مدلی ترکیبی برای کاهش هشدارهای نادرست در سیستم های تشخیص نفوذ

زهره باطنی [۱]، الهه میرکریمی [۲]

[۱] عضو هیئت علمی-گروه کامپیوتر، دانشگاه علم و فرهنگ
bateni@usc.ac.ir

[۲] کارشناس ارشد-گروه کامپیوتر، دانشگاه علم و فرهنگ

چکیده

در دو دهه اخیر، سیستم‌های تشخیص نفوذ به عنوان اجزاء اصلی برای افزایش امنیت در شبکه‌های کامپیوتری مطرح شدند. یکی از مشکلات اساسی سیستمهای تشخیص نفوذ تولید حجم زیادی از هشدارها است، که ممکن است بیش از ۹۹ درصد آنها نادرست باشند. هنر مدیریت سیستم های تشخیص نفوذ استفاده از روش‌هایی به منظور کاهش FPها است، بدون اینکه مانع تشخیص حملات واقعی به سازمان شوند.

در این مقاله راه کاری برای کاهش حجم وسیع هشدارهای نادرست و حذف هشدارهای تکراری ارائه گردیده. روش پیشنهادی از ترکیب سه نظریه زیر جهت کاهش هشدارهای نادرست استفاده می‌کند. هشدارهای درست معمولاً دسته‌ای از هشدارها می‌باشند که دارای آدرس‌های IP یکسانی هستند. امضاهای مربوط به هشدارهای درست در مقایسه با میانگین امضاها، دارای فرکانس بالاتری می‌باشد. تعداد هشدارهای همسایه برای هشدارهای درست به طور قابل ملاحظه ای بیشتر از تعداد همسایه ها برای هشدارهای نادرست می باشد. سیستم پیشنهادی توسط مجموعه داده DARPA1999 مورد ارزیابی قرار گرفته است. نتایج نشان داده است که سیستم پیشنهادی با نرخ کاهش هشدار ۸۶.۴٪، نرخ کاهش هشدار نادرست ۸۵.۹٪ و کاهش ۱۰۰ درصدی هشدارهای تکراری می‌تواند تأثیر به سزایی در مدیریت هشدارها داشته باشد.

کلمات کلیدی

امنیت، سیستم تشخیص نفوذ، کاهش هشدار، اسنورت.

۱- مقدمه

یکی از نکات مهم در شبکه کامپیوتری، تضمین امنیت شبکه است. امنیت در شبکه برای دستیابی به سه عامل مهم محرمانگی(Confidentiality)، یکپارچگی(Integrity) و دسترس پذیری(Availability (CIA) در محیطهای نگهداری و تبادل اطلاعات است. در شبکه‌های کامپیوتری به دلیل دسترسی از راه دور و حجم زیاد اطلاعات مهم و محرمانه، مشکل نفوذ به سیستم‌های کامپیوتری مطرح می شود. پس از پیشگیری از نفوذ به سیستم در هنگام ساخت سیستم های کامپیوتری، توجه به سیستم های تشخیص نفوذ انجام می شود.

چون اصول و روش های حملات دائماً در حال تغییر است [۱] ، طراحی سیستم های تشخیص نفوذ مهم اند. دو مفهوم اساسی امنیت در شبکه حفاظت(Protection) و نظارت(Supervision) می باشد [۲] . امنیت در سه مورد، امنیت کامپیوترها، شبکه‌های کامپیوتری و اطلاعات بررسی می شود. . در این مقاله دو مورد اول بررسی می شود. روش های مختلفی برای مقابله با حملات وجود دارد. معمولا جهت مقابله با نفوذ در سیستم راهکارهای پیشگیری (Prevention)، پیش‌دستی

(Preemption)، بـازداری(Deterrence)، انحـراف(Deflection)، تشخیص (Detection) و مقابلـه (Countermeasure) ارائـه شـده است.

سیسـتم‌هـای تشـخیص نفـوذ (Intrusion Detection System (IDS)) با نظارت بر وقایع رخ داده و تحلیل آن‌ها، به دنبال کشف موارد انحراف از سیاست‌های امنیتی و اعلان خطر می‌باشد [۳].

هر ساله میزان نفوذ به شبکه های کامپیوتری افزایش می‌یابـد. بنـابراین سیستم‌های تشخیص نفوذ به منظور افزایش امنیت لازم است [۴] ، کـه ۶۹ درصد سازمان‌ها از سیستم های تشخیص نفـوذ بـه عنـوان عناصـر امنیتی خود استفاده می‌کنند[۵]. سیستم های تشخیص نفوذ در صـورت تشخیص نفوذ، هشداری تولید کرده و به مدیر شـبکه ارسـال مـی‌کننـد. بیشتر هشدارهای تولید شده توسط سیستم های تشخیص نفوذ مربوط به مشکلات امنیتی نیستند و برای مدیریت سیاست‌ها مناسب می‌باشند[۶]. علت به وجود آمدن این نوع هشدارها ممکن است به توپولـوژی شـبکه، پیکربندی اشتباه میزبان و غیره، مربوط شود[۷].

مشکل اصلی در سیستم های تشخیص نفوذ ، تولید هـزاران هشـدار در روز می‌باشد که ممکن است ۹۹٪ آن‌ها، هشـدارهای نادرسـت(False alarm) باشند[۸ ، ۹]. پس تشخیص آنکه کدام هشدار درسـت و کـدام هشدار نادرست می‌باشد، مهم است. مدیریت سیستم های تشخیص نفوذ استفاده از روش‌هایی به منظور کاهش هشدارهای نادرست است، بـدون اینکه مانع تشخیص حملات واقعی به سازمان شوند.[۱۰].

۲- تعاریف و مفاهیم

تهدید امنیتی در شبکه های کامپیوتری، هر وضعیت یا اتفاقی است کـه قابلیت ضرر زدن به سیستم را داشته باشد. این ضرر می‌تواند به صورت انکـار، افشاء، خرابی یا تغییر داده‌ها و منابع سیستم باشد[۳]. نقطه ضعف‌های شبکه و پروتکل‌ها یا آسیب پذیری در سیستم عامل باعث ظهور تهدید می شود.

یک نمونه از تهدید آنکه در زمان انتقال بسته، بین عناصر شبکه ممکـن است تداخل بین بسته‌ها به وجود بیاید و محتوای آن‌هـا تغییـر کنـد، از قبیـل حمله شماره ترتیب (initial sequence number attack) عددی صحیح که به هر بسته انتقال یافته نسبت داده می‌شود. در حملـه، مهـاجم آدرس IP ارسال شده به سرور را بدست می‌آورد. سرور تأییدی را به یک سرویس گیرنده کلاه‌بردار صادر می‌کند[۳]. درضمن تهدیدات امنیتی داخلی ماننـد اعتمـاد بـه کاربران مجاز و کارمندان که فعالیت‌های ناصحیح انجـام مـی دهنـد. اشـتباه مدیران که امنیت سازمان را به خطر می‌اندازد غفلت از قفل کردن درب هـای پشتی(back door) ، رمزگذاری داده‌ها حساس در نوتبوک هایشان یا حـذف نکردن امتیازات دسترسی کاربران که سازمان را ترک کـرده‌انـد، هـم تهدیـد می‌باشد [۳].

انواع حملات از یک نگاه به دو دسته فعال و غیر فعال تقسیم می‌شوند و از جنبه دیگر بر اساس عامل این حملات به چهار دسته کلی تقسیم می شوند. شامل:[۱۱] Probe (مهاجم در پی شناسایی شبکه و جمع آوری اطلاعـات از وضعیت شبکه می‌باشد. که حمله محسوب نمی‌شود بلکه پیش زمینه حمـلات بعدی می‌باشد.) Denial of service (DOS) (مهاجمان دسترسی کاربران قانونی به سرور را قطع می کنند.) User to Root (U2R) (مهـاجم کلمـه رمز عبور کاربران قانونی شبکه را می یابد.) و Remote to Local (R2L) (مهاجم با استفاده از نقاط آسیب پذیر سیستم، کنترل یک ماشین خارجی را از طریق شبکه به عنوان یک کاربر محلی بدست می آورد.)

سیستم های تشخیص نفوذ مطابق با داده هایی که برای تشخیص نفوذ استفاده می‌کنند به دو دسته سیستم مبتنی بر شبـکه (Network-based Intrusion Detection System-NIDS)و سیستم مبتنی بر میزبان ((HIDS Host-based IDS))طبقه بندی می‌شوند [۶]. NIDSها می‌توانند شبکه را به وسیله نظارت و تحلیل ترافیک شبکه کنترل کنند، در حالی که HIDSها فایل‌های ثبت رویداد و فراخوان‌های سیستمی مربوط به یک میزبان خاص را بررسی می‌کنند. سیستم های تشخیص نفوذ همچنین مطابق با منطقی که برای تشخیص نفوذ در این داده‌ها استفاده می‌کنند به چهار دسته مبتنی بر امضا (Signature-based IDS-SIDS) ، مبتنی بر ناهنجاری (Anomaly-based IDS (AIDS)) ، مبتنی بر تحلیل حالت پروتکل و ترکیبی طبقه بندی می‌شوند[۱۲]. در SIDSها الگوهایی از حملات خاص استخراج شده و این الگوها با داده‌های مورد بررسی مقایسه می‌شوند. در صورت مطابق بودن الگو با داده‌های مورد نظر، هشداری مرتبط با حمله شناسایی شده تولید می‌شود. AIDSها الگویی را به عنوان رفتار نرمال سیستم در نظر گرفته و سعی می‌کنند هر گونه انحرافی از این الگو را شناسایی کرده و هشدار مناسبی که نشان دهنده نفوذ یا انحراف شناسایی شده است، را تولید کنند. تفاوت اصلی این دو روش در مفاهیم حمله و ناهنجاری است[۱۳]. یک حمله می‌تواند توالی از عملیاتی که امنیت سیستم را با ریسک مواجه می‌کند، تعریف شود، در حالی که یک ناهنجاری فقط یک رویداد مشکوک امنیتی را بیان می‌کند.

۳- انواع روش‌های تشخیص نفوذ

چهار روش مهم سیستم های تشخیص نفوذ، جهت تشخیص حملات خارجی و یا سوءاستفاده ی کاربران داخلی: روش‌های مبتنی بر امضا، مبتنی بر ناهنجاری، مبتنی بر تحلیل حالت پروتکل و روش ترکیبی است. تنها تفاوت آن‌ها در نحوه پردازش اطلاعات جمع آوری شده از محیط‌های مورد نظارت می‌باشد. هر سیستم تشخیص نفوذ از چهار بلاک عملیاتی تشکیل می‌شود. بلاک مربوط به رخداد، تمام رویدادهای اتفاق افتاده در محیط مورد نظارت را جمع آوری می‌کند و در پایگاه داده قرار می‌دهد. سپس بلاک مربوط به تحلیل رویدادها را پردازش کرده و در صورت لزوم هشداری را تولید و به بلاک بعدی ارسال می‌کند. نهایتاً بلاک پاسخ رویداد تهاجمی را مشخص کرده و آن را متوقف می‌کند[۱۴].

تشخیص مبتنی بر امضا ((Signature Detection (SD))، فرآیند مقایسه الگوها با رویدادهای بدست آمده از نفوذهای ممکن سیستم است. سیستم های تشخیص نفوذ مبتنی بر امضا معمولاً بر اساس قوانین نوشته شده توسط کارشناسان می‌باشند.[۱۲]. سیستم‌های تشخیص مبتنی بر امضا می‌توانند به راحتی توسط مهاجمان نقض شوند، به این صورت که مهاجمان حملات شناخته را تغییر می‌دهند و یا سیستم‌های هدف را که به وسیله امضاهای جدید بروزرسانی نمی‌شوند را استفاده می‌کند[۱۴]. در دنیای نرم افزارها تشخیص مبتنی بر امضا رایج‌تر از دیگر روش‌ها می‌باشد، زیرا نرخ هشدارهای نادرست نسبتاً کمتر می‌باشد[۶].

تشخیص نفـوذ مبتنـی بـر ناهنجاری(رفتـار غیرعـادی) (Anomaly Detection (AD) یک ناهنجاری یعنی انحراف از رفتـار شـناخته شـده و

مستندات ارائه شده از رفتار نرمال و مورد انتظار است، که از نظارت روی فعالیت‌های سیستم، اتصالات شبکه که طی دوره‌های زمانی از میزبان، کاربران و شبکه بدست می‌آید، استنتاج می‌شود. زمانی که سیستم‌ها در محیط‌های مورد نظارت هیچ گونه بروز رسانی نداشته باشند، تشخیص نفوذ مبتنی بر ناهنجاری(AD)) می‌تواند حملات جدید یا به عبارتی حملات صفر روزه را شناسایی کند. ADها از سه تکنیک تشخیص ناهنجاری آماری، دانش/داده کاوی و بر اساس یادگیری ماشین برای تشخیص ناهنجاری‌ها استفاده می‌کنند [۱۴].

تشخیص نفوذ مبتنی بر تحلیل حالت پروتکل:

(Statefull Protocol Analysis (SPA)) نشان می‌دهد که سیستم تشخیص نفوذ می‌تواند از حالت پروتکل آگاه باشد و آن را ردیابی کند. به نظر می‌رسد که فرآیند SPA شبیه به ADها می‌باشد، اما آن‌ها کاملاً متفاوت از یکدیگر هستند. ADها توصیف‌های مختصری از شبکه یا میزبان خاصی را بارگذاری می‌کنند، در حالیکه SPA مربوط به تولید تاریخچه یا توصیف‌های مختصر برای پروتکلی خاص است [۶].

روش‌های تشخیص نفوذ از طریق ویژگی‌ها به پنج زیر کلاس مبتنی بر آمار، مبتنی بر الگو، مبتنی بر قانون، مبتنی بر حالت و مبتنی بر بحث اکتشافی دسته بندی می‌شوند[۶].

تشخیص نفوذ ترکیبی (Hybrid) دو یا تعداد بیشتری از روشها را ترکیب می‌کند. نتایج تولید شده توسط این روش برتری‌هایی را نسبت به روش‌های دیگر دارد، زیرا از مزایای هر یک از روش‌ها بهره می‌گیرد. برای نمونه در اسنورت[۱۵] دو موتور مبتنی بر ناهنجاری و امضا اضافه شد و نتایج آن با استفاده از داده‌های یکسان با اسنورت معمولی مورد ارزیابی قرار گرفت، در نهایت نشان داد که روش ترکیبی نتایج بهتری را تولید خواهد کرد. به عبارت دیگر بیشتر نفوذهای مربوط به میزبان و یا شبکه را شناسایی می کند.

٤- پیشینه تحقیق

در اکثر مقالات از تکنیک خوشه بندی جهت کاهش هشدارها استفاده می‌شود. روش‌هایی که از این تکنیک استفاده می‌کنند، معمولاً هشدارها را در خوشه‌های مختلف قرار می‌دهند و برای هر خوشه یک هشدار اصلی(Master Alarm) تولید می‌کنند، که این هشدار به عنوان نماینده‌ای برای تمام هشدارهای موجود در خوشه استفاده می‌شود. برای نمونه در مرجع [۱۶] از ترکیب دو تکنیک طبقه بندی و خوشه بندی جهت کاهش هشدارها استفاده می شود. در مرجع [۱۷] دلایل تولید هشدارهای نادرست بررسی می شود. بسیاری از این دلایل مربوط به حملات نمی‌باشند، اما سیستم تشخیص نفوذ را مجبور به تولید هشدارهایی می‌کنند که دارای ویژگی‌های مشابهی هستند. در مرجع [۱۸] کاهش هشدارها در دو سطح حسگر و سطح بعد از تشخیص نفوذ، گروه بندی می شود. درمرجع [۱۹] از الگوهای حملات به منظور طبقه بندی و کاهش هشدارهای تکراری استفاده کردند.

همانگونه که قبلا ذکر شد، سیستم های تشخیص نفوذ می تواند مبتنی بر امضا یا مبتنی بر ناهنجاری باشد. معمولا روش مبتنی بر امضا تعداد هشدارهای نادرست تولید بسیار زیاد است. علاوه بر این ساخت مدلی که تمام ترافیک نرمال ممکن را ارائه دهد مشکل است[۶].

مرجع [۲۰] یک سیستم تشخیص نفوذ ترکیبی را ارائه کرد. این سیستم دو روش مبتنی بر امضا و مبتنی بر ناهنجاری را ترکیب کرده و از مزیت‌های هر دو بهره می‌گیرد. این سیستم علاوه بر اینکه نرخ بالایی از فعالیت‌های مخرب را تشخیص می‌دهد می‌تواند نرخ هشدارهای نادرست (False Positive Rate) را نیز کاهش دهد.

در مرجع [۲۱] سیستمی جهت کاهش هشدارها در مرحله پس پردازش (یعنی بعد از تولید هشدار) ارائه شده. این سیستم از سه مرحله‌ی آماده سازی، خوشه بندی و مجازی سازی تشکیل شده. با توجه به اینکه حملات می‌توانند طی مراحل مختلفی انجام شوند، ممکن است سیستم های تشخیص نفوذ برای هر مرحله هشداری خاص را تولید کنند. بنابراین در مرحله خوشه بندی که اصلی‌ترین مرحله این سیستم است، سعی شده هشدارهای ادغام شده را گروه بندی کند و به تعداد حملات سطح بالا خوشه ایجاد کند. نوآوری این سیستم، در این است که رویدادهای امنیتی از دست رفته یا به عبارتی رویدادهایی که هیچ هشدار مرتبطی ندارند، را نیز در نظر بگیرد.

٥-روش تحقیق

هدف اصلی این بخش ارائه روش پیشنهادی و بیان دلایل استفاده از چنین روشی جهت کاهش هشدار و نهایتاً پیاده سازی این روش می‌باشد.

برای انتخاب سودمندترین اطلاعات موجود در منابع اطلاعاتی و حذف هشدارهای کم اهمیت راه‌های مختلفی وجود دارد که یکی از این راه‌ها استفاده از روش طبقه بندی هشدارها و قرار دادن هشدارهای مشابه در گروه‌های مجزا و در واقع تولید اطلاعات مختصرتر است تا علاوه بر کاهش حجم هشدارها، هیچ یک از هشدارهای درستِ موجود در منابع اطلاعاتی کنار گذاشته نشوند.فیلتر ارائه شده در[۷] از سه مولفه استفاده و به این مولفه ها با توجه به ویژگی های آماری هر هشدار، امتیازی اختصاص می دهد. سپس امتیازات نسبت داده شده به هر هشدار با یکدیگر ترکیب شده و یک امتیاز نهایی برای هشدار مورد نظر صادر می شود (انتخاب بیشترین امتیاز به عنوان امتیاز نهایی). این امتیاز میزان درست بودن هشدار را مشخص می کند. اما در این فیلتر دو مشکل وجود دارد. یکی آنکه در تعیین امتیاز مؤلفه ها از نتایج دیگران اطلاعی ندارند، در نتیجه میزان محاسبات مورد نیاز زیاد است. علاوه برآن با توجه به اینکه بیشترین امتیاز نسبت داده شده به هشدار در نظر گرفته می شود. فرآیند انجام شده توسط دو مولفه دیگر که امتیاز کمتری را به هشدار نسبت دادند نادیده گرفته می شود.

با توجه به این که کاهش هشدارهای نادرست تنها با بهبود تکنیک‌های تشخیص نفوذ دشوار است[۹]. فیلتر ارائه شده در این مقاله داده های ورودی، هشدارهای تولید شده توسط سیستم تشخیص نفوذ اسنورت [۱۵] می باشند. به منظور دستیابی به این هشدارها از دیتاست DARPA 1999 به همراه سیستم تشخیص نفوذ اسنورت استفاده می شود. به عبارت دیگر داده‌های موجود در DARPA به همراه مجموعه‌ای از قوانین به اسنورت داده و اسنورت مجموعه ای از هشدارها را تولید می کند. سپس هشدارهای تولید شده توسط اسنورت به عنوان ورودی برای فیلتر ارائه شده استفاده می شود. در نهایت فیلتر ارائه شده مجموعه ای از امتیازات را برای هشدارهای ورودی مشخص می کند که این امتیاز میزان درست بودن هشدار را نشان می دهد.

این فیلتر عملکرد بهتری را جهت کاهش هشدار نسبت به فیلتر ارائه شده در مرجع [۲۱] با استفاده از طبقه بندی هشدارها ارائه می دهد و نشان می‌دهد که با استفاده از روش پیشنهادی و طبقه بندی هشدارها چگونه می‌توان با کمتر کردن میزان محاسبات، کاهش هشدار بهتری را نسبت به روش‌های

پیشین بدست آورد. در نتیجه عملکرد سیستم تشخیص نفوذ تا حد امکان بهبود می‌یابد.

کارایی یک سیستم تشخیص نفوذ شدیداً وابسته به ویژگی‌های انتخاب شده می‌باشد. در حالت کلی سیستم تشخیص نفوذ شامل داده‌هایی با ویژگی‌های کم اهمیت و اضافه می‌باشد [۲۲] و در اکثر کارهای قبلی برای بالا بردن کارایی و کاهش بُعد مسئله به انتخاب ویژگی‌های مهم و یا تولید ویژگی‌های جدید می‌پردازند [۱۲]. از آنجایی که با افزایش تعداد ویژگی‌ها هزینه محاسباتی یک سیستم افزایش می‌یابد، طراحی و پیاده سازی سیستم‌ها با کم‌ترین تعداد ویژگی ممکن، ضروری است. ویژگی مناسب تا حد زیادی دقت طبقه بندی را بالا برده و از پیچیدگی پردازش داده‌ها در مراحل بعدی می کاهد. با حداقل کردن اندازه ورودی می توان نرخ مصرف CPU را هم کاهش داد [۲۳].

داده‌های موجود در دیتاست مورد استفاده در این تحقیق ۵ ویژگی دارد:

۱. cid: شناسه مربوط به هر هشدار (چون دو آدرس IP منبع و مقصد نفوذ جهت بررسی هشدارهای درست نیاز می‌باشد.)

۲.signature: شناسه امضای مربوط به تهاجم اتفاق افتاده را مشخص می‌کند.

۳.timestamp: این ویژگی تاریخ و زمان وقوع تهاجم را مشخص می‌کند؛ زمان وقوع هشدارها نیاز است..

۴.source-ip: آدرس IP منبع نفوذ را نشان می‌دهد؛ به منظور متمایز ساختن هشدارهای مختلف از یکدیگر.

۵.dist-ip: آدرس IP مقصد نفوذ را نشان می‌دهد.

برای معیارهای ارزیابی دو مفهوم اصلی برای ارزیابی کارایی روش‌های تشخیص نفوذ عبارتنداز تأثیرپذیری فرآیند تشخیص و هزینه ای که انجام عملیات شامل می‌شود[۱۳] چهار وضعیت وجود دارد:[۲۳]

۱-False Positive (FP) : اگر رویداد نفوذ نباشد ولی به عنوان رویداد نفوذی معرفی شود.

۲-True Positive (TP) : اگر رویداد به درستی به عنوان نفوذ یا تهاجم شناسایی شود.

۳-False Negative (FN): اگر رویداد مهاجم باشد و لی رویداد عادی معرفی شود.

۴-True Negative (TN): اگر رویداد تحلیل شده به درستی به عنوان رویداد عادی و نرمال شناسایی شود.

پیاده سازی فیلتر ارائه شده شامل پنج مرحله می‌باشد، که عبارتند از:

۱.طبقه بندی هشدارها بر اساس ویژگی signature؛ اطلاعات هشدارها می‌توانند به وسیله امضای مربوط به حملات که هشدارها به آن‌ها اشاره می‌کنند طبقه بندی شوند. قبل از عملیات طبقه بندی به منظور کاهش بُعد اطلاعات مورد استفاده، در ابتدا اطلاعات مربوط به پنج ویژگی signature، timestamp، dest-ip، source-ip و cid برای هر هشدار استخراج می‌شود. تمام عملیات و مراحل مختلف فیلترسازی روی این اطلاعات استخراج شده اعمال می‌شوند.

۲.محاسبه امتیاز برای هر هشدار بر اساس ویژگی‌های timestamp، source-ip، dest-ip؛ با توجه به نظریه " امضاهای مربوط به هشدارهای درست در مقایسه با میانگین امضاها، دارای فرکانس بالاتری می‌باشند"، در امتیاز مربوط به هر هشدار از دو ویژگی source-ip و dest-ip استفاده می‌شود. بنابراین در صورت مساوی بودن مقادیر این دو ویژگی برای هر یک از هشدارهای موجود در هر گروه از امضاها می‌توان نتیجه گرفت که این هشدارها علاوه بر اینکه دارای آدرس‌های IP منبع و مقصد یکسانی هستند به حمله یکسانی نیز اشاره می‌کنند. اما تنها مساوی بودن مقادیر مربوط به این ویژگی‌ها کافی نیست و باید نظریه " تعداد هشدارهای همسایه برای هشدارهای درست به طور قابل ملاحظه‌ای بیشتر از تعداد همسایه‌ها برای هشدارهای نادرست می‌باشند" را در این امتیازدهی اعمال کرد. در مرجع[۷]، هشدارهای درست معمولاً هشدارهایی هستند با امضای یکسان که در فاصله زمانی کمتر از ۲ ثانیه اتفاق می‌افتند. بعلاوه با افزایش زمان از تعداد هشدارهای درست کاسته می‌شود به تعداد FPها افزوده می‌شود .

در نهایت امتیاز نسبت داده شده به هر هشدار تلفیقی از نظریه های مطرح شده می‌باشند. ذکر این نکته حائز اهمیت است که امتیازات مربوط به هر هشدار میزان درست بودن هشدار را نشان می‌دهد.

۳.بررسی امتیاز نسبت داده شده به هر هشدار و مقایسه آن با حد آستانه تعیین شده توسط کاربر: این مقادیر با یکدیگر مقایسه شده و اگر امتیاز نسبت داده شده به هر هشدار از حد آستانه تعیین شده بیشتر بود، هشدار مورد نظر به عنوان هشدار درست و در غیر این صورت به عنوان هشدار نادرست به مدیر شبکه ارائه می‌شود.

۴.حذف هشدارهای تکراری و هشدارهایی که دارای امتیاز کمتر از حد آستانه می‌باشند؛ امتیاز نسبت داده شده به هر هشدار میزان درست بودن هشدار را نشان می‌دهد. با استفاده از حد آستانه تعیین شده در فیلتر، درست یا نادرست بودن هشدارها مشخص می‌شود. بنابراین اگر حد آستانه مقدار بزرگی باشد هشدارهای زیادی به عنوان FP حذف خواهند شد، در نتیجه ممکن است هشدارهای درست نیز به عنوان FP حذف شوند. عکس این قضیه هم صادق است که اگر مقدار حد آستانه کم باشد تعداد هشدارهای حذف شده کاهش پیدا کرده و ممکن است هشدارهای FP نیز به عنوان هشدارهای درست به مدیر شبکه ارسال شوند و این روند باعث افت کارایی فیلتر خواهد شد. بنابراین با تعیین حد آستانه توسط مدیر(با توجه به حساسیت شبکه)، می توان تا حد ممکن از بروز چنین مشکلاتی جلوگیری کرد.

در این مرحله امتیازات مربوط به تک تک هشدارها بررسی شده و در صورتی که امتیاز هشدار از حد آستانه تعیین شده کمتر باشد، هشدار مورد نظر به عنوان FP حذف خواهد شد.

فیلتر ارائه شده در این پژوهش علاوه بر حذف FPها، هشدارهای تکراری را نیز حذف می کند. این فیلتر برای حذف هشدارهای تکراری از همان ویژگی‌هایی که برای امتیازدهی به هشدار استفاده می‌کند بهره می‌برد. بنابراین هشدارهایی که علاوه بر داشتن signature یکسان دارای آدرس‌های IP منبع و مقصد یکسانی هستند و فاصله زمانی کمتر از یک دقیقه دارند به عنوان هشدارهای تکراری شناسایی شده و حذف می‌شوند.

۵. ارائه نتایج در قالب فایل Excel به مدیر امنیتی شبکه: در نهایت هشدارهای باقی مانده به همراه نمودارهای تولید شده توسط فیلتر،که عملکرد فیلتر را نشان می‌دهند، به مدیر شبکه ارسال خواهند شد. با استفاده از نمودارهای ارائه شده مدیر شبکه می تواند راحتتر به انتخاب حد آستانه بپردازد. با توجه به اینکه خروجی اسنورت و ورودی فیلتر در غالب فایل اکسل بوده، فیلتر نیز نتایج خود را در غالب فایل اکسل به مدیر شبکه ارائه می‌دهد.

٦- نتایج

در این بخش نتایج بدست آمده از عملکرد فیلتر ارائه شده ارزیابی می شود. به منظور بررسی عملکرد فیلتر از جداول و نمودارهای تولید شده توسط خودِ فیلتر به همراه نرم افزار IBM SPSS Statistics (v 19) استفاده می‌شود. در مراحل طراحی و آزمایش فیلتر ارائه شده، از مجموعه داده‌های DARPA استفاده می‌شود. این مجموعه داده به منظور بهبود مجموعه داده ارائه شده در سال ۱۹۹۸ تولید گردید[۷]. این داده‌ها از طریق شبیه سازی یک شبکه واقعی که متشکل از ۴ دستگاه قربانی با سیستم عامل‌های مختلف و صدها دستگاه شبیه سازی شده دیگر در داخل و خارج از دروازه‌های مسیریاب می‌باشند، ایجاد شده‌اند.

ترافیک شبکه حاصل از این شبیه سازی (منظور همان مجموعه داده DARPA می‌باشد) به منظور تولید مجموعه هشدارها به عنوان ورودی به سیستم تشخیص نفوذ اسنورت (بصورت سیستم مبتنی بر شبکه عمل می‌کند) ارسال شده است. اسنورت مجموعه‌ای از هشدارها را تولید می‌کند که به عنوان ورودی فیلتر ارائه شده در این تحقیق استفاده می‌شوند. در ادامه به بررسی دقیق‌تر این مجموعه می‌پردازد.

در این تحقیق به منظور طراحی و ارزیابی فیلتر ارائه شده سه معیار زیر در نظر گرفته شده‌اند.

- تعداد کل هشدارهای ارائه شده توسط فیلتر و درصد کاهش این تعداد نسبت به کل هشدارهای ورودی (به فیلتر).
- تعداد FPهای انتخاب شده توسط فیلتر و درصد کاهش این تعداد نسبت به کل FPهای ورودی (به فیلتر).
- تعداد هشدارهای تکراری که توسط فیلتر انتخاب شده‌اند و درصد کاهش این تعداد هشدار نسبت به کل هشدارهای تکراری ورودی.

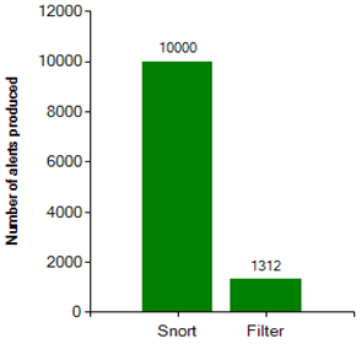
این فیلتر برای تعین بهترین تنظیمات برای مقدار حد آستانه از روش آزمون و خطا استفاده کرده و مقدار ۱ را به عنوان حد آستانه پیش فرض در نظر گرفته است (این مقدار با توجه به نظر کاربر قابل تغییر می‌باشد). عملکرد فیلتر با استفاده از محاسبه تعداد کل هشدارهای انتخاب شده توسط فیلتر، تعداد و درصد کاهش FPها و هشدارهای تکراری باقی مانده ارزیابی می‌شود.

در جدول ۱ تعداد کل هشدارها برابر با ۱۰۰۰۰ هشدار است که از این تعداد هشدار ۷.۱٪ هشدارها (یعنی تعداد ۷۱۴ هشدار) به عنوان TP و ۹۲.۹٪ هشدارها (یعنی تعداد ۹۲۸۶ هشدار) به عنوان FP شناسایی شده است.

جدول ۱. کلیات مجموعه داده استفاده شده

	Frequency	Percent	Valid Percent	Cumulative Percent
FP	۹۲۸۶	۹۲.۹	۹۲.۹	۹۲.۹
TP	۷۱۴	۷.۱	۹۲.۹	۱۰۰.۰
Total	۱۰۰۰۰	۱۰۰.۰	۱۰۰.۰	

مجموعه داده‌ای با مشخصات بالا به عنوان ورودی به فیلتر ارائه شده ارسال می‌شود. نمودار ۱ نتایج حاصل از عملکرد فیلتر را با انتخاب حد آستانه ۱ با هدف کاهش FPها به همراه حذف هشدارهای تکراری نشان می‌دهد.



نمودار ۱. تعداد هشدارهای انتخاب شده در حالتی که فیلتر به کاهش FPها و حذف هشدارهای تکراری می‌پردازد.

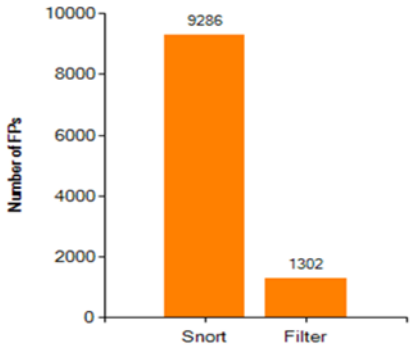
با توجه به نمودار ۱ از ۱۰۰۰۰ هشدار تولید شده توسط اسنورت تنها ۱۳۱۲ هشدار توسط فیلتر انتخاب و به مدیر شبکه ارائه شده است. بنابراین در این حالت کاهش ۸۶٪ اتفاق افتاده است. اما این سؤال مطرح می‌شود که از ۱۳۱۲ هشدار انتخاب شده توسط فیلتر چه تعداد از هشدارهای درست انتخاب شده اند؟ به عبارت دیگر با کاهش هشدارها، تعداد هشدارهای درست هم کاهش پیدا کرده یا همچنان نرخ انتخاب هشدارهای درست نسبت به قبل از عملیات فیلترسازی ثابت است. در ادامه، این موضوع به طور دقیق مورد بررسی قرار گرفته است.

جدول ۲ عملکرد فیلتر را در حالتی که فیلتر تنها به کاهش FPها می پردازد نشان می دهد. همان‌طور که در جدول ۲ مشخص شده از تعداد ۹۲۸۶ FP تولید شده توسط اسنورت تعداد ۷۸۴۲ FP توسط فیلتر انتخاب شده است. درست است که یک کاهش ۱۵.۵۵٪ خیلی قابل قبول نیست اما نکته مهم اینجاست که با توجه به جداول ۱ و ۲ از ۷۱۴ هشدار درست تولید شده توسط اسنورت تعداد ۶۸۹ هشدار درست توسط فیلتر انتخاب شده است. در این حالت فیلتر پیشنهادی به میزان ۹۶٪ در انتخاب هشدارهای درست موفق بوده است.

درصد کاهش	فیلتر	اسنورت	
٪ ۱۴	۸۵۳۱	۱۰۰۰۰	تعداد کل هشدارها
٪ ۱۵.۵۵	۷۸۴۲	۹۲۸۶	تعداد FPها
٪ ۰	۷۲۱۹	۷۲۱۹	تعداد هشدارهای تکراری

در نمودار ۲ تعداد FPها یی را نشان می دهد که فیلتر علاوه بر کاهش FP ها به حذف هشدارهای تکراری نیز پرداخته است. در نمودار نشان می دهد از ۹۲۸۶ هشدار FP تولید شده توسط اسنورت تنها ۱۳۰۲ FP توسط فیلتر انتخاب شده، که در آن یک کاهش ۶۵.۸۹٪ از FPها وجود دارد.

در ادامه نموداری که در آن تعداد FPها را در حالتی که فیلتر علاوه بر کاهش FP ها به حذف هشدارهای تکراری نیز میپردازد، نشان می دهد. همان‌طور که در نمودار ۲ مشخص شده از ۹۲۸۶ هشدار FP تولید شده توسط اسنورت تنها ۱۳۰۲ FP توسط فیلتر انتخاب شده، که در این حالت یک کاهش ۶۵.۸۹٪ از FPها وجود دارد.



نمودار ۲ . تعداد FPهای انتخاب شده در حالتی که فیلتر به کاهش FPها و حذف هشدارهای تکراری می‌پردازد

با توجه به اعداد نشان داده شده در نمودارهای ۱ و ۲ از ۱۳۱۲ هشدار انتخاب شده توسط فیلتر ۱۳۰۲ هشدار FP وجود دارد. بنابراین از بین هشدارهای انتخاب شده تنها ۱۰ هشدار درست وجود دارد. در توضیح این امر آن که فیلتر ارائه شده به منظور حذف FPها از امتیازات نسبت داده شده به هر هشدار استفاده می‌کند و هر هشداری که دارای امتیازی کمتر از مقدار حد آستانه باشد به عنوان یک FP حذف می‌گردد. از طرف دیگر این فیلتر به منظور حذف هشدارهای تکراری از شباهت مقادیر موجود در ویژگی‌های signature، source-ip، dest-ip و اختلاف زمانی کمتر از ۱ دقیقه بین هشدارهای موجود در یک دسته استفاده می‌کند. بنابراین حذف هشدارهای تکراری هیچ ارتباطی با حذف FPها ندارد.

در نهایت با در نظر گرفتن این نکته که هشدارهای درست نیز می‌توانند تکراری باشند و با توجه به جداول ۱ و ۲ از تعداد ۷۱۴ هشدار درست تولید شده توسط اسنورت تعداد ۶۸۹ = ۸۵۳۱-۷۸۴۲ هشدار درست توسط فیلتر انتخاب شده است. بنابراین در نتیجه که از بین ۷۱۴ هشدار درست انتخاب شده توسط فیلتر تنها ۱۰ هشدار غیر تکراری وجود دارد و بقیه هشدارهای درست، هشدارهایی هستند که در یک زمان یا در فاصله زمانی کمتر از ۱ دقیقه اتفاق افتاده‌اند و حملات یکسانی را از IP خاصی به IP خاص دیگری نشان می‌دهند. بنابراین چنین هشدارهایی به عنوان هشدارهای تکراری حذف می‌گردند (در این حالت فرقی نمی‌کند که هشدار حذف شده یک هشدار درست یا یک FP باشد).

۷- نتیجه گیری

این فیلتر با هدف کاهش FPها و حذف هشدارهای تکراری می‌تواند برای مجموعه هشدارهای تولید شده توسط هر سیستم تشخیص نفوذی اجرا شود.. همان‌طور که در بخش ۲.۳.۳ بیان شد این فیلتر از ترکیب سه نظریه استفاده کرده و امتیازاتی برای هر هشدار در نظر می‌گیرد. امتیاز نسبت داده شده به هر هشدار میزان درست بودن هشدار را نشان می‌دهد. بنابراین هر هشداری که امتیازی بیشتر از حد آستانه تعریف شده توسط مدیر شبکه داشته باشد به عنوان هشدار درست باید به مدیر شبکه ارسال شود و در غیر این صورت به عنوان هشدار نادرست از مجموعه هشدارهای تولید شده توسط سیستم تشخیص نفوذ حذف می‌گردد.

در این فیلتر سعی شده تا با حفظ نرخ تشخیص، به حذف هشدارهای نادرست و تکراری بپردازد و بدین صورت با کاهش تعداد هشدارهای ارسال شده، زمان مورد نیاز برای تحلیل و بررسی هشدارها را کاهش دهد.نویسندگان محترم مقالات سعی کنند تمام موارد ذکر شده را دقیقاً رعایت کنند، و از همین سند بعنوان الگوی نگارش مقاله خود استفاده کنند.

مراجع

[1] Herrero, Alvaro, Marti Navarro, Emilio Corchado, and Vicente Julian. "*RT-MOVICAB-IDS: Addressing real-time intrusion detection*.", Future Generation Computer Systems 29, no. 1 (2013): 250-261.Sannella, M. J., *Constraint Satisfaction and Debugging for Interactive User Interfaces*, Ph.D. Thesis, University of Washington, Seattle, WA, 1994.

[2] Ganame, Abdoul Karim, Julien Bourgeois, Renaud Bidou, and Francois Spies. "*A global security architecture for intrusion detection on computer networks*." Computers & Security 27, no. 1-2 (2008): 30-47.Plamondon, R., Lorette, G., "Automatic Signature Verification and Writer Identification - The State of the Art", Pattern Recognition, Vol. 22, pp. 107-131, 1989.

[3] Kizza, Joseph Migga. *Guide to Computer*. Edited by A.J. Sammes. London, 2013.

[4] Sangkatsanee, Phurivit, Naruemon Wattanapongsakor, and Chalermpol Charnsripinyo. "*Practical real-time intrusion detection using machine learning approaches*." Computer Communications 34, no. 18 (2011).

[5] Sadoddin, Reza, and Ali A Ghorbani. "*An incremental frequent structure mining framework for real-time alert correlation*." Computers & Security 28, no. 3-4 (2009).

[6] Liao, Hung-Jen, Chun-Hung Richard Lin, Ying-Chi Lin, and Kuang-Yuan Tung. "*Intrusion detection system: A comprehensive review*." Journal of Network and Computer Applications 36, no. 1 (2013).

[7]] Spathoulas, Georgios P, and Sokratis K Katsikas. "*Reducing false positives in intrusion detection systems*." Computers & Security 29, no. 1 (2010): 35-44.

[8] Patel, Ahmed, Mona Taghavi, kaveh Bakhtiyari, and Joaquim Celestino Junior. "*An intrusion detection and prevention system in cloud computing: A systematic review*." Journal of Network and Computer Applications 36, no. 1 (2013): 25-41.

[9] Ghorbani, Ali A, Wei Lu, and Mahbod Tavallaee. "*Alert Management and Correlation*." Advances in Information Security 47 (2010): 129-160.

[10] Huwaida, Tagelsir Elshoush, and Mohamed Osman Izzeldin. "*Alert correlation in collaborative intelligent intrusion detection systems—A survey*." Applied Soft Computing 11, no. 7 (2011).

[11]] Wu, Su-Yun, and Ester Yen. "*Data mining-based intrusion detectors*." Expert Systems with Applications 36, no. 3 (2009): 5605-5612.

[12] Davis, Jonathan J, and Andrew J Clark. "*Data preprocessing for anomaly based network intrusion detection: A review*." Computers & Security 30, no. 6-7 (2011).

[13] Garcia-Teodoro, P, J Diaz-Verdejo, G Macia-Fernández, and E Vazquez. "*Anomaly-based network intrusion detection: Techniques, systems and challenges*." Computers & Security 28, no. 1-2 (2009).

[14] Mudzingwa, David, and Rajeev Agrawal. "*A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS)*." Southeastcon Proceedings of IEEE, 2012: 1-6.

[15] Baker, Andrew R, and Joel Esler. *Snort IDS and IPS Toolkit*. Canada: Andrew Williams, 2007.

[16] Perdisci, Roberto , Giorgio Giacinto, and Fabio Roli. "*Alarm clustering for intrusion detection systems in*

computer networks." Engineering Applications of Artificial Intelligence, 2006.

[17] Al-mamory, Safaa O, and Hongli Zhang. "*Intrusion detection alarms reduction using root cause analysis and clustering*." Computer Communications 23, no. 2 (2009).

[18] El-Taj, Homam, Omar Abouabdalla, Ahmed Manasrah, and Sureswaran Ramadas. "*False positive reduction in intrusion detectionsystem: A survey*." Proceedings of IC-BNMT, 2009.

[19] Vaarandi, Risto, and Karlis Podiņš. "*Network IDS Alert Classification with Frequent Itemset Mining and Data Clustering*." Network and Service Management (CNSM), 2010: 451-456.

[20] Om, Hari, and Aritra Kundu. "*A hybrid system for reducing the false alarm rate ofanomaly intrusion detection system*." Recent Advances in Information Technology, 2012: 131 - 136.

[21] Spathoulas, Georgios p, and Sokratis K Katsikas. "*Enhancing IDS performance through comprehensive alert post-processing*." Computers & Security 37 (2013).

[22] Louvieris, Panos, Natalie Clewley, and Xiaohui Liu. "*Effects-based feature identification for network intrusion detection*." Neurocomputing 121 (2013): 265-273.

[23]] Meng, Yuxin , and Lam-For Kwok. "*Adaptive blacklist-based packet filter with a statistic-based approach in network intrusion detection*." Network and Computer Applications 39 (2013): 83-92.