وزارت ارتباطات و فناوری اطلاعات شرکت ارتباطات زیرساخت	عنوان مقاله: حوزه فناوری و کاربردهای تشخیص و مقابله با حملات Firewall&Detection&Attack تهیه کنندگان: رشته تحصیلی رشته شغلی اداره کل/دفتر میثم عابدی / دانشجوی دکترای کامپیوتر / کارشناس / امنیت شبکه های زیرساختی جعفر باقریان / مدیرکل/ امنیت شبکه های زیرساختی حامد محمدزاده / معاون اداره کل/ امنیت شبکه های زیرساختی فرشاد پیری/ رئیس اداره / امنیت شبکه های زیرساختی عنوان حوزه تحقیقاتی مورد نیاز شرکت: حوزه فناوری و کاربردهای تشخیص و مقابله با حملات Firewall&Detection&Attack شماره ردیف حوزه تحقیقاتی مورد نیاز شرکت: ۷۰
این قسمت توسط دبیرخانه کمیته علمی تکمیل می‌گردد.	شماره مقاله: حوزه کاربردی:

چکیده – امروزه با افزایش استفاده از فناوری‌های نوین و پیشرفته، شبکه‌های کامپیوتری به یکی از اهداف اصلی حملات سایبری تبدیل شده‌اند. این حملات می‌توانند منجر به خسارات مالی، سرقت اطلاعات و اختلال در عملکرد شبکه شوند. برای مقابله با این حملات، راهکارهای مختلفی وجود دارد که یکی از مهم‌ترین آنها، تشخیص و مقابله با حملات است.

در این مقاله، به بررسی حوزه فناوری و کاربردهای تشخیص و مقابله با حملات پرداخته می‌شود. ابتدا، روش‌های تشخیص حملات معرفی می‌شوند. سپس، روش‌های مقابله با حملات مورد بررسی قرار می‌گیرند. در ادامه، کاربردهای تشخیص و مقابله با حملات بیان می‌شوند. در نهایت، فناوری‌های نوین در حوزه تشخیص و مقابله با حملات بررسی می‌شوند.

کلید واژه– تشخیص حملات، مقابله با حملات، فناوری‌های نوین

۱–مقدمه :

در دنیای امروزی که فناوری‌ها و شبکه‌های کامپیوتری به نقطه‌ی بی‌بدیلی از زندگی ما تبدیل شده‌اند، مسائل امنیتی و حفاظت از اطلاعات از اهمیت بسیاری برخوردارند. از این رو، مفهوم‌های تشخیص و جلوگیری از حملات شبکه، از جمله نصب و پیکربندی فایروال (Firewall)، تشخیص حملات (Detection) و مقابله با آن‌ها، اهمیت چشمگیری برای تضمین امنیت و ادامه‌ی عملکرد صحیح سیستم‌ها و شبکه‌های کامپیوتری دارند.

نگرانی‌ها درباره‌ی تهدیدات امنیتی، از جمله حملات دیده‌ی نفوذ (Intrusion Attacks)، نفوذگران (Intruders) و حملات از طریق نرم‌افزارهای آسیب‌پذیر، همواره بر سر کاربران و مدیران سیستم‌ها استوار بوده است. استفاده از فایروال‌ها برای کنترل دسترسی به شبکه و ترافیک آن، همچنین سیستم‌های تشخیص نفوذ (Intrusion Detection Systems - IDS) و سیستم‌های تشخیص و پیشگیری از تهدیدات (Intrusion Prevention Systems - IPS)، از جمله روش‌های اصلی برای مقابله با این تهدیدات محسوب می‌شوند.

این مقاله به بررسی عمیق‌تر و بیشتری از فناوری‌های مورد استفاده برای تشخیص حملات شبکه و نحوه‌ی مقابله با آن‌ها می‌پردازد. هدف اصلی این مقاله، ارائه‌ی یک مرور جامع از فایروال‌ها و سیستم‌های تشخیص نفوذ و جلوگیری از حملات شبکه به‌منظور بهبود امنیت شبکه‌ها و سیستم‌های کامپیوتری است.

در این مقاله، ابتدا به مفاهیم اساسی فایروال‌ها و نحوه‌ی عملکرد آن‌ها پرداخته خواهد شد. سپس، به بررسی روش‌های تشخیص حملات شبکه، از جمله سیستم‌های تشخیص نفوذ (IDS) و جلوگیری از حملات (IPS) می‌پردازیم. در ادامه، به مطالعه موردی و مقایسه‌ی این فناوری‌ها و نیز بررسی بهترین روش‌های پیاده‌سازی و استفاده از آن‌ها می‌پردازیم.

۲-تعریف مسئله :

با توجه به اهمیت فناوری‌های مذکور برای حفاظت از شبکه‌ها و اطلاعات، مقاله‌ی حاضر با هدف ارتقاء دانش و شناخت در این زمینه ارائه شده است تا امکان دسترسی به اطلاعاتی که برای مقابله با تهدیدات شبکه ضروری است، فراهم گردد.

با افزایش استفاده از فناوری‌های نوین و پیشرفته، شبکه‌های کامپیوتری به یکی از اهداف اصلی حملات سایبری تبدیل شده‌اند. این حملات می‌توانند منجر به خسارات مالی، سرقت اطلاعات و اختلال در عملکرد شبکه شوند. برای مقابله با این حملات، راهکارهای مختلفی وجود دارد که یکی از مهم‌ترین آنها، تشخیص و مقابله با حملات است.

تشخیص و مقابله با حملات، فرآیندی است که در آن فعالیت‌های مشکوک در شبکه شناسایی و اقدامات لازم برای مقابله با آنها انجام می‌شود. این فرآیند شامل دو مرحله اصلی است:

۲-۱- تشخیص حملات: در این مرحله، فعالیت‌های مشکوک در شبکه شناسایی می‌شوند.

۲-۲- مقابله با حملات: در این مرحله، اقدامات لازم برای مقابله با حملات انجام می‌شوند.

۲-۱-روش‌های تشخیص حملات:

روش‌های تشخیص حملات را می‌توان به سه دسته کلی تقسیم کرد: روش‌های مبتنی بر امضای حملات ، روش‌های مبتنی بر رفتار و روش‌های مبتنی بر یادگیری ماشین

۲-۱-۱- روش‌های مبتنی بر امضای حملات

در این روش‌ها، امضای حملات شناخته شده به سیستم تشخیص حملات ارائه می‌شود. سیستم تشخیص حملات با مقایسه فعالیت‌های شبکه با امضای حملات، فعالیت‌های مشکوک را شناسایی می‌کند. این روش‌ها ساده و کارآمد هستند، اما در برابر حملات جدید و ناشناخته عملکرد خوبی ندارند.

در روش‌های مبتنی بر امضای حملات، یک پایگاه داده از امضای حملات شناخته شده ایجاد می‌شود. امضای حمله، یک الگو یا ویژگی منحصر به فرد است که در حملات خاص یافت می‌شود. سیستم تشخیص حملات، فعالیت‌های شبکه را با امضای حملات موجود در پایگاه داده مقایسه می‌کند. اگر فعالیتی با یک امضای حمله شناخته شده مطابقت داشته باشد، به عنوان یک فعالیت مشکوک شناسایی می‌شود.

روش‌های مبتنی بر امضای حملات دارای مزایای زیر هستند:

- ساده و کارآمد هستند.
- نیاز به داده‌های آموزشی زیادی ندارند.

روش‌های مبتنی بر امضای حملات دارای معایب زیر هستند:

- در برابر حملات جدید و ناشناخته عملکرد خوبی ندارند.
- ممکن است حملات جدیدی که امضای آنها در پایگاه داده وجود ندارد، شناسایی نشوند.

۲-۱-۲- روش‌های مبتنی بر رفتار

در این روش‌ها، فعالیت‌های شبکه به صورت رفتاری بررسی می‌شوند. سیستم تشخیص حملات با یادگیری از رفتارهای طبیعی شبکه، فعالیت‌های مشکوک را شناسایی می‌کند. این روش‌ها در برابر حملات جدید و ناشناخته عملکرد بهتری دارند، اما پیچیده‌تر و نیازمند داده‌های آموزشی بیشتری هستند.

در روش‌های مبتنی بر رفتار، فعالیت‌های شبکه به صورت رفتاری بررسی می‌شوند. سیستم تشخیص حملات با یادگیری از رفتارهای طبیعی شبکه، فعالیت‌های مشکوک را شناسایی می‌کند.

روش‌های مبتنی بر رفتار دارای مزایای زیر هستند:

- در برابر حملات جدید و ناشناخته عملکرد بهتری دارند.
- می‌توانند حملات را شناسایی کنند که امضای آنها در پایگاه داده وجود ندارد.

روش‌های مبتنی بر رفتار دارای معایب زیر هستند:

- پیچیده‌تر هستند.
- نیاز به داده‌های آموزشی زیادی دارند.

۳-۱-۲- روش‌های مبتنی بر یادگیری ماشین

روش‌های مبتنی بر یادگیری ماشین، ترکیبی از روش‌های مبتنی بر امضای حملات و روش‌های مبتنی بر رفتار هستند. در این روش‌ها، از الگوریتم‌های یادگیری ماشین برای شناسایی فعالیت‌های مشکوک استفاده می‌شود. این روش‌ها می‌توانند عملکرد بهتری نسبت به روش‌های مبتنی بر امضای حملات و روش‌های مبتنی بر رفتار داشته باشند.

روش‌های مبتنی بر یادگیری ماشین دارای مزایای زیر هستند:

- می‌توانند از مزایای روش‌های مبتنی بر امضای حملات و روش‌های مبتنی بر رفتار بهره ببرند.
- در برابر حملات جدید و ناشناخته عملکرد خوبی دارند.

روش‌های مبتنی بر یادگیری ماشین دارای معایب زیر هستند:

- پیچیده‌تر هستند.
- نیاز به داده‌های آموزشی زیادی دارند.

انتخاب روش تشخیص حملات

انتخاب روش تشخیص حملات به عوامل مختلفی بستگی دارد، از جمله:

- نوع حمله: برخی از روش‌ها برای تشخیص برخی از انواع حملات بهتر هستند.
- پیچیدگی حمله: برخی از روش‌ها برای تشخیص حملات پیچیده بهتر هستند.
- مقدار داده‌های آموزشی: برخی از روش‌ها به داده‌های آموزشی بیشتری نیاز دارند.
- هزینه: برخی از روش‌ها هزینه بیشتری دارند.

در نهایت، بهترین روش تشخیص حملات، روشی است که برای شرایط خاص شبکه بهترین عملکرد را داشته باشد.

۲-۲- روش‌های مقابله با حملات:

پس از تشخیص حملات، اقدامات لازم برای مقابله با آنها باید انجام شود. این اقدامات عبارتند از:

- مسدود کردن دسترسی مهاجم به شبکه: این اقدام مهم‌ترین اقدام برای مقابله با حملات است.
- حذف فایل‌های مخرب: فایل‌های مخربی که توسط مهاجم وارد شبکه شده‌اند، باید حذف شوند.
- بازیابی اطلاعات آسیب‌دیده: اطلاعات آسیب‌دیده باید بازیابی شوند.

۱-۲-۲- مسدود کردن دسترسی مهاجم به شبکه

پس از تشخیص حمله، مهم است که دسترسی مهاجم به شبکه مسدود شود. این کار می‌تواند از گسترش حمله و آسیب بیشتر به شبکه جلوگیری کند.

برای مسدود کردن دسترسی مهاجم به شبکه، می‌توان از روش‌های مختلفی استفاده کرد، از جمله:

- استفاده از فایروال: فایروال می‌تواند دسترسی به شبکه را بر اساس آدرس IP، پورت یا پروتکل محدود کند.
- استفاده از سیستم‌های شناسایی و جلوگیری از نفوذ (IPS/IDS): IPS/IDS می‌تواند ترافیک شبکه را برای فعالیت‌های مشکوک بررسی کند و در صورت تشخیص حمله، دسترسی مهاجم را مسدود کند.
- استفاده از سیستم‌های مدیریت دسترسی به شبکه (NAC): NAC می‌تواند وضعیت امنیتی دستگاه‌های متصل به شبکه را بررسی کند و در صورت تشخیص دستگاه‌های آلوده، دسترسی آنها را مسدود کند.

۲-۲-۲- حذف فایل‌های مخرب:

پس از مسدود کردن دسترسی مهاجم به شبکه، باید فایل‌های مخربی که توسط مهاجم وارد شبکه شده‌اند، حذف شوند. این فایل‌ها می‌توانند شامل ویروس‌ها، تروجان‌ها، نرم‌افزارهای جاسوسی و سایر نرم‌افزارهای مخرب باشند.

برای حذف فایل‌های مخرب، می‌توان از روش‌های مختلفی استفاده کرد، از جمله:

- استفاده از آنتی‌ویروس: آنتی‌ویروس می‌تواند فایل‌های مخرب را شناسایی و حذف کند.
- استفاده از ابزارهای پاکسازی: ابزارهای پاکسازی می‌توانند فایل‌های مخرب را به طور کامل از سیستم پاک کنند.

۳-۲-۲- بازیابی اطلاعات آسیب‌دیده:

اگر در اثر حمله، اطلاعات شبکه آسیب دیده باشند، باید آنها را بازیابی کرد. این کار می‌تواند از دست رفتن اطلاعات مهم را جلوگیری کند.

برای بازیابی اطلاعات آسیب‌دیده، می‌توان از روش‌های مختلفی استفاده کرد، از جمله:

- استفاده از نسخه پشتیبان: اگر از اطلاعات شبکه نسخه پشتیبان تهیه شده باشد، می‌توان از آن برای بازیابی اطلاعات آسیب‌دیده استفاده کرد.
- استفاده از ابزارهای بازیابی اطلاعات: ابزارهای بازیابی اطلاعات می‌توانند اطلاعات آسیب‌دیده را از سیستم بازیابی کنند.

۴-۲-۲- سایر اقدامات مقابله با حملات

علاوه بر اقدامات ذکر شده، می‌توان از اقدامات دیگری نیز برای مقابله با حملات استفاده کرد، از جمله:

- آموزش کاربران: آموزش کاربران در مورد نحوه شناسایی و مقابله با حملات می‌تواند به کاهش خطر حملات کمک کند.
- به‌روزرسانی سیستم‌ها و نرم‌افزارها: به‌روزرسانی سیستم‌ها و نرم‌افزارها می‌تواند به رفع آسیب‌پذیری‌های امنیتی کمک کند که می‌توانند مورد استفاده مهاجمان قرار گیرند.
- استفاده از معماری امنیتی چند لایه: استفاده از معماری امنیتی چند لایه می‌تواند از شبکه در برابر حملات مختلف محافظت کند.

با اتخاذ اقدامات مناسب برای تشخیص و مقابله با حملات، می‌توان از شبکه در برابر حملات سایبری محافظت کرد.

۳-۲- کاربردهای تشخیص و مقابله با حملات:

تشخیص و مقابله با حملات کاربردهای مختلفی دارد که عبارتند از:

- امنیت شبکه :تشخیص و مقابله با حملات، یکی از مهم‌ترین اقدامات برای افزایش امنیت شبکه است. این امر می‌تواند از شبکه در برابر حملات مختلفی، از جمله حملات هک، حملات DDoSو حملات ransomware محافظت کند.
- حفظ حریم خصوصی :تشخیص و مقابله با حملات، به حفظ حریم خصوصی کاربران کمک می‌کند. این امر می‌تواند از سرقت اطلاعات شخصی، مانند رمزهای عبور و اطلاعات کارت اعتباری، جلوگیری کند.
- اطمینان از عملکرد شبکه :تشخیص و مقابله با حملات، به اطمینان از عملکرد شبکه کمک می‌کند. این امر می‌تواند از اختلال در شبکه، مانند قطعی سرویس یا سرقت اطلاعات، جلوگیری کند.

کاربردهای خاص تشخیص و مقابله با حملات

تشخیص و مقابله با حملات در زمینه‌های مختلف کاربرد دارد، از جمله:

- اداره کسب‌وکارها :تشخیص و مقابله با حملات می‌تواند به محافظت از اطلاعات تجاری و جلوگیری از خسارات مالی کمک کند.
- سازمان‌های دولتی :تشخیص و مقابله با حملات می‌تواند به محافظت از اطلاعات حساس دولتی و جلوگیری از جاسوسی کمک کند.
- مؤسسات آموزشی :تشخیص و مقابله با حملات می‌تواند به محافظت از اطلاعات شخصی دانشجویان و کارکنان و جلوگیری از انتشار اطلاعات محرمانه کمک کند.

با افزایش پیچیدگی حملات سایبری، تشخیص و مقابله با حملات نیز اهمیت بیشتری پیدا می‌کند. با اتخاذ اقدامات مناسب برای تشخیص و مقابله با حملات، می‌توان از شبکه در برابر حملات سایبری محافظت کرد و از خسارات مالی، از دست رفتن اطلاعات و سایر آسیب‌ها جلوگیری کرد.

۴-۲- فناوری‌های نوین در حوزه تشخیص و مقابله با حملات:

فناوری‌های نوین نقش مهمی در بهبود عملکرد سیستم‌های تشخیص و مقابله با حملات ایفا کرده‌اند. از جمله این فناوری‌ها می‌توان به موارد زیر اشاره کرد:

- یادگیری ماشین: یادگیری ماشین به سیستم‌های تشخیص و مقابله با حملات کمک می‌کند تا در شناسایی فعالیت‌های مشکوک دقیق‌تر عمل کنند.
- هوش مصنوعی: هوش مصنوعی به سیستم‌های تشخیص و مقابله با حملات کمک می‌کند تا در مقابله با حملات پیچیده‌تر، عملکرد بهتری داشته باشند.
- بلاک چین: بلاک چین به سیستم‌های تشخیص و مقابله با حملات کمک می‌کند تا اطلاعات مربوط به حملات را به طور ایمن ذخیره کنند.

۱-۴-۲- یادگیری ماشین

یادگیری ماشین یکی از مهم‌ترین فناوری‌های نوین در حوزه تشخیص و مقابله با حملات است. یادگیری ماشین به سیستم‌های تشخیص و مقابله با حملات کمک می‌کند تا الگوهای رفتاری مهاجمان را یاد بگیرند و در آینده آنها را شناسایی کنند.

۲-۴-۲- هوش مصنوعی

هوش مصنوعی نیز یکی دیگر از فناوری‌های نوین در حوزه تشخیص و مقابله با حملات است. هوش مصنوعی به سیستم‌های تشخیص و مقابله با حملات کمک می‌کند تا در مقابله با حملات پیچیده‌تر، عملکرد بهتری داشته باشند.

۳-۴-۲- بلاک چین

بلاک چین نیز یک فناوری نوین است که می‌تواند در حوزه تشخیص و مقابله با حملات کاربرد داشته باشد. بلاک چین می‌تواند برای ذخیره اطلاعات مربوط به حملات استفاده شود. این امر می‌تواند به سازمان‌ها کمک کند تا حملات را بهتر شناسایی و مقابله کنند.

۴-۴-۲- سایر فناوری‌های نوین

علاوه بر فناوری‌های ذکر شده، فناوری‌های نوین دیگری نیز در حوزه تشخیص و مقابله با حملات در حال توسعه هستند. از جمله این فناوری‌ها می‌توان به موارد زیر اشاره کرد:

- آنالیز رفتار کاربران: این فناوری با بررسی رفتار کاربران می‌تواند فعالیت‌های مشکوک را شناسایی کند.
- تجزیه و تحلیل شبکه: این فناوری با تجزیه و تحلیل ترافیک شبکه می‌تواند فعالیت‌های مشکوک را شناسایی کند.
- خودکارسازی: این فناوری می‌تواند بسیاری از فرآیندهای دستی تشخیص و مقابله با حملات را خودکار کند.

با توسعه فناوری‌های نوین، سیستم‌های تشخیص و مقابله با حملات نیز پیشرفت‌های زیادی کرده‌اند. این پیشرفت‌ها به سازمان‌ها کمک می‌کند تا از شبکه‌های خود در برابر حملات سایبری محافظت کنند.

۵-۲- چالش‌های تشخیص و مقابله با حملات

تشخیص و مقابله با حملات چالش‌های مختلفی دارد، از جمله:

- تنوع حملات: حملات سایبری بسیار متنوع هستند و هر روز حملات جدیدی ابداع می‌شوند. این امر تشخیص حملات را دشوار می‌کند.
- پیچیدگی حملات: حملات سایبری روز به روز پیچیده‌تر می‌شوند. این امر مقابله با حملات را دشوار می‌کند.
- سرعت حملات: حملات سایبری اغلب بسیار سریع هستند. این امر تشخیص و مقابله با حملات را دشوار می‌کند.
- نقص‌های امنیتی: هیچ سیستم امنیتی کاملی وجود ندارد. همیشه نقص‌های امنیتی وجود دارند که می‌توانند مورد استفاده مهاجمان قرار گیرند.

۳- آینده تشخیص و مقابله با حملات

با توجه به چالش‌های ذکر شده، آینده تشخیص و مقابله با حملات با چالش‌هایی همراه خواهد بود. با این حال، فناوری‌های نوین می‌توانند به بهبود عملکرد سیستم‌های تشخیص و مقابله با حملات کمک کنند. از جمله این فناوری‌ها می‌توان به موارد زیر اشاره کرد:

- یادگیری ماشین: یادگیری ماشین می‌تواند به سیستم‌های تشخیص و مقابله با حملات کمک کند تا در شناسایی حملات جدید و ناشناخته عملکرد بهتری داشته باشند.
- هوش مصنوعی: هوش مصنوعی می‌تواند به سیستم‌های تشخیص و مقابله با حملات کمک کند تا در مقابله با حملات پیچیده‌تر عملکرد بهتری داشته باشند.
- خودکارسازی: خودکارسازی می‌تواند فرآیندهای دستی تشخیص و مقابله با حملات را سریع‌تر و کارآمدتر کند.

با توسعه فناوری‌های نوین، سیستم‌های تشخیص و مقابله با حملات می‌توانند در آینده عملکرد بهتری داشته باشند. با این حال، همچنان چالش‌هایی در این حوزه وجود خواهد داشت. سازمان‌ها باید برای مقابله با این چالش‌ها آماده باشند.

۴- راهکارهای مقابله با چالش‌های تشخیص و مقابله با حملات

برای مقابله با چالش‌های تشخیص و مقابله با حملات، سازمان‌ها می‌توانند از راهکارهای زیر استفاده کنند:

- استفاده از فناوری‌های نوین: استفاده از فناوری‌های نوین مانند یادگیری ماشین و هوش مصنوعی می‌تواند به بهبود عملکرد سیستم‌های تشخیص و مقابله با حملات کمک کند.
- آموزش کارکنان: آموزش کارکنان در مورد حملات سایبری می‌تواند به آنها کمک کند تا فعالیت‌های مشکوک را شناسایی کنند.
- به‌روزرسانی سیستم‌ها و نرم‌افزارها: به‌روزرسانی سیستم‌ها و نرم‌افزارها می‌تواند به رفع آسیب‌پذیری‌های امنیتی کمک کند.
- استفاده از معماری امنیتی چند لایه: استفاده از معماری امنیتی چند لایه می‌تواند از شبکه در برابر حملات مختلف محافظت کند.

۵- نتیجه‌گیری

با توجه به افزایش حملات سایبری، تشخیص و مقابله با حملات یکی از مهم‌ترین چالش‌های پیش روی شبکه‌های کامپیوتری است. فناوری‌های نوین نقش مهمی در بهبود عملکرد سیستم‌های تشخیص و مقابله با حملات ایفا کرده‌اند. استفاده از این فناوری‌ها می‌تواند به افزایش امنیت شبکه‌ها و کاهش آسیب‌های ناشی از حملات سایبری کمک کند. با توسعه فناوری‌های نوین، سیستم‌های تشخیص و مقابله با حملات نیز پیشرفت‌های زیادی کرده‌اند. این پیشرفت‌ها به سازمان‌ها کمک می‌کند تا از شبکه‌های خود در برابر حملات سایبری محافظت کنند. با اتخاذ این راهکارها، سازمان‌ها می‌توانند از شبکه‌های خود در برابر حملات سایبری محافظت کنند.

مراجع

[۱]S. Singh, A. Pise, O. Alfarraj, A. Tolba, B. Yoon, A Cryptographic Approach to Prevent Network Incursion for Enhancement of QoS in Sustainable Smart City Using MANET, vol. 79, Sustainable Cities and Society, 2022, 103483.

[2]S. Dalal, B. Seth, V. Jaglan, M. Malik, N. Dahiya, U. Rani, D.N. Le, Y.C. Hu, An adaptive traffic routing approach toward load balancing and congestion control in Cloud–MANET ad hoc networks, Soft Comput. 26 (11) (2022)

[3]O. Faker, E. Dogdu, Intrusion detection using big data and deep learning techniques, in: Proceedings of the 2019 ACM Southeast Conference, 2019, April

[4]S. Rajabi, S. Jamali, J. Javidan, An intrusion detection system in computer networks using the firefly algorithm and the fast learning network, Int. J. Wine Res. 3 (1) (2020).

[5]S. Kanthimathi, J.R. Prathuri, Classification of misbehaving nodes in MANETS using machine learning techniques, in: 2020 2nd PhD Colloquium on Ethically Fig. 5.Percentage of maliciousness in performance analysis.

[6]M.R. Ghori, T.C. Wan, G.C. Sodhy, Bluetooth low energy mesh networks: survey of communication and security protocols, (2020).

[7]H.M.A. Fahmy, Wireless sensor networks essentials, in: Wireless Sensor Networks, Springer, Cham, 2020, pp. 3–39.

[8]S.S.S. Sugi, S.R. Ratna, Investigation of machine learning techniques in intrusion detection system for IoT network, in: 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), IEEE, 2020.

[9]H. Zhang, K.Y. Lin, W. Chen, L. Genyuan, Using machine learning techniques to improve intrusion detection accuracy, in: 2019 IEEE 2nd International Conference on Knowledge Innovation and Invention (ICKII), IEEE, 2019, July.

[10]Y. Koizumi, Y. Kawaguchi, K. Imoto, T. Nakamura, Y. Nikaido, R. Tanabe, H. Purohit, K. Suefusa, T. Endo, M. Yasuda, N. Harada, Description and Discussion on DCASE2020 Challenge Task2: Unsupervised Anomalous Sound Detection for Machine Condition Monitoring, 2020.

[11]A. Divekar, M. Parekh, V. Savla, R. Mishra, M. Shirole, Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives, in: 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), IEEE, 2018, October.
[12]N. Singh, A. Dumka, R. Sharma, A novel technique to defend DDOS attack in manet, J. Comput. Eng. Inf. Technol. 7 (2018)
[13]S. Kanthimathi, J.R. Prathuri, Classification of misbehaving nodes in MANETS using machine learning techniques, in: 2020 2nd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS), IEEE, 2020.
[14]T.V. Nguyen, T.N. Tran, T. Huynh-The, B. An, An Efficient QoS Routing Protocol in Cognitive Radio MANETs: Cross-Layer Design Meets Deep Reinforcement Learning, 2021.
[15]S. Mohammadi, H. Mirvaziri, M. Ghazizadeh-Ahsaee, H. Karimipour, Cyber intrusion detection by combined feature selection algorithm, J. Inf. Secur. Appl. 44 (2019).
[16]A. Chawla, B. Lee, S. Fallon, P. Jacob, Host based intrusion detection system with combined CNN/RNN model, in: Joint European Conference on Machine Learning