بررسی تشخیص نفوذ در شبکه های کامپیوتری با استفاده ازتکنیک های ترکیبی یادگیری ماشین

رضا خدابنده لو[1]– سمیه خلیفه لو[2]– مجتبی مظفری هشجین[3]

Intrusion detection in computer networks using a combination of machine learning technique: A Review

Reza Khodabandehlo-Somayeh Khalifeloo- Mojtaba Mozafari Hashjin
Taninrayaneh@Yahoo.Com

چکیده

توسعه ابزارهای حمله ودسترسی آسان هکرها به سیستم ها ونرم افزارها، به آنها این امکان را می دهد تا بتوانند حملات پیچیده را به راحتی ودر کوتاهترین زمان وحتی با دانش کم به انجام رسانند. تشخیص وجلوگیری از نفوذ امروزه به عنوان یکی از مکانیزم های اصلی ایجاد امنیت در شبکه ها و سیستم های رایانه ای مطرح است وعموما در کنار Firewall مورد استفاده قرار می گیرد. تشخیص نفوذ یک مشکل مهم تحقیقاتی در امنیت شبکه می باشد، همچنین سیستم های تشخیص نفوذ خبره نمی توانند خود را با حملات جدید تطبیق دهند بنابراین استفاده از تکنیک های یادگیری ماشین در یک سیستم تشخیص نفوذ که باعث افزایش قابلیت این سیستم ها شود بسیار مناسب می باشد. در این مقاله ابتدا با طرح سیستم تشخیص نفوذ به بررسی انواع روش های یادگیری ماشین می پردازیم.

کلمات کلیدی

تشخیص نفوذ – یادگیری ماشین – داده کاوی – شبکه بیزین – در خت تصمیم

۱. مقدمه

با ظهور اینترنت، اشتراک گذاری منابع به یک امر بسیار آسان تبدیل شده است. با این حال تهدیدات امنیتی سایبری ، روز به روز در حال افزایش است.بنابراین محافظت از سیستم در برابر فعالیت های نفوذی در کانون توجه محققین است. به تازگی IDS رشد قابل توجهی با توجه به اهمیت آن در امنیت شبکه داشته است . توسعه سیستم تشخیص نفوذ هوشمند برای حفاظت از شبکه محدوده ای از تکنیک های امنیتی شبکه مانند رمزنگاری ، فایروال (دیواره آتش) وسیستم کشف نفوذ را شامل می شود. پیش از این سیستم های امنیتی شبکه بر مبنای قانون قرار داشتند که تنها قادر به تشخیص ردیابی رویدادهای خاص بودند، با این حال ماهیت حملات در حال تغییر می باشد که نیازمند یک سیستم هوشمند وسازگاری برای تشخیص انواع حملاتی است که با استفاده از روش غیر معمول امنیت شبکه را به خطر می اندازند.تکنیک های هوش مصنوعی مبتنی بر یادگیری ماشین شامل روش ژنتیکی، روش الگوریتم، روش منطق فازی والگوریتم مبتنی بر داده کاوی بر فراگیری ماشین، تکنیک های مبتنی بر وعده

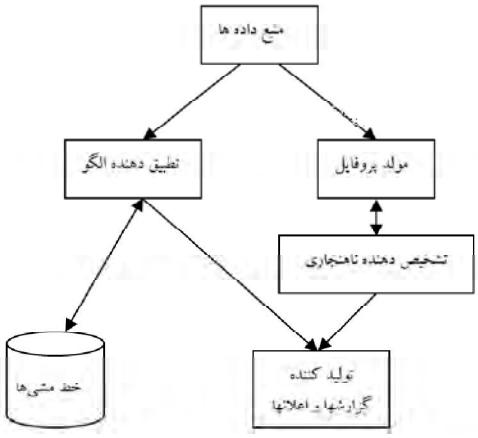
---

[1] مدرس دانشگاه جامع علمی کاربردی خانه کارگرواحد شهرقدس
[2] دانشجوی دانشگاه جامع علمی کاربردی خانه کارگرواحد شهرقدس
[3] دانشجوی دانشگاه جامع علمی کاربردی خانه کارگرواحد شهرقدس

می باشندکه در انجام وظایف مربوط به تشخیص نفوذ بسیار موفق هستند.از مزایای یادگیری ماشین این است که می تواند اطلاعات جدید از داده های قبلی را استنباط کند.[۱۷]

۲. سیستم تشخیص نفوذ

سیستم تشخیص نفوذ به عنوان خط دوم دفاعی در امنیت شبکه در نظر گرفته می شود. این یک کلاس ازیک نرم افزار است که می تواند یک حمله خاص را تشخیص وعلیه آن اقدام نماید. در یک معماری کلی IDS دارای واحد ذخیره سازی وتجزیه وتحلیل داده ها است که به تصمیم گیری از نفوذ می پردازد. داده ها در این واحد تغذیه توسط واحد نظارت که قطاری ازداده ها وانتقال آنها ست منتقل می شوند. براساس نتیجه تجزیه وتحلیل داده ها، IDS می تواند در مورد نفوذ هشدار یا خود اقدام نماید. [۱۷] به منظور پیاده سازی روش های تشخیص نفوذ ، سیستم های متعددی تحت عنوان سیستم تشخیص نفوذ (IDS) طراحی وساخته شده اند. در حوزه امنیت کامپیوتر، سیستم های تشخیص نفوذ نقش هشدار دهنده را ایفا می کنند، نهاد دیگری که مسئول امنیت سایت نامیده می شود می تواند به این هشدار پاسخ داده واقدام لازم را انجام دهد.[۲]



شکل ۱ : ساختار یک سیستم تشخیص نفوذ

۳. داده های سیستم تشخیص نفوذ

به طور کلی بیان خصوصیات و نحوه رفتار حمله ها و نفوذ کنندگان به شبکه های کامپیوتری معمولاً بسیار مشکل بوده و نیازمند شخص خبره میباشد. علاوه بر این با پیشرفت شبکه های کامپیوتری تعداد حمله ها و نفوذکنندگان نیز بیشتر و بیشتر میشود .در واقع دانشی که از انسانهای خبره به دست می آید با گذشت زمان ارزش خود را از دست میدهد و بایستی بروز شده و در اختیار سیستم قرار گیرد و همین عامل باعث میشود که نیاز به شخص خبره همواره احساس شود .در تکنیک های یادگیری ماشین دانش از خود داده ها استخراج میشود و همین عامل نقش شخص خبره را کمرنگ کرده است .[۲] جهت شبیه سازی ، تست وتعیین کارایی سیستم های IDS باید از داده های استاندارد استفاده شود.اولین داده های استاندارد ترافیک شبکه KDD-CUP۹۹ توسط گروه IST از آزمایشگاه MIT زیرنظر DARPA و AFRL/SNHS در طول چند هفته جمع آوری نمودند .این داده ها دارای ۴۱ ویژگی از هر داده می باشد.در داده های آموزشی ۲۶ نوع حمله شناخته شده ودر داده های تست ۱۴ نوع حمله ناشناخته دیگر گنجانده شد ومعمولاً برای ارزیابی IDS های بدون ناظر مورد استفاده قرار می گیرد.

حملات گنجانده شده در داده های تست عبارتنداز:

۱- حملات DOS انکار سرویس

۲- حملات PROBE بررسی وپویش برای یافتن راههای نفوذ
۳- حملات R۲L دسترسی غیر مجاز از یک ماشین راه دور
۴- حملات U۲R با بدست آوردن مجوز کاربر ROOT ، دسترسی ها انجام می گیرد .

البته داده های تکراری تا ۷۸٪در KDD دیده می شوند، بانک های اطلاعاتی ویرایش شدهNSL-KDD تا KDD۲۰۱۴ معمولا مورد استفاده طراحان IDS جدید قرار می گیرد که داده های تکراری بسیار کمتری دارند.در طراحی معمولاً از تعداد ویژگی کمتری استفاده می شوداز ویژگی هایی که بیشترین تاثیر را در خوشه بندی ایفا می کنند. نرمال سازی داده های KDD-CUP به روش پیوسته با استفاده از فرمول زیر انجام میشود .

$$xi = \frac{Xi - Xi\ min}{Xi\ max - Xi\ min} \quad (۱)$$

Xi مقدار واقعی داده، Xi min کوچکترین مقدار داده آموزشی ، Xi max بزرگترین مقدار داده آموزشی مقدار بدست آمده در محدوده [۱و۰] می باشد برای تبدیل مقادیر متنی به عددی ابتدا شماره گذاری در انواع متن استاندارد تعبیه شده انجام می دهیم ، مثلا نوع پروتکل به ۳ دسته TCP ،UDP،ICMP می باشد که شماره های ۱تا۳ را برای آنها در نظر می گیریم.[۱]

۴. داده کاوی و تشخیص نفوذ

داده کاوی برنامه های مختلف مورد نیاز برای تحلیل داده هاست. داده کاوی یک جزء مهم در تشخیص نفوذ می باشد. داده کاوی از روش های مختلف مانند طبقه بندی، خوشه، تشخیص نفوذ دور افتاده برای تجزیه و تحلیل داده های شبکه برای کشف نفوذ مورد استفاده قرار می دهد.[۱۰] داده کاوی استخراج دانش از اطلاعات می باشد. منظور از استخراج اطلاعات دستیابی به اطلاعاتی است که قبلا بدیهی نبوده وبرای ما ناشناخته بوده اند، بعد از انجام کاوش واستخراج الگوهای مفید ، ممکن است نیاز به انجام پردازش هایی روی این الگوها باشد، مجموعه این اعمال را استخراج دانش از پایگاه داده می نامند. فرایند کشف دانش متشکل از چند مرحله می باشد :

- پاکسازی داده ها
- تمامیت داده ها
- تبدیل صورت داده ها
- داده کاوی
- ارزیابی ارزش الگوها
- اکتشاف دانش

به منظور مقابله با نفوذگنندگان به سیستم ها وشبکه های کامپیوتری توسط کاربران داخلی وحمله کنندگان خارجی، روش های متعددی پیشنهاد شده است که تکنیک های تشخیص نفوذ نامیده می شوند. هدف از تشخیص نفوذ این است که استفاده غیر مجاز، سوء استفاده و آسیب رساندن به سیسیتم ها وشبکه های کامپیوتری شناسایی وبا آنها مقابله شود. [۵]

۵. یادگیری ماشین

تکنیک یادگیری ماشین توانایی محاسبه یک ماشین برای بهبود عملکرد خود براساس نتایج قبلی تعریف می شود. یادگیری ماشین شاخه ای از هوش مصنوعی است که برخی از تکنولوژی هایی را که در آنها کامپیوتر، شرایط یادگیری اتوماتیک را دارد، گسترش می دهد. یادگیری ماشین وداده کاوی هر دو با روش های آماری وتئوری دانش

کامپیوتر در ارتباط هستند. تکنیک های یادگیری ماشین در مواقعی کاربرد دارند که علمی در مورد الگوهای داده وجود نداشته باشد.[۱۴]

۶. طبقه بندی IDS براساس الگوریتم یادگیری ماشین

۱. ۶. شبکه های عصبی مصنوعی

ANN شاخه ای از هوش مصنوعی است که شبیه به سیستم عصبی انسان می باشد.قسمت عمده ANN نورون است که تابع خاص در مقادیر ورودی وخروجی را اعمال می کند. مزایای ANN در این است که می تواند داده های مبهم را تحلیل وباد بگیرد حتی اگر در داده ها بی نظمی وجود داشته باشد. در IDS، شبکه های عصبی مصنوعی برای پیش بینی رفتار یک کاربر مورد استفاده قرار می گیرند. شبکه های عصبی به عنوان یکی از تکنیک های هوشمند کاربرد زیادی در یافتن الگوها در سیستم تشخیص نفوذ دارد، هدف از کاربرد شبکه های عصبی در تشخیص نفوذ ایجاد قابلیت تعمیم از یک سری مجموعه داده ناکامل وسپس توانایی دسته بندی داده ها می باشد.[۶,۹]

سیستم های عصبی IDS طراحی شده به دو دسته تقسیم می شوند:

الف- باناظرSupervised

ب- نظارت نشده Unsupervised

نوع باناظر بادو ساختار بیان می شود:

۱- شبکه عصبی پیشخور چند لایه MLF مانند MLPوBP

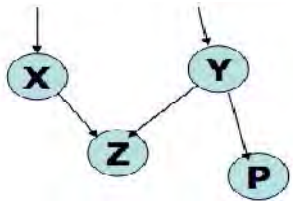
۲- شبکه عصبی بازگشتی مانند CMAC و ELMANکه با بازگشت خروجی به ورودی تغییرات انجام می گیرد.

نوع بدون ناظر :

شبکه های عصبی IDS نظارت نشده که با خوشه بندی ورودی ها وتفکیک آنها به رفتار نرمال وحمله پرداخته و می تواند حملات شناخته شده وشناخته نشده با درصد خوبی دسته بندی نماید. [۱]

۲. ۶. شبکه های بیزین

شبکه های بیزین به عنوان احتمالاتی از مدل گراف، به نمایندگی از متغیرهای تصادفی وروابط آنها مورد استفاده قرار می گیرد. هر متغیر تصادفی در یک شبکه بیزین توسط یک گره به نمایندگی وابستگی خود با لبه های بین آنها ارائه شده است.BN یا شبکه بیزین به طور گسترده در یادگیری ماشین مورد استفاده قرار می گیرد . شناخت وبیوانفورماتیک (اطلاعات زیستی) شبکه های بیزی در ترکیب با برخی از تکنیک های آماری برای شناسایی نفوذ استفاده می شود. [۱۱]



شکل۲ : شبکه بیزین

۳. ۶. مدل مارکوف

مارکوف زنجیره یک فرایند تصادفی است که در آن زنجیره ای از کیفیت وجود دارد وهر کیفیت وابسته به کیفیت قبلی است . تغییر کیفیت توس احتمالات مختلف در ارتباط با آن اداره می شود. HMM یک فرایند تصادفی دوگانه است که در آن کیفیت غیر قابل مشاهده می باشد. این تغییر در ایجاد یک زنجیره انتقال به عنوان پوسته زنجیره مارکوف

شناخته می شود. در مدل مارکوف انسجام تشخیص نفوذ ، توسط مجموعه ای از متغیرها با برخی از احتمالات وانتقال کیفیت از داده های نمونه آموزش تخمین زده می شود. در مرحله تشخیص، داده ها را بررسی وبرعلیه این احتمالات براساس یک آستانه خاص در خصوص ترافیک طبیعی وغیرطبیعی تصمیم گیری می شود. به دلیل سادگی وانعطاف پذیری آن در بسیاری ازحوزه ها، محبوبیت کسب کرده است. مارکوف زنجیره ای ، به طور گسترده برای کشف نفوذ مورد استفاده قرار می گیرد. [۸,۱۷]

۴. ۶.درخت تصمیم

یک مدل پیشگویی در یادگیری ماشین است که یک گراف با الگوی درختی وشبیه به ساختمان داده ی نمودارگردشی است . درخت تصمیم درختی است که در آن نمونه ها را به نحوی دسته بندی می کند که از ریشه به سمت پایین رشد می کندودر نهایت به گره های برگ می رسد . مهمترین واساسی ترین الگوریتم هایی که در درخت تصمیم استفاده می شود ID۳ و C۴.۵ که هر دو متعلق به ساختمان داده کاوی درخت هستند . از مزایای درخت تصمیم می توان به ۱- کارکردن با داده های بزرگ وپیچیده، ۲- استفاده مجدد آسان، ۳- قابلیت ترکیب با روش های دیگر اشاره کرد.[۵] درخت تصمیم دارای نرخ هشدار نادرست کم و نرخ تشخیص نفوذ بالایی است، ولی ایراد این روش این است که مدت زمان آموزش این الگوریتم در فاز آموزش نسبتا زیاد است بنابراین باید حجم مجموعه داده ای که در فاز آموزش برای ساخت مدل استفاده می شود کاهش یابد.[۱۲]

۵. ۶. الگوریتم ژنتیک (GA)

از کامپیوتر برای اجرای انتخاب طبیعی وتکامل تدریجی استفاده می کند. این مفهوم به معنی بقا تطبیقی در موجودات طبیعی که به صورت تصادفی از تولید یک جمعیت بزرگ شروع می شود. برخی از معیار سازگاری برای ارزیابی عملکرد هر فرد در یک جمعیت استفاده می کنند وتعداد زیادی از تکرار وسپس برنامه های اجرایی جایگزین توسط ژنتیک نوترکیب بهره می برند. به این معنی که یک برنامه با سازگاری کم برای باقی ماندن تکرار کامپیوتر بعدی حذف می شود. [۱۳]

۶. ۶. منطق فازی

یک روش محاسبات درجه ای ازحقیقت براساس منطق بولین مستقر در کامپیوترهای مدرن می باشد.[۲۰] منطق فازی با تئوری مجموعه فازی مشتق شده و می توان آن را کاربرد تئوری مجموعه فازی در رابطه با مقادیر جهان واقعی برای یک مسئله پیچیده دانست . محققان از تکنیک های داده کاوی فازی برای استخراج الگوها استفاده می کنند که رفتار نرمال برای ردیابی حمله های نفوذی را نشان می دهد .[۱۶] منطق فازی در مفهوم براساس پدیده های فازی واغلب در دنیای واقعی رخ می دهد . نظریه مجموعه فازی ارزش مجموعه عضویت برای استدلال مقادیر بین محدوده ۰ و ۱ می باشد. [۱۳]

۷. ۶. ماشین بردارپشتیبان

ماشین بردار پشتیبان یک طبقه بندی کننده دودویی است که دو کلاس را با استفاده از یک مرز خطی از هم جدا می کند . بردار پشتیبان از آموزش نمونه نزدیک به مرز تصمیم گیری است . [۱۳]ماشین بردار در دسته بندی داده ای خطی وغیر خطی کاربرد دارد. این الگوریتم از نگاشت غیرخطی برای تبدیل داده های اصلی به ابعاد بالاتر استفاده می کند. داده ها از دو کلاس توسط ابر صفحه جدا شده اند. SVM ابر صفحه را با استفاده از داده های آموزشی وحاشیه که توسط بردار پشتیبان تعریف می شود، پیدا می کند. [۷]

۷. کارهای مرتبط

با استفاده از شبکه های عصبی MLP و ART سیستم جدیدی پیشنهاد شده که کارایی موثری در تشخیص نفوذ بدون ناظر بدست آمده که نوع حمله قطع سرویس با تشخیص ۱۰۰٪ و حملات پویش در حد ۹۹.۴۸٪ و حملات U۲R ۹۹.۹٪ و در حملات R۲L ۹۹.۳ ٪ تشخیص صحیح حمله بدست آمده است . [۱]

به ارائه یک روش ترکیبی یادگیری ماشین به منظور تشخیص نفوذ می پردازد. روش ترکیبی ارائه شده مبتنی بر مفهوم کاهش ابعاد والگوریتم های درخت تصمیم وروش یادگیری می باشد که از دقت ۹۷/۱۹٪ برخوردار است. مجموعه داده های بکار رفته مجموعه NSL-KDD می باشد که نسبت به مجموعه داده های دیگر که برای سیستم تشخیص نفوذ استفاده می شود از رکورد واقعی تری برخوردار می باشد.[۲]

سیستم پیشنهادی با استفاده ازتکنیک بهره وری اطلاعات کاهش ویژگیها را با ۲۱ ویژگی انتخاب کرده و با ترکیب الگوریتم های بهبود یافته درخت تصمیم j ۴۸ و SVM وبیزین یک الگوریتم ترکیبی بر پایه الگوریتم Desition Tree ارائه گردیده است و معیار درستی آن۹۶.۲۸٪ وخطای دسته بندی به میزان۳.۷۲٪می باشد.[۴]

در این روش با استفاده از درخت تصمیم یک مکانیزم کشف نفوذ به شبکه طراحی شده است . با توجه به نتایج شبیه سازی در این روش نه تنها مدت زمان فاز آموزش کاهش یافته ، بلکه نرخ هشدار نادرست و نرخ تشخیص نفوذ نیز بهبود نسبی پیدا می کند.[۵]

یک الگوریتم ترکیبی با استفاده از ترکیب بیز ودرخت تصمیم برای تولید بهترین نرخ تشخیص با نرخ مثبت کاذب در طراحی سیستم نفوذ استفاده شده است. این ترکیب با توجه به دقت بالای آن دارای زمان اجرای طولانی جهت ساخت مدل می باشد که بزرگترین عیب این روش است.[۱۵]

این روش براساس داده کاوی ومنطق فازی می باشد . در این روش از مجموعه داده های KDD-Cup۹۹ برای ارزیابی عملکرد سیستم استفاده شده است. نتایج نشان می دهد با توجه به اینکه قواعد فازی می تواند یک مرزبندی ملایم بین اتصالات سیستم ایجاد کند ، در نتیجه الگوریتم های ردیابی نفوذ بدون منطق فازی ، دارای نرخ هشدار مثبت کمتری می باشند. سیستم پیشنهادی در این روش که براساس منطق فازی و قوانین انجمنی است ، نرخ هشدار مثبت غلط راکاهش ونرخ تشخیص نیز افزایش می دهد .[۱۶]

در بررسی های انجام شده IDS ترکیبی از مدل شبکه عصبی وبردار پشتیبان(SVM,SOM) جهت شناسایی حملات ناشناخته وتغییر ر یافته واستفاده از KDD-CUD DATASET بازدهی تشخیص صحیح درحملات Anomalyبه تنهایی در شبکه عصبی مخصوصاً درPROBE ٪۸۲/۴ وSVM ٪۸۳/۸ بوده که با ترکیب این دو روش به کارایی ۹۷/۴رسیده است[۱۹] .

نتیجه

روش های یادگیری ماشین ، سیستم های مختلف را قادر می سازد که یاد بگیرند، استنتاج کنند و به ما پیشنهاد های کاربردی ارائه دهند. با استفاده از رویکرد های یادگیری ماشین و هوش مصنوعی ، این سیستم ها قادر هستند ما را در حل مسائل مهم ، کاربردی یاری دهند. غالبا این کار با استناد واستفاده از داده هایی انجام می شودکه به دلیل حجم زیاد ویا ماهیت نامفهوم ، برای ما چندان قابل استناد نیست.با توجه به موارد ذکر شده و بالا بودن سرعت تشخیص در زمینه دقت نفوذ باید تحقیقات بیشتری صورت پذیرد.

منابع

[۱]خدابنده لو رضا ، خلیلیان مجید. سیستم تشخیص نفوذ ترکیبیART وMLP مبتنی بر شبکه های عصبی،همایش الکترونیکی پیشرفت های تکنولوژی در مهندسی برق ، الکترونیک وکامپیوتر. ۲۰۱۵،ص ۱ الی ۸

[۲]خدایار، محمد و عصاره ، علیرضا، تشخیص نفوذ در شبکه های کامپیوتری با استفاده از تکنیک های ترکیبی یادگیری ماشین، نهمین همایش ملی علوم ومهندسی کامپیوتر با محوریت امنیت ملی وتوسعه پایدار، مشهد ،۲۰۱۵

[۳]فضلی مقصودی ، حسن و مومنی ، حسین، مقایسه وبررسی الگوریتم های داده کاوی شبکه بیزین و بردار پشتیبان برای تشخیص نفوذ، هشتمین سمپوزیوم ملی مهندسی و توسعه پایدار با محوریت شبکه های کامپیوتری ، مدل سازی وامنیت سیستم ها، مشهد، ۲۰۱۴

[۴]برومندزاده مصطفی ،" ارائه یک روش ترکیبی داده کاوی و یادگیری ماشین سیستم به منظور تشخیص نفوذ در شبکه‌های کامپیوتری"، اولین کنفرانس ملی علوم مهندسی، ایده‌های نو ، ۲۰۱۴

[۵]جعفرزاده پریسا، جمالی شهرام ، افزایش نرخ کشف نفوذ به شبکه های کامپیوتری با استفاده از درخت تصمیم،مجله علمی – پژوهشی رایانش نرم وفناوری اطلاعات، جلد۱،شماره ۳، ۲۰۱۵،ص ۶۷ الی ۷۷

[٦]Cunningham R, Lippmann R, Detecting computer attackers: recognizing patterns of malicious stealthy behavior. MIT Lincoln Laboratory—presentation to CERIAS ۲۰۰۰.

*[۷]*J.Han, and M.Kamber, "*Data Mining: Concepts and Techniques*", San Diego Academic Press, ۲۰۰۱.

[۸] Mahoney, Matthew, ChanPHAD: Packet header anomaly detection for identifying hostile network, traffic. Florida Institute of Technology Technical Report CS-۲۰۰۱

[۹] Sarasamma, Suseela T., Qiuming A. Zhu and Julie Huff, Hierarchical Kohonenen net for anomaly detection in Network Security: Systems, Man, and Cybernetics, Part B: IEEE Transactions on Cybernetics. ۲۰۰۵,۳۵ (۲): ۳۰۲-۳۱۲

[۱۰]Chang-Tien Lu, Arnold P Boedihardjo,PrajwalManalwar and Falls Church."Exploiting Efficient Data Mining Techniques to Enhance Intrusion Detection Systems".IRI ۲۰۰۵ IEEE International Conference on Information Reuse and Integration Conf ۲۰۰۵.

[۱۱]Ben Gal, Irad, Bayesian Networks. Encyclopedia of Statistics in Quality and Reliability. ۲۰۰۷.

[۱۲]Sabahi, F., &Movaghar, a.. "Intrusion detection: A survey'. In Proceedings of the ۳rd International Conference on Systems and Networks Communications pp. ۲۳–۲٦, *New York, NY, USA,* ۲۰۰۸, *October.*

[۱۳]Chih-Fong Tsai, Yu-Feng Hsu, Chia-Ying Lin , Wei-Yang Lin ," Intrusion detection by machine learning: A review", journal homepage: www.elsevier.com/locate/eswa, Expert Systems with Applications ۳٦ (۲۰۰۹) pp۱۱۹۹٤–۱۲۰۰۰

[۱٤]*Ming Xue, Changjun Zhu."A Study andApplication on Machine Learning of ArtificialIntelligence". International Joint Conference on Artificial Intelligence, pp.* ۲۷۲-۲۷٤, ۲۰۰۹.

[۱٥]Panda, M., Abraham, A., Das, S., & Patra, M. R, Network intrusion detection system: A machine learning approach, Intelligent Decision Technologies, ٥(٤), ۳٤۷-۳٥٦, ۲۰۱۱.

[۱٦]G.Rajabi, J. Mirabedini," Application of fuzzy logic intrusion detection systems in computer networks", The First Regional Conference on the Advanced Mathematics and Its Applications ۲۹ *FEB-۱ MAR* ۲۰۱۲

[۱۷] Jalilzade and Jamali, ۲۰۱۳. *Modeling Based on Hidden Markovian Chain in Mobile Ad Hoc Networks.Journal of Basic and Applied Scientific Research., ۳(۱):* ٤۰-٤٤

[۱۸]Mehr Yahya Durrani, M. Taimoor Khan, Armughan Ali, Ali Mustafa۱, Shehzad Khalid" .Machine Learning:A Solution for Intrusion Detection". Journal of Basic and Applied Scientific Research, TextRoad Publication, ۲۰۱٤.pp۱۳٤-۱۳۹

[۱۹]Roshani Gaid hane ,M.Raghuwanshi "Leavnin Techigues For Intrusion Detection System (IDS)" ,ijafrc ,vol ۱, ۲۰۱٤

*[۲۰]Zamani.M , Movahedi.M, "Machine Learning Techniques for Intrusion Detection", arXiv:*۱۳۱۲.۲۱۷۷v۲ *[cs.CR]* ۹ *May* ۲۰۱٥