ایجاد یک سیستم تشخیص نفوذ براساس روش تشخیص رفتارهای غیرعادی همیشه کار آسانی نیست[8].

روش تشخیص مبتنی بر امضاء: در این تکنیک که معمولاً با نام تشخیص مبتنی بر امضاء شناخته شده است، الگوهای نفوذ از پیش ساخته شده (امضاء) به صورت قانون نگهداری می شوند. به طوری که هر الگو انواع متفاوتی از یک نفوذ خاص را در بر گرفته و در صورت بروز چنین الگویی در سیستم، وقوع نفوذ اعلام می‌شود. در این روش‌ها، معمولاً تشخیص دهنده دارای پایگاه داده‌ای از امضاء ها یا الگوهای حمله است و سعی می کند با بررسی ترافیک شبکه، الگوهای مشابه با آن‌چه را که در پایگاه داده‌ی خود نگهداری می کند، بیابد. این دسته از روش‌ها تنها قادر به تشخیص نفوذهای شناخته شده می‌باشند و در صورت بروز حملات جدید در سطح شبکه، نمی‌توانند آن‌ها را شناسایی کنند و مدیر شبکه باید همواره الگوی حملات جدید را به سیستم تشخیص نفوذ اضافه کند. از مزایای این روش دقت در تشخیص نفوذهایی است که الگوی آن‌ها عیناً به سیستم داده شده است[7].

انواع معماری سیستم های تشخیص نفوذ

سیستم تشخیص نفوذ مبتنی بر میزبان(HIDS) : این سیستم، شناسایی و تشخیص فعالیت های غیرمجاز بر روی کامپیوتر میزبان را بر عهده دارد. سیستم تشخیص نفوذ مبتنی بر میزبان می تواند حملات و تهدیداتی را روی سیستم های بحرانی تشخیص دهد (شامل دسترسی به فایل ها، اسب های تروا و ...) که توسط سیستم های تشخیص نفوذ مبتنی بر شبکه قابل تشخیص نیستند. HIDS فقط از میزبان هایی که روی آن ها مستقر است محافظت می کند. مزیت HIDS توانایی سازماندهی بسیار خوب تصمیمات برای هر میزبان منحصر به فرد می‌باشد. به عنوان مثال نیازی نیست روی میزبانی که سرویس نام گذاری دامنه (DNS) را اجرا نمی کند، قوانین چندگانه‌ای بررسی شوند که برای تشخیص سوءاستفاده‌ها از DNS طراحی شده‌اند. در نتیجه کاهش تعداد قوانین مربوطه، کارآیی را بالا می‌برد و سربار پردازنده را برای هر میزبان کاهش می‌دهد. همچنین HIDS ها اطلاعات مشخصی در این باره که نفوذ از کجا، توسط چه کسی و چه موقع اتفاق افتاده است را فراهم می کنند. این عمل بسیار مفید است چون هیچ گونه کم کاری و حذف وجود ندارد. درIDSهای مبتنی بر میزبان احتمال هشدارهای نادرست بسیار کم است، چرا که اطلاعات مستقیماً به کاربران برنامه های کاربردی بر می گردد. این IDSها ترافیک کمتری نسبت به NIDS (که در ادامه توضیح داده ایم) داشته و تأکید بیشتری روی حسگرهای چندگانه ی مجزا و ایستگاه های مدیریت مرکزی دارند. از معایب آن‌ها سازگاری کم بین سیستم عامل و در نتیجه نرم‌افزارهای چندگانه است. اغلب IDSهای مبتنی بر میزبان تنها برای یک سیستم عامل نوشته می شوند. دیگر این که آن‌ها بعضی از حملات را که در لایه های پایین شبکه انجام می شوند، شناسایی نمی کنند[7].

سیستم تشخیص نفوذ مبتنی بر شبکه(NIDS) :نام NIDS از این حقیقت مشتق شده است که از منظر محلی که قرار گرفته، بر تمام شبکه نظارت دارد. شناسایی و تشخیص نفوذهای غیرمجاز قبل از رسیدن به سیستم های بحرانی، به عهده‌ی سیستم تشخیص نفوذ مبتنی بر شبکه است NIDS ها اغلب از دو بخش ناظر (حسگر) و عامل تشکیل شده اند. این دو بخش اغلب در پشت دیواره‌ی آتش و بقیه‌ی نقاط دسترسی برای تشخیص هر نوع فعالیت غیرمجاز نصب می‌شود. عامل‌های شبکه می توانند جایگزین زیرساختار شبکه شوند تا ترافیک شبکه را جستجو کنند. نصب عامل‌ها و ناظرها این مزیت را دارد که هر نوع حمله‌ای را در ابتدا از بین می‌برد. ضمناً دنباله‌های بررسی یک یا چند میزبان می‌توانند برای جستجوی علائم حملات، مفید باشند. NIDS ها می‌توانند طوری برنامه ریزی شوند که مزاحمتی در طول کار ایجاد نشود. به طوری که هر حمله‌ای که NIDS تشخیص می‌دهد، درون فایل رویدادها ثبت کرده و بدون این که مهاجم متوجه شود، به مدیر شبکه اطلاع می‌دهد. سیستم‌های تشخیص نفوذ مبتنی بر شبکه نیاز به کلمه‌ی عبور برای برنامه‌های کاربردی، حقوق مربوط به سیستم عامل شبکه یا اتصالات مربوط به سیستم در هنگام اجرای نرم‌افزار ندارد. همچنین از آنجا که این سیستم‌ها در سطح لایه‌ی شبکه عمل می کنند، به سیستم عامل وابستگی ندارند. ضمناً هیچگونه سربار و تغییری روی سرویس دهنده‌ها و ایستگاه‌های کاری به وجود نمی‌آورند، چرا که برای این سیستم‌های تشخیص نفوذ نیازی به نصب ابزارهای اضافی نیست[9].

سیستم تشخیص نفوذ توزیع شده(DIDS) : این سیستم‌ها از چندین NIDS یا HIDS یا ترکیبی از این دو نوع همراه یک ایستگاه مدیریت مرکزی تشکیل شده است. بدین صورت که هر IDS که در شبکه موجود است گزارش‌های خود را برای ایستگاه مدیریت مرکزی ارسال می کند. ایستگاه مرکزی وظیفه بررسی گزارش‌های رسیده و آگاه سازی مسئول امنیتی سیستم را برعهده دارد. این ایستگاه مرکزی همچنین وظیفه به روزرسانی پایگاه قوانین تشخیص هر یک از IDS های موجود در شبکه را برعهده دارد . شبکه بین NIDSها با سامانه مدیریت مرکزی می تواند خصوصی باشد و یا این که از زیرساخت موجود برای ارسال داده ها استفاده شود. وقتی از شبکه‌ی موجود برای ارسال داده های مدیریتی استفاده شود، امنیت‌های اضافی به وسیله‌ی رمزنگاری یا تکنولوژی شبکه‌های خصوصی مجازی حاصل می گردد[9].

2. تحقیقات پیشین

در تحقیقات انجام شده [10] در این زمینه ، یک معماری IDS توزیع شده و مشارکتی با استفاده از عامل‌های سیار پیشنهاد کرده‌اند. در این معماری روی هر نود یک سیستم تشخیص نفوذ محلی (LIDS) برای عملیات تشخیص نفوذ محلی پیاده سازی شده است که می‌تواند با همکاری دیگر LIDSها گسترش پیدا کرده تا عملیات تشخیص نفوذ را بصورت سراسری انجام دهد. دو نوع داده بین LIDSها مبادله می‌شود. برای بدست آوردن اطلاعات تکمیلی از طریق همکاری دیگر نودها و هشدارهای نفوذ برای اطلاع دادن به دیگر نودها از تشخیص نفوذ محلی استفاده می‌شود. در روش‌های شناسایی، از عامل IDSمحلی می‌توان هم در تشخیص‌های مبتنی بر ناهنجاری ، هم در مبتنی بر سوءرفتار و هم در مبتنی بر معیار بهره برد. هنگامیکه یک نفوذ محلی شناسایی می‌شود، LIDS پاسخی را تولید کرده و به دیگر نودهای شبکه نیز اطلاع رسانی می‌کند. به‌دنبال دریافت یک هشدار ، LIDSهای دیگر می‌توانند خود را در مقابل نفوذ محافظت نمایند.

در تحقیق درگری یک سیستم تشخیص نفوذ چند سنسوری را مبتنی بر تکنولوژی عامل سیار پیشنهاد شد[11] .این سیستم را می‌توان به سه ماژول اصلی تقسیم نمود که هر کدام بیانگر یک عامل سیار با یک عملکرد مشخص است. این معماری از سه عامل سیار؛ عامل ناظر، عامل تصمیم گیر و عامل تولید پاسخ برای شناسایی و مقابله با نفوذهای صورت گرفته، استفاده می‌کند. عامل ناظر مسئول نظارت در سطح شبکه و میزبان است؛ عامل عمل نیز در صورت مشاهده فعالیت‌های نفوذی عکس العمل مناسبی مانند قطع یا مسدود کردن نفوذ را انجام می دهد و عامل تصمیم گیر هم عمل تصمیم گیری در سطح بالا و با دقت کافی را انجام می دهد. از آنجائیکه نودها می‌توانند آزادانه در سراسر شبکه های موردی سیار حرکت کنند، داشتن ساختار سلسله مراتبی ایستا برای این نوع شبکه ها با توجه به توپولوژی پویا، مناسب نمی باشد. به همین دلیل در تحقیق دیگری [12] یک تشخیص نفوذ سلسله مراتبی که قابلیت مقیاس پذیری برای شبکه های بزرگ با استفاده از خوشه بندی را دارد، پیشنهاد شده است که شبیه روش [11] است، اما می‌تواند ساختاری گسترده‌تر از ساختار دو سطحی داشته باشد. بنابراین، نودهای سطح اول، سرخوشه ها می‌باشند در حالیکه نودهای سطح دوم، نودهای برگ هستند. در این مدل هر نود وظیفه نظارت، ثبت وقایع، آنالیز، پاسخ و دادن هشدار یا گزارش به سرخوشه‌ها را دارد. سرخوشه ها علاوه براین وظایف، باید 1)یکپارچه سازی و فیلتر کردن داده‌ها 2) انجام محاسباتی در مورد نفوذ 3) و مدیریت امنیت را بر عهده گیرند.

در تحقیق دیگری یک سیستم تشخیص نفوذ مبتنی بر ناحیه را پیشنهاد شده است، که در آن شبکه موردی سیار به چندین ناحیه غیر هم پوشش تقسیم می شود. در این سیستم نودها را می توان به دو نوع تقسیم بندی نمود نودهای درون ناحیه‌ای و نودهای لبه ناحیه ای . دیگر مولفه‌های این سیستم ماژول جمع آوری اطلاعات، موتور تشخیص،ماژول‌های تجمیع و همبستگی محلی و تجمیع و همبستگی سراسری می‌باشد. ماژول جمع‌آوری اطلاعات و موتور تشخیص به ترتیب مسئول جمع‌آوری اطلاعات حسابرسی محلی و آنالیز هر نشانه‌ای از نفوذ می‌باشند. ماژول تجمیع و همبستگی محلی ، مسئول ترکیب نتایج حاصله از موتورهای تشخیص محلی و تولید هشدار در صورت شناسایی یک رفتار ناهنجار، می‌باشد .این هشدارها برای تمامی نودها داخل یک ناحیه منتشر می‌شود . در این سیستم عملکرد تجمیع و همبستگی سراسری به نوع نود وابسته است. اگر نود یک نود درون ناحیه‌ای باشد، فقط گزارش‌های تولید شده را به نودهای لبه ناحیه‌ای ارسال می‌کند؛ و اگر نود یک نود لبه ناحیه‌ای باشد، گزارش‌ها را از بقیه نودهای درون ناحیه‌ای دریافت کرده، و آن‌ها را تجمیع و سرهم کرده و با گزارش‌های خودش مقایسه می‌کند و درصورت لزوم هشدارهایی را تولید می‌کند.ماژول پاسخ به نفوذ نیز مسئول مدیریت هشدارهای تولید شده از تجمیع و همبستگی سراسری می‌باشد[13].

در جدول 1 مقایسه اجمالی از روش های توضیح داده شده ارائه شده است. این روش ها را از لحاظ معماری، نوع حمله و تکنیک شناسایی مورد بررسی قرار داده ایم. بعضی حملات در فاز مسیریابی نیز شبکه مورد حمله قرار گرفته است و سیستم های پیشنهادی متناسب با نوع تهدید نام برده شده است.

جدول1 : مقایسه IDSهای پیشنهاد شده برای Manet

نویسندگان	نام روش	معماری	نوع حملات			تکنیک شناسایی	مسیریابی	همکاری
			خودخواه	مسیریابی	تصدیق			
Zhang,Lee [13]	-	توزیع شده و مشارکتی	خیر	بلی	خیر	ناهنجاری	AODV, DSR, DSDV	عامل IDS برای تشخیص بصورت مشارکتی
Albers, Camp[10]	LIDS	توزیع شده و مشارکتی	خیر	خیر	خیر	سوءرفتار، ناهنجاری	تعریف نشده	عامل سیار IDS محلی برای تشخیص نفوذ
Kachirski, Guha[11	-	سلسله مراتبی	خیر	خیر	خیر	ناهنجاری	تعریف نشده	IDS سلسله‌مراتبی با استفاده از عامل سیار
Steme و همکاران [12]	-	سلسله مراتبی	خیر	خیر	خیر	سوءرفتار، ناهنجاری	تعریف نشده	IDS سلسله‌مراتبی پویا
Wu,Sun, W.pooch [14]	ZBIDS	توزیع شده و مشارکتی	خیر	بلی	خیر	ناهنجاری	DSR	محافظت پروتکل مسیریابی از تخریب‌شدن

3. نتیجه گیری

امروزه کاربرد شبکه‌های بی سیم بر هیچکس پوشیده نیست، به اطرافمان که نگاه می‌کنیم در می‌یابیم که چقدر این‌گونه شبکه‌ها در نحوهٔ زندگی ما تاثیر دارند. یکی از انواع شبکه‌های بی‌سیم شبکه‌های موردی سیار می‌باشند. از جمله کاربردهای آن‌ها می توان به کاربردهای نظامی و میادین جنگی، عملیات نجات و کمک رسانی، کشتی‌ها و ناوگان دریایی، سالن‌های کنفرانس و کلاس‌های آموزشی اشاره کرد. برای برپا کردن شبکه‌های موردی سیار هیچ زیرساخت خاصی لازم نیست، گره‌ها به هر طریق که می‌خواهند جابجا می‌شوند، هر گره هم نقش میزبان را دارد و هم به عنوان مسیریاب عمل می‌کند.

از مزایای این نوع شبکه‌ها برپا شدن سریع آن‌ها و عدم نیاز به زیرساخت‌ها می‌باشد. اما به علت نوع خاص شبکه بندی آنها از لحاظ مسائل امنیتی نگرانی‌هایی را ایجاد می‌کنند. مثلا پروتکل‌های مسیریابی ارائه شده برای این شبکه‌ها بر اساس همکاری بین گره‌های شبکه ارائه شده‌اند و اگر در این میان یکی از گره‌ها متخاصم و اخلال‌گر باشد می‌تواند کل شبکه را آلوده کرده و صدمات جبران ناپذیری را به شبکه وارد کند.

با توجه به این مطالب پیشنهاد می‌شود که در کارهای آینده از روش‌های ترکیبی یادگیری ماشین و روش‌های آماری برای نیل به دقت بیشتر در فرآیند تشخیص نفوذ استفاده شود. هم‌چنین بنظر می‌رسد اینگونه سیستم‌ها تا زمانی که به صورت واقعی و کاربردی پیاده سازی و آزمایش نشوند، نمی‌توان با اطمینان بالایی در مورد کارایی و موثر بودن آن‌ها بحث کرد.

4. مراجع

1. K. Kumar, (2009), "Intrusion detection in mobile Ad hoc networks," University of Toledo,

2. M. Ngadi, A. H. Abdullah, and S. Mandala, (2008), "A survey on MANET intrusion detection," International Journal of Computer Science and Security, vol. 2, pp. 1-11,

3. Ujwala Ravale, Nilesh Marathe, Puja Padiya.(2015) "Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function." International Conference on Advanced Computing Technologies and Applications (ICACTA), Procedia Computer Science, 45, 428-435.

4. S.E. Smaha, Haystack, (1988),"An Intrusion Detection System", In Fourth Aerospace Computer Security Applications Conference, TX

5. Wei-Chao Lin, Shih-Wen Ke, and Chin-Frong Tsai. (2015)"CANN: An Intrusion Detection System Based On Combining Cluster Centers And Nearest Neighbors."Knowledge-Basedsystem pp.13-21.

6. Solane Duque,Mohd Nizam Bin Omar. (2015) "Using Data Mining Algorithms for Developing a Model for Intrusion Detection System (Ids)." Conference Organized by Missouri University of Science and Technology San Jose, CA, Procedia Computer Science pp.46-51

[7].مسعود ستوده فر، "کشف نفوذ در شبکه مبتنی بر قوانین فازی تطبیق پذیر "،پایان نامه کارشناسی ارشد، دانشگاه فردوسی مشهد، نهمین کنفرانس سالانه انجمن کامپیوتر ایران،2004-01-21

8. Paul Innella and Oba McMillan,(2001) "An Introduction to Intrusion Detection Systems", Tetrad Digital Integrity, LLC,

9. B. Caswell, J. Beale, and A. Baker, (2007)"Snort IDS and IPS Toolkit," America: Syngress,

10. P. Albers, O. Camp, J.-M. Percher, B. Jouga, L. M, ©and R. S. Puttini, (2002) "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," in Wireless Information Systems, pp. 1-12

11. O. Kachirski and R. Guha, (2003)"Effective intrusion detection using multiple sensors in wireless ad hoc networks," in System Sciences, Proceedings of the 36th Annual Hawaii International Conference on, , p. 8 pp.

12. D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C. Y.Tseng, and T. Bowen,(2005) "A general cooperative intrusion detection architecture for MANETs," inInformation Assurance, 2005. Proceedings. Third IEEE International Workshop on, pp. 57-70

13- Y. Zhang and W. Lee, (2000)"Intrusion Detection in Wireless Ad Hoc Networks", 6th Int'l. Conf. Mobile Comp. and Net. Aug, pp. 275–83.

14- B.Sun,k.Wu,and U.W.pooch. (2003), "Routing Anomaly Detection in Mobile Ad hok networks", proceedings of 12th international conference on computer communications and networks (ICCCN 03), Dallas, Texas, pp.69-78.