۱۳۶۵
دانشگاه جامع امام حسین(ع)
دانشکده و پژوهشکده فنی و مهندسی

مجله علمی- پژوهشی «علوم و فناوری‌های پدافند غیرعامل»
سال اول، شماره ۱، پائیز ۱۳۸۹: ص ۱۵-۲۲

Available online:
www.adst.ir

ارائهٔ یک سامانهٔ تشخیص نفوذ برای مقابله با حملهٔ منع سرویس در شبکه‌های بی‌سیم اقتضایی

محمود صالح اصفهانی[1*]، مهرداد ابوعلی[2]

۱- استادیار، ۲- کارشناس ارشد، گروه رایانه، دانشکده و پژوهشکده فناوری اطلاعات و ارتباطات، دانشگاه جامع امام حسین(ع)

E-mail: msaleh@ihu.ac.ir

(دریافت: ۸۸/٤/۲۳ ، پذیرش: ۸۸/۸/۲٤)

چکیده

در سال‌های اخیر توجه روزافزون به تبادل داده دیجیتال به صورت بی‌سیم موجب بوجود آمدن فناوری‌های جدیدی در عرصه شبکه‌های رایانه‌ای گردیده است. یکی از این فناوری‌ها، شبکه‌های بی‌سیم اقتضایی می‌باشد که در آن گره‌های شبکه بدون استفاده از زیرساخت ثابت و معین قادرند به‌سرعت یک شبکه چند پرشی رادیویی را تشکیل دهند و در آن به تبادل داده بپردازند. تغییرات توپولوژیکی، مداوم و عدم وابستگی گره‌ها به یک واحد مرکزی، از خصوصیات طبیعی شبکه‌های اقتضایی می‌باشد. به دلیل طبیعت متغیر ارتباطات بین گره‌ها و همچنین برخی خصوصیات ذاتی شبکه‌های بی‌سیم، برقراری امنیت در اینگونه شبکه‌ها کار ساده‌ای نیست.

در این مقاله، یک سامانه تشخیص نفوذ جدید برای تشخیص حملات فعال علیه مسیریابی در شبکه‌های اقتضایی ارائه می‌گردد. این سامانه پس از تشخیص حمله با اتخاذ تدابیری، اثر حمله را به حداقل رسانده و عملکرد شبکه را در حد قابل قبولی نگه می‌دارد. مزیت این سامانه تشخیص نفوذ، مقابله سریع یا عاجل آن با گره‌های حمله‌کننده و خنثی کردن حمله آنها می‌باشد. سامانه تشخیص نفوذ پیشنهادی، منجر به تغییر پروتکل مسیریابی نمی‌گردد، بلکه به‌عنوان یک واسط بین ترافیک شبکه و پروتکل مسیریابی قرار می‌گیرد. عملکرد سامانه پیشنهادی با استفاده از نرم‌افزار OPNET شبیه‌سازی و تحلیل شده و نتایج عددی آن نیز ارائه گردیده است.

کلیدواژه‌ها: سامانه‌های تشخیص نفوذ؛ شبکه‌های بیسیم اقتضایی؛ حملات منع سرویس

An IDS for Detection of Active Attacks against Routing in Mobile Ad Hoc Networks

M. Saleh Esfehani*, M. Abo Ali
Department of ITC, Imam Hossein University, Tehran, Iran
Email: msaleh@ihu.ac.ir

Abstract

In recent years, wireless technology has experienced a tremendous rise in popularity and usage, opening new fields of applications in the domain of networking. One of such fields concerns Ad Hoc networks in which the mobile nodes do not rely on any predefined network infrastructure. By definition, the nature of Ad Hoc networks is dynamically changing and they have a fully decentralized topology. Hence security is hard to achieve due to the dynamic nature of the participating nodes as well as the vulnerabilities and limitations of the wireless transmission medium. In this paper, an IDS for detection of active attacks against the routing fabric of mobile Ad Hoc networks is proposed. The system is designed to take countermeasures to minimize the effectiveness of an attack and keep the performance of the network within acceptable limits. The novelty of the system lies in the fact that it does not alter the basic routing protocol of the network. The proposed architecture was simulated with OPNET network simulator and numerical results were studied and analyzed.

Keywords: Ad Hoc Networks; Intrusion Detection System; Routing Fabric; Active Attack; Security

۱. مقدمه

شبکه‌های بی‌سیم اقتضایی اغلب در جایی پیاده‌سازی می‌شوند که امکان ایجاد زیرساخت شبکه سیم‌کشی شده یا سلولی وجود نداشته باشد و یا نیازی به این کار احساس نشود. ارسال اطلاعات صوتی و تصویری در مناطق جنگی و آگاهی از موقعیت تاکسی‌ها در شهر، نمونه‌هایی از به‌کارگیری اینگونه شبکه‌ها است. یکی از ویژگی‌های مهم شبکه‌های اقتضایی این است که گره‌های شبکه بدون نیاز به هرگونه زیر ساخت قبلی شبکه با هم ارتباط برقرار می‌کنند [۱]. شبکه‌های بی‌سیم اقتضایی در حقیقت مجموعه‌ای از گره‌های بی‌سیم می‌باشند که قادرند به‌سرعت یک شبکه چند پرشی رادیویی را بدون نیاز به زیرساخت خاص یا مدیریت مرکزی، تشکیل دهند [۲].

یکی از مشخصه‌های شبکه‌های اقتضایی این است که همه گره‌ها باید در امر مسیریابی شرکت داده شوند [۳]. از این رو روش‌های مسیریابی سنتی در این شبکه‌ها قابل استفاده نیست. بنابراین گره‌های واقع در مسیر بستهٔ داده قادر به واکاوی محتوای بسته هستند. همچنین هر گرهٔ جدید که در تیررس گره‌های این شبکه قرار گیرد قادر خواهد بود داده‌های در حال تبادل در اطراف خود را شنود نموده و حتی به این شبکه بپیوندد. بنابراین شبکه‌های اقتضایی علاوه بر مخاطرات شبکه‌های باسیم، در معرض مخاطرات امنیتی جدیدی هستند که با استفاده از روشهای امنیتی مخصوص شبکه‌های باسیم قابل حل نمی‌باشد [٤]. بدین دلیل امنیت در شبکه‌های اقتضایی مسئله بزرگی است که محققان بسیاری در سرتاسر دنیا را به خود مشغول داشته است.

رویکردهای اصلی محققان برای حل مسئله امنیت در این شبکه‌ها را می‌توان به دو دسته اصلی تقسیم کرد [۵]. رویکرد اول طراحی و استفاده از روش‌های مسیریابی امن در اینگونه شبکه‌ها می‌باشد. مبنای این روش‌های مسیریابی معمولاً بر پایه استفاده از رمزنگاری در شبکه می‌باشد. اما از آنجا که به‌خاطر ساختار غیر متمرکز شبکه‌های اقتضایی، امکان استفاده از مراکز قابل اعتماد برای مدیریت کلید و احراز هویت وجود ندارد، این روش بخوبی مورد استقبال قرار نگرفته است.

رویکرد دوم و اصلی محققان برای حل مشکل امنیت در شبکه‌های اقتضایی، استفاده از سیستم‌های تشخیص نفوذ می‌باشد. با استفاده از این روشها، امکان شناسایی رفتارهای مشکوک و حمله‌های احتمالی محقق می‌گردد. هدف سیستم‌های تشخیص نفوذ معمولاً یا تشخیص رفتارهای مشکوک و یا تشخیص حملات شناخته شده می‌باشد [٦].

در روش تشخیص رفتارهای مشکوک، معمولاً با استفاده از روش‌هایی مثل شبکه‌های عصبی یا داده کاوی[1]، رفتارهای غیر عادی از رفتارهای عادی جدا شده و گره‌ای که رفتار مشکوکی از خود نشان می‌دهد به‌عنوان گره حمله‌کننده معرفی می‌گردد. از این رو این روش‌ها معمولاً با قطعیت عمل نمی‌کنند و گاهی اوقات به اشتباه گره‌های عادی به‌عنوان گره‌های خاطی معرفی می‌شوند. در گونه دوم سیستم‌های تشخیص نفوذ، ابتدا عملکرد حملات شناخته شده به سیستم آموزش داده می‌شود تا در مواقع رخداد حمله در شبکه تمهیدات لازم را جهت مقابله با حمله‌کننده اتخاذ کرده و تا حد ممکن آثار حمله را کاهش دهد. به‌خاطر قطعیت بیشتر این روش در تشخیص گره‌های خاطی، بسیاری از شرکت‌ها از این روش برای تشخیص حملات در محصولات تجاری خود استفاده می‌کنند [٥].

در این مقاله جهت برقراری امنیت در شبکه‌های اقتضایی، یک سامانه تشخیص نفوذ با استفاده از روش دوم، یعنی تشخیص حملات شناخته شده، معرفی می‌گردد. سامانه تشخیص نفوذ معرفی شده، در صدد تشخیص حمله منع سرویس در شبکه از طریق *هدر دادن منابع* گره‌ها می‌باشد. به عبارت دیگر در زمانی که شخص حمله‌کننده در صدد به اشباع رساندن شبکه و تحلیل منابع شبکه می‌باشد، سامانه تشخیص نفوذ، گره حمله‌کننده را شناسایی کرده و گره خاطی را از شبکه اخراج می‌نماید.

سایر بخش‌های این مقاله بصورت زیر می‌باشد؛ در بخش ۲ پاره‌ای از تحقیقات و کارهای صورت گرفته در زمینه سیستم‌های تشخیص نفوذ در شبکه‌های اقتضایی مورد بررسی قرار گرفته و مخاطرات امنیتی شبکه‌های اقتضایی و روش‌های مقابله آنها بیان می‌گردد. طراحی سامانه تشخیص نفوذ پیشنهادی در بخش ۳ ارائه شده که با استفاده از آن، حمله به شبکه شناسایی گردیده و تمهیدات دفاعی اعمال می‌گردد. نتایج شبیه‌سازی عملکرد سامانه تشخیص نفوذ پیشنهادی در بخش ۴ مورد ارزیابی قرار خواهد گرفت. بخش ۵ نیز به جمع‌بندی عملکرد روش پیشنهادی و کارهای آینده اختصاص داده شده است.

1- Data Mining

۲. مخاطرات امنیتی شبکه‌های اقتضایی

گسترش استفاده از شبکه‌های اقتضایی و اهمیت برقراری امنیت در اینگونه شبکه‌ها باعث شده است که تحقیقات فراوانی در این زمینه صورت پذیرد. «**ژانگ**» و « **لی**» از نخستین افرادی هستند که به بررسی سیستم‌های تشخیص نفوذ در شبکه‌های اقتضایی پرداخته‌اند [۷]. در این مقاله به دو تکنیک اصلی تشخیص حملات شناخته شده و تشخیص رفتارهای مشکوک اشاره شده و نویسندگان بر اساس یک ساختار توزیع شده همه گره‌ها را به IDS مجهز ساخته‌اند. همچنین در نهایت برای تشخیص حملات از روش تشخیص رفتارهای مشکوک بهره جسته و با استفاده از معیارهایی چون سرعت گره، درصد تغییر مسیر، درصد تغییر تعداد پرش، و فاصله، رفتارهای مشکوک شناسایی می‌گردد. قابلیت پروتکل‌های مسیریابی مختلف در جهت تسهیل عملیات تشخیص نفوذ در زمانی که هدف، تشخیص حملات شناخته شده می‌باشد، مورد مطالعه قرار گرفته است [۸]. این مطالعه با اجرای IDS بر روی تعدادی از گره‌ها، سعی در کم کردن استفاده از منابع دارد. این مطالعه نشان می‌دهد که لازم نیست همه گروه‌ها IDS برداشته باشند؛ بلکه می‌توان به‌طور تصادفی تعدادی از گره‌ها را به IDS مجهز کرد. در گزارش دیگری امنیت در لایه شبکه مورد بررسی قرار گرفته و از IDS به‌عنوان ابزاری جهت تشخیص حملات بر اساس یک SVM[1] استفاده شده است [۹]. آنها به این نتیجه رسیدند که یک سامانه تشخیص نفوذ سلسه مراتبی توزیع شده، کارایی بسیار بالایی دارد.

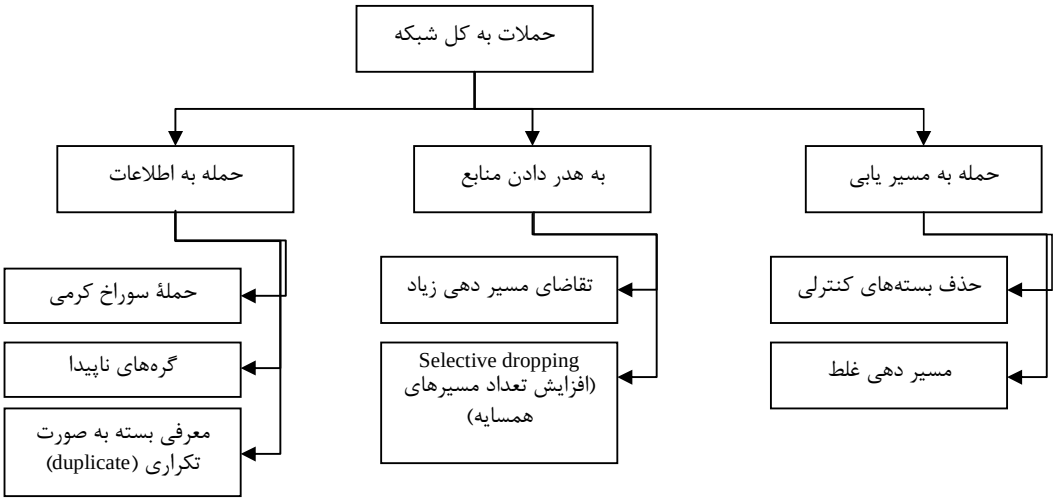
«**بروچ**» و «**کالوین**» مروری بر تحقیقات جدید درباره سیستم‌های تشخیص نفوذ در شبکه‌های اقتضایی ارائه می‌نمایند [۱۰]. در حقیقت نویسندگان، IDS ها را به سه دسته مبتنی بر امضاء، مبتنی بر رفتار مشکوک و مبتنی بر مشخصه‌ها تقسیم‌بندی کرده‌اند. تشخیص بر مبنای امضاء، ترافیک شبکه را برای یافتن حملات شناخته شده بررسی می‌کند. بنابراین، این روش نمی‌تواند حملات جدید را شناسایی کند. در تشخیص مبتنی بر رفتار مشکوک، با توجه به رفتار عادی شبکه، رفتارهای غیر عادی شناسایی می‌گردد. بنابراین با استفاده از این روش ممکن است حملات جدید شناسایی شوند. در روش سوم یعنی تشخیص مبتنی بر مشخصه‌ها، مجموعه‌ای از حدود عملکردهای صحیح مشخص می‌گردد و انحراف از این حدود به‌عنوان حمله شناخته می‌شود. بنابراین، این روش نیز می‌تواند منجر به تشخیص حملات جدید گردد. در گزارش دیگری نویسندگان یک ماشین حالت متناهی برای مشخص کردن عملکرد صحیح مسیریابی AODV طراحی نموده و با استفاده از ترافیک مشاهده شده در هر گره، انحرافات گره‌ها را از عملکرد صحیح مشخص کرده‌اند [۱۱]. روشی برای شناسایی گره‌های خودخواه در شبکه با استفاده از یک ماشین حالت متناهی در مسیریابی AODV نیز ارائه شده است [۱۲]. با استفاده از این ماشین، حالت رفتار گره‌های شبکه مورد بررسی قرار گرفته و در نهایت گره‌های شبکه در دو دسته گره‌های خودخواه و گره‌های عادی قرار می‌گیرند. در مقاله‌ای با استفاده از سازوکار پاسبانی[2]، گره‌هایی که بسته‌های داده را حذف می‌کنند شناسایی شده و با استفاده از سازوکار نمره‌دهی به مسیرها[3]، از مسیرهای شامل گره خطاکار پرهیز می‌گردد [۱۳].

یک تقسیم‌بندی درباره مخاطرات امنیتی شبکه‌های اقتضایی، از نقطه نظر هدف حمله می‌باشد. بدین صورت که هدف برخی از حملات در شبکه، یک گره خاص می‌باشد و برخی دیگر با هدف از کار انداختن کل شبکه کار می‌کنند. حالت دوم خود به سه دسته حمله به مسیریابی، به هدر دادن منابع و حمله به اطلاعات تقسیم‌بندی می‌گردد [٦]. این دسته‌بندی به‌طور کامل در شکل (۱) نشان داده شده است. در زمان حمله به مسیریابی، گره خطاکار می‌تواند اقدام به حذف بسته‌های واپایشی کرده و یا مسیرهای اشتباه را در شبکه ترویج دهد. حمله‌کننده‌ای که می‌خواهد منابع شبکه را به هدر دهد، ممکن است اقدام به ارسال درخواست‌های مکرر مسیریابی نماید. همچنین می‌تواند بسته‌های خاصی را در شبکه حذف کند تا در اثر آن، گره‌های همسایه به‌طور مرتب اقدام به مسیریابی نمایند.

از طرف دیگر، تهدیدها و حملات موجود در شبکه‌های محلی بی‌سیم مبتنی بر استاندارد IEEE802.11 به دو دسته فعال و غیرفعال تقسیم می‌گردند [١٤]. در حملات غیرفعال، نفوذگر به نحوی به منابع اطلاعاتی دست می‌یابد، ولی محتوای اطلاعات منبع را تغییر نمی‌دهد. این نوع حملات می توانند به یکی از شکل‌ها شنود ساده یا تحلیل ترافیک باشد [١٤]. در حملات فعال، برخلاف حملات غیرفعال، نفوذگر، اطلاعات مورد نظر را که از منابع به‌دست می‌آورد، به‌طور غیر مجاز تغییر

1- Support Vector Machine

2- Watchdog
3- Path Rater



شکل ۱. دسته‌بندی حملات با هدف از کار اندازی کل شبکه

می‌دهد. از آن‌جا که در این نوع حملات اطلاعات تغییر می‌کند شناسایی رخداد حملات، فرایندی امکان‌پذیر است. این حملات به چهار دستهٔ تغییر هویت، پاسخ‌های جعلی، تغییر پیام و حمله‌های منع سرویس[1] تقسیم می‌گردند. در حملاتی از نوع منع سرویس، نفوذگر یا حمله‌کننده برای تغییر نحوه کارکرد یا مدیریت یک سامانه ارتباطی یا اطلاعاتی اقدام می‌کند. ساده‌ترین نمونه، سعی در از کار انداختن نرم‌افزاری و سخت‌افزاری سامانه‌ها می‌باشد. پیرو چنین حملاتی، نفوذگر می‌تواند با از کار انداختن یک سامانه، اقدام به سرقت، تغییر یا نفوذ به منبع اطلاعاتی نماید. در برخی از حالات، در پی حمله انجام شده، سرویس مورد نظر به‌طور کامل قطع نشده و تنها کارایی آن مختل می‌گردد.

در این مقاله قصد داریم گونه‌ای از حمله به هدر دادن منابع را مورد بررسی قرار دهیم. این حمله که جزء حملات فعال محسوب می‌گردد، با ارسال بیش از حد تقاضای مسیریابی، در صدد به هدر دادن منابع گره‌های دیگر و در نهایت به خطر انداختن دسترس‌پذیری گره ها می‌باشد. ابتدا با در نظر گرفتن توپولوژی متغیر در ارتباطات و روابط قابل اعتماد در می‌یابیم که آیا می‌شود به یک گره اعتماد کرد؟ دوم اینکه ما باید عدم زیر ساخت در شبکه‌های اقتضایی را مد نظر داشته باشیم: هر طرح متمرکز ممکن است با مشکلاتی در آرایش و قرارگیری گره‌ها مواجه باشد. گروهی برای جلوگیری از دخالت و خرابکاری گره‌های دیگر، از ساختار کلید عمومی، برای طراحی مسیریابی‌های امن، استفاده می‌کنند؛ اما این روش بسیار گران تمام می‌شود[۵]. رویکرد دیگر، استفاده از سیستم‌های تشخیص نفوذ می‌باشد که هدف آن، تجهیز گره‌های موجود درشبکه جهت شناسایی و مقابله با رفتارهای بدخواهانه بدون تغییر در پروتکل‌های مسیریابی یا زیرساخت مورد استفاده می‌باشد. مقصود از نفوذ، هر مجموعه‌ای از کارهایی است که در صدد به مخاطره انداختن تمامیت، محرمانگی یا در دسترس بودن منابع اطلاعاتی می‌باشد [۱۵]. تکنیک‌های جلوگیری از حملات به‌عنوان اولین خط دفاع محسوب می‌شوند. از آنجا که جلوگیری از حملات به تنهایی جهت برقراری امنیت کافی نمی‌باشد، سیستم‌های تشخیص نفوذ می‌توانند به‌عنوان دومین خط دفاع در نظر گرفته شوند [۷]. به محض تشخیص یک حمله در مراحل اولیه، تمهیدات لازم جهت کاهش اثر حمله صورت خواهد گرفت. سیستم‌های تشخیص نفوذ را می‌توان از نظر نوع اطلاعاتی که مورد استفاده قرار می‌دهد به دو دسته مبتنی بر شبکه[2] و مبتنی بر میزبان[3] تقسیم کرد. یک IDS وقتی مبتنی بر شبکه خوانده می‌شود که بتواند ترافیک شبکه‌ای که بر روی آن قرار دارد را مورد بررسی

1- Denial of Service ≡ DoS

2- Network Based
3- Host Based

قرار دهد. مسلماً این رویکرد برای شبکه‌های اقتضایی مناسب نمی‌باشد. زیرا هیچ نقطه مرکزی برای جمع آوری اطلاعات درشبکه‌های اقتضایی وجود ندارد. یک IDS مبتنی بر میزبان با جمع‌آوری و تجزیه و تحلیل اطلاعات در هر گره، از فعالیت‌های غیر معمول و یا حملات انجام گرفته به میزبان مطلع می‌گردد. در این نوع IDS از نتایج تحلیل، برای دو منظور امن کردن فعالیت‌های گره مذکور و نیز آگاهی دادن به گره‌های دیگر از وجود گره حمله‌کننده استفاده می‌شود.

در بخش بعد یک سامانه تشخیص نفوذ مبتنی بر میزبان در شبکه‌های اقتضایی برای کنترل حملهٔ منع سرویس در شبکه معرفی خواهد شد.

۳. طراحی سامانه تشخیص نفوذ

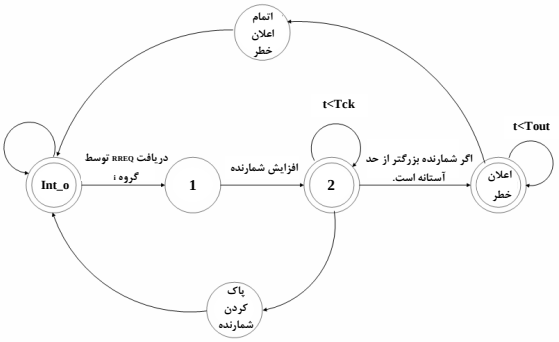
سامانه تشخیص نفوذ ارائه شده، به منظور تشخیص حملات در شبکه‌های بی‌سیم اقتضایی و بخصوص در هنگام استفاده از مسیریابی DSR[1] طراحی شده است [۱۶]. با این حال با اعمال تغییرات اندک این سیستم در همه پروتکل‌های مسیریابی بنا به درخواست از جمله AODV[2] قابل پیاده‌سازی می‌باشد. این سیستم در حقیقت با گوش سپردن به ترافیک ورودی به گره و بررسی آن می تواند وجود حمله را در شبکه تشخیص داده و در صدد مقابله با آن برآید. از آنجا که سامانه برای تشخیص حمله نیازمند ارسال هیچ گونه داده‌ای نمی‌باشد، منجر به اعمال هیچ‌گونه سرباری به شبکه نخواهد شد و هیچ ظرفیت ارتباطی اضافی را به خود اختصاص نخواهد داد. به‌علاوه از آنجا که این سامانه هیچگونه عملیات رمزنگاری را برای محافظت در برابر گره‌های بدخواه اعمال نمی‌دارد، بنابراین سربار محاسباتی خاصی را نیز به گره‌ها اعمال نخواهد کرد. از آنجا که واحد تشخیص نفوذ بر روی همه گره‌های شبکه نصب می‌گردد سامانه مزبور، یک سامانه کاملاً توزیع شده می‌باشد که در آن گره ها مستقلاً حملات را تشخیص داده و به مقابله با آن می‌پردازند. از طرف دیگر این سامانه برای تشخیص حملات شناخته شده طراحی شده است.

عملکرد سامانه بدین صورت است که واحد شنود، اطلاعات ترافیکی ورودی به گره را مورد بررسی قرار داده و مشخص می‌کند که چه بسته‌هایی نیاز به بررسی بیشتر دارند. واحد شنود، اطلاعات مشکوک را به واحد ثبت رخداد تحویل می‌دهد. وظیفه واحد ثبت رخداد، تهیه اطلاعات مورد نیاز واحد تشخیص حمله می‌باشد. در حقیقت، واحد ثبت رخداد، تعداد انحرافات گره‌های همسایه از عملکرد عادی را جمع‌آوری می‌کند و واحد تشخیص حمله با استفاده از این اطلاعات نوع حمله را تشخیص داده و به واحد مقابله با حمله اعلام می‌کند. در پایان واحد مقابله با حمله، تمهیدات لازم جهت کاهش اثر حمله و مقابله با آن را اتخاذ می‌نماید. در حقیقت، هدف اصلی ما ارائه یک سامانه تشخیص نفوذ برای شبکه‌های اقتضایی بی‌سیم می‌باشد، به نحوی که به محض تشخیص حمله، گره تشخیص دهنده باید واکنش مناسبی را برای مقابله با گره حمله کننده و حفظ کارایی شبکه در حد قابل قبول، اتخاذ نماید. در اینجا مشخص می‌شود که آیا گره همسایه همان گره حمله‌کننده است یا نه. البته به‌خاطر رفتارهای متفاوت شبکه‌های اقتضایی ممکن است در برخی موارد به اشتباه گره‌ای به‌عنوان گره خطاکار شناسایی شود. مثلاً در شرایطی که یک گره از نظر جغرافیای در جایی قرار گرفته باشد که تنها واسط بین دو گروه از گره‌های کنار هم باشد، ممکن است تعداد زیادی بستهٔ RREQ ارسال کند، یا در شرایط خاصی مجبور به برقراری ارتباط با گره‌های متعددی باشد. در این صورت اگر سیستم این گره را به‌عنوان گره خاطی از شبکه طرد کند، یک خطای بزرگ رخ داده است. برای کم کردن اینگونه خطاها، سیستم به گونه‌ای طراحی شده است که گره خاطی را برای یک مدت زمان محدود قابل تنظیم ـ مثلاً یک دقیقه ـ از شبکه طرد می‌کند.

شکل (۲)، نمودار ماشین حالت زمان‌دار سامانه تشخیص حمله را نشان می‌دهد. آنچنانکه مشاهده می‌گردد، هر زمان که یک پیام RREQ از یکی از گره‌های همسایه دریافت شود، ماشین حالت راه اندازی می‌شود، گره مشاهده‌کننده، لیستی از تمامی کسانی که اخیراً پیام RREQ فرستاده‌اند را تهیه کرده و به‌وسیله یک شمارنده تعداد بسته‌های RREQ ارسالی توسط هر گره را محاسبه می‌نماید. همچنین علاوه بر تهیه لیست و شمارش تعداد تقاضا، به یک زمان‌سنج نیز نیاز می‌باشد. وظیفهٔ این زمان‌سنج تعیین مدت زمانی است که در آن مدت زمان، تعداد بسته‌های RREQ ارسالی هرگره نباید از یک حد آستانه بیشتر گردد. برای مثال در شبکه‌ای، IDS ها به گونه‌ای تنظیم شده‌اند که در صورتی که تعداد RREQ های ارسالی توسط یک گره طی مدت زمان یک ثانیه بیش از ۱۰ بسته باشد، آن گره

1- Dynamic Source Routing
2- Ad Hoc On-Demand Distance Vector

به‌عنوان گره خاطی در نظر گرفته خواهد شد و در غیر این صورت حمله تشخیص داده نمی‌شود.



شکل ۲. نمودار ماشین حالت سامانه تشخیص نفوذ

همان‌گونه که در شکل (۲) نشان داده شده است، ماشین حالت با دریافت هر بسته RREQ، شمارنده مربوط به گره فرستنده پیام را یک واحد افزایش می‌دهد. و تا زمانی که دوره تناوب به پایان نرسیده است (t< Tck) ماشین حالت در مرحله ۲ باقی خواهد ماند و همچنین در صورت دریافت RREQ، شمارنده مربوط به گره فرستنده افزایش می‌یابد. پس از پایان یافتن وقت زمان‌سنج، مقدار شمارنده‌های مربوط به گره‌های مختلف محاسبه می‌شود و در صورتی که هر یک از این مقادیر از یک حد آستانه قابل تنظیم بزرگ‌تر باشد گره فرستنده این RREQها، به‌عنوان گره خاطی در نظر گرفته می‌شود. در این صورت ماشین حالت به وضعیت اعلام خطر رفته و به مدت Tout از گره خاطی هیچ پیامی پذیرفته نمی‌شود. پس از گذشت زمان Tout، خطای گره خاطی بخشیده شده و به آن گره اجازه داده می‌شود که دوباره به شبکه بپیوندد.

۴. شبیه‌سازی و ارزیابی عملکرد

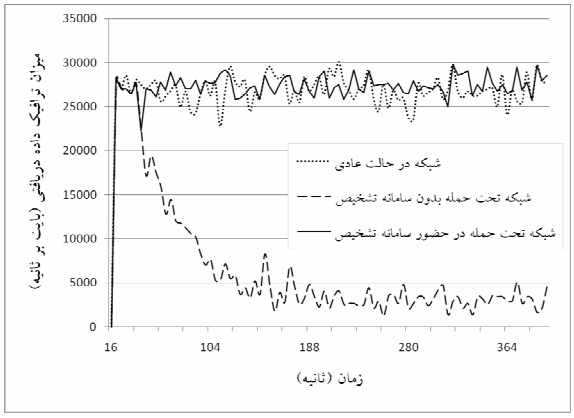
برای شبیه‌سازی و پیاده‌سازی سامانه تشخیص نفوذ پیشنهادی، از نرم‌افزار OPNET که یکی از ابزارهای شبیه‌سازی شبکه است، استفاده گردید. نسخه ۱۰ نرم‌افزار OPNET پروتکل مسیریابی DSR را برای استفاده در شبکه‌های اقتضایی فراهم می‌آورد. پارامترهای شبیه‌سازی در جدول (۱) بیان شده است.

همان‌گونه که ملاحظه می‌گردد، در یک فضا به مساحت ۲۰۰۰ متر مربع، تعداد ۳۰ گره در نظر گرفته شده است که هر کدام ترافیکی در حدود ۱۰۲۴ بایت بر ثانیه را به شبکه اعمال می‌کنند. در ادامه، میزان ترافیک دریافتی در حالات مختلف شبکه را در وضعیتی که ترافیک ارسالی آنها در هر سه حالت با هم برابر و معادل ۲۸ کیلو بایت بر ثانیه می‌باشد را در یک نمودار با هم مقایسه می‌کنیم. شکل (۳)، میزان ترافیک دادهٔ دریافتی در شرایط مختلف شبکه را با هم مقایسه می‌کند. این شکل به خوبی تاثیر وجود سامانه تشخیص نفوذ در شبکه را نشان می‌دهد. نموداری که در بالای همه قرار گرفته است، عملکرد شبکه را در حالت عادی نشان می‌دهد. نموداری که در پایین‌ترین وضعیت قرار دارد، عملکرد شبکه را در زمان حمله نشان می‌دهد و البته در این حالت گره‌های شبکه، مجهز به سامانه تشخیص نفوذ نمی‌باشند و نمودار بالا بیانگر عملکرد سامانه تشخیص نفوذ می‌باشد.

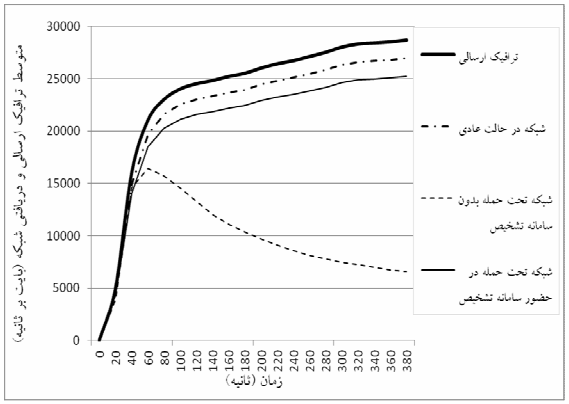
جدول ۱. پارامترهای شبیه‌سازی

شبیه‌ساز	OPNET_v10
مدت زمان شبیه‌سازی	۴۰۰ ثانیه
مساحت فضای پیاده‌سازی	۲۰۰۰ × ۲۰۰۰ متر
تعداد گره‌ها	۳۰
برد رادیویی	۴۰۰ متر
نوع ترافیک	CBR (UDP)
حجم اطلاعات هر بسته	۵۱۲ بایت
نرخ ارسال	۲ بسته در ثانیه
تعداد گره‌های مخرب	۱

شکل (۴)، مقادیر متوسط نمودارهای ترسیم شده در شکل (۳) را نشان می‌دهد. نمودار مشکی رنگ که در بالای همه قرار دارد، مقدار متوسط اطلاعات ارسالی را نشان می‌دهد. نمودار آبی رنگ مقدار متوسط اطلاعات دریافتی درحالت عادی شبکه را نشان داده و نمودارها به ترتیب داده‌های دریافتی در وضعیت استفاده از سامانه تشخیص نفوذ و شبکه تحت حمله را نشان می‌دهند. با استفاده از این شکل در نهایت مشاهده می‌شود که بازده شبکه در شرایط عادی در حدود ۹۴٪، در شرایط حمله حدود ۱۶٪ و در شرایطی که سامانه تشخیص نفوذ وجود دارد معادل ۸۸٪ می‌باشد. در نتیجه سامانه تشخیص نفوذ پیشنهادی ما، به میزان ۷۲٪ موجب افزایش کارآیی شبکه در زمان حمله شده است.



شکل ۳. مقایسه میزان ترافیک داده دریافتی در شرایط مختلف شبکه



شکل ۴. متوسط ترافیک‌های ارسالی و دریافتی شبکه در حالات مختلف

۵. نتیجه‌گیری و پیشنهادها

همان‌گونه که از نتایج ارزیابی مشاهده می‌گردد، سامانه تشخیص نفوذ پیشنهادی موجب افزایش عملکرد چشمگیری در زمان وقوع حمله می‌شود. نتایج بدست آمده در این ارزیابی، تصدیقی بر نتایج حاصل از سامانه تشخیص نفوذ RIDAN در [۵] می‌باشد. سامانه تشخیص RIDAN نیز با روشی مشابه ـ البته در مسیریابی AODV ـ گره خرابکاری را که اقدام به ارسال مکرر RREQ می‌کند، شناسایی و طرد می‌نماید. سناریو و نتایج روش پیشنهادی ما دو مزیت نسبت به [۵] دارد: نخست اینکه، کارایی عادی سیستم در سناریوی شبیه‌سازی شده در [۵] نیز در حدود ۹۴٪ است، اما حمله‌ای که در آنجا پیاده‌سازی شده است، کارایی سیستم را فقط تا حد ۵۰٪ کاهش می‌دهد. این در حالی است که حمله پیاده‌سازی شده در روش پیشنهادی قوی‌تر است، به‌طوری که عملکرد شبکه را به حدود ۱۶٪ می‌رساند. دوم اینکه گره‌های مجهز به سامانه تشخیص نفوذ RIDAN، با شناسایی گره مخرب، کارایی شبکه را به ۷۸٪ می‌رساند، و این در حالی است که سامانه تشخیص نفوذ کارایی شبکه تحت حمله را از ۱۶٪ به ۸۸٪ می‌رساند.

با وجود عملکرد خوب سامانه تشخیص نفوذ پیشنهادی، این سامانه توانایی شناخت همه حملات را ندارد. از این رو در جهت تکمیل این سامانه تشخیص نفوذ، به‌کارگیری یک سامانه کامل‌تر که در حقیقت یک سامانه تشخیص نفوذ ترکیبی می‌باشد، پیشنهاد می‌گردد. به عبارت دیگر این سامانه با شنود ترافیک شبکه در بخش *پایش* خود، با توجه به عملکرد گره‌ها به هر گره یک امتیاز خواهد داد، تعیین افزایش یا کاهش امتیاز گره توسط الگوریتم‌های ویژه‌ای در بخش تشخیص خطا صورت می‌گیرد.

۶. مراجع

[1] Gaviani, S. “Detecting Packet-Dropping Faults in Mobile Ad-Hoc Networks”; Washington State University, 2004.

[2] Corson, M.; Ephremides, A. "A Distributed Routing Algorithm for Mobile Radio Networks"; in Proceedings of Military Communication Conference, 1989.

[3] Borg , J. “A Comparative Study of Ad Hoc & Peer to Peer Networks”; University College, London, 2003.

[4] Ramanathan, R.; Redi, J. “A Brief Overview of Ad Hoc Networks: Challenges and Directions”; IEEE Communications, no. 50th Anniversary Commemorative Issue, 2002; pp 20-22.

[5] Stamouli, Ioanna “Real-time Intrusion Detection for Ad Hoc Networks”; University of Dublin, 2003.

[6] Patwardhan, A.; Parker, J.; Joshi, A. “Secure Routing and Intrusion Detection in Ad Hoc Networks”; University Of Maryland, 2003.

[7] Zhang, Y.; Lee, W. “Intrusion Detection on Wireless Ad Hoc Networks”; in Proceedings 6th Annual International Conference on Mobile Computing and Networking (MobiCom’00), 2000.

[8] Anjum, F.; Subhadrabandhu, D.; Sarkar, S. “Signature-based Intrusion Detection for Wireless Ad-Hoc Networks"; In Proceedings of Vehicular Technology Conference, Wireless Security Symposium, Orlando, Florida, 2003.

[9] Deng,, H.; Zeng,, Q. A.; Agrawal, D. P. “SVM-Based Intrusion Detection System for Wireless Ad Hoc Networks.”; In Proceedings of the IEEE Vehicular Technology Conference, 2003.

[10] Brutch, P.; Ko, C. “Challenges in Intrusion Detection for Wireless Ad Hoc Networks.”; Proceedings of the Workshop on Security and Assurance in Ad-hoc Networks in Orlando, 2003.

[11] Tseng, C. Y.; Balasubramanyam, P.; Ko, C.; Limprasittiporn, R.; Rowe, J.; Levitt, K. “A Specification based Intrusion Detection System for AODV”; In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003, pp. 125–134. ACM Press,.

[12] Wang, B.; Soltani, S.; Shapiro, Jonathan K.; Tan, P. N. “Local Detection of Selfish Routing Behavior in Ad Hoc Networks”; Department of Computer Science and Engineering, Michigan State University, 2004.

[13] Marti, S.; Giuli, T. J.; Lai, K.; Baker M. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks."; In Proceedings MobiCom 2000, pp. 255–265.

[14] http://www. ircert. com/articles/ IRCAR-251104. htm

[15] Heady, R.; Luger, G.; Maccade, A.; Servilla, M. “The Architecture of a Network Level Intrusion Detection System”; Technical Report, Computer Science Department, University of New Mexico, 1990.

[16] Johnson, D.; Hu, Y. “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for IPv4”; The IETF Trust, 2007.