Archvie of SID

ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

ارتقاء یک سیستم تشخیص نفوذ ترکیبی با استفاده از شبکه‌های عصبی غیر نظارتی

سعید بخشایش خانیکی [۱]، علیرضا رحمانی [۲]، حمید رضا اسکندری [۳]

[۱] دانشگاه صنعتی امیرکبیر
bakhshayesh@aut.ac.ir
[۲] دانشگاه تربیت مدرس
e_a_rahmani@modares.ac.ir
[۳] دانشکده فنی، دانشگاه تربیت مدرس
eskandari@modares.ac.ir

چکیده

سیستمهای تشخیص نفوذ ابزارهایی هستند که برای شناسایی تهدیدات شناخته شده یا بالقوه در ترافیک شبکه یا داده‌های ذخیره شده بکار می‌روند. توسعه ابزارهای حمله و دسترسی آسان هکرها به آسیب پذیرهای[۱] سیستمها و نرم افزارها، به آنها این امکان را داده است تا بتوانند حملات پیچیده را به راحتی و درکوتاهترین زمان و با دانش کمتر به انجام رسانند. اگر چه سیستمهای تشخیص نفوذ موجودبی عیب و نقص نمی باشند، اما یک جزء مهم و اساسی در تشکیل دیوارهای دفاعی سیستمهای اطلاعاتی یک سازمان و شناسایی حملات به شمار می‌آیند. در این مقاله از روشهای تشخیص ناهنجاری[۲] و هم تشخیص سوء استفاده[۳] که مبتنی برشبکه‌های عصبی غیر نظارتی و درخت تصمیم‌گیری می‌باشند در سیستم پیشنهادی استفاده شده است. مزیت این روش استفاده از دو ماژول به منظورتشخیص نفوذ است که این موضوع باعث کاهش درصد خطای ناشی از تشخیص نفوذ اشتباه [۴] و افزایش سرعت تشخیص نفوذ [۵] می‌شود.

واژه‌های کلیدی

تشخیص ناهنجاری، تشخیص سوء استفاده، سیستمهای پشتیبان تصمیم‌گیری[۶]، نگاشت خود سازمانده[۷]، تشخیص نفوذ هیبرید، درختهای تصمیم گیری[۸]

[1] Vulnerability
[2] anomaly detection
[3] misuse detection
[4] false positive
[5] Detection Rate
[6] Decision Support System
[7] Self Organization Map
[8] decision trees

www.SID.ir

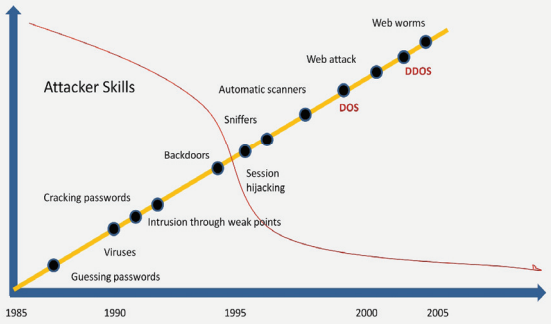
Archive of SID

۱- مقدمه

امروزه با پیشرفت تکنولوژی و رشد فناوری اتصال داخلی بین سیستمهای کامپیوتری بسرعت در حال رشد می‌باشد و امنیت شبکه بعنوان یک چالش اصلی مطرح است شبکه‌های کامپیوتری برضد حملات، افشای بدون مجوز اطلاعات و دستکاری و خرابکاری اطلاعات باید محافظت شده و میزان دسترسی، قابلیت-اعتماد و یکپارچگی سیستمهای دارای اطلاعات حیاتی، باید تامین شود [1].

نمودار ۱ از یک طرف انواع حملات و میزان آنها را از سالهای ۱۹۸۵ تا ۲۰۰۵ نشان می‌دهد و از طرف دیگر این نمودار نشان می‌دهد که باگذشت زمان، نیاز به وجود مهارتهای خاص برای حمله و نفوذ، کاهش یافته و علت آن نیز ابزارهایی است‌که امکان نفوذ را به راحتی برای نفوذگران فراهم می‌کنند.

حمله‌های توزیع شده اختلال در سرویس دهی[1] جایگاه ویژه‌ای در روند افزایشی تهدیدات سالهای اخیر درمیان دیگر تهدیدهای



اینترنتی داشته‌است.

نمودار ۱: توسعه حمله ومهارت حمله کنندگان

یک سیستم تشخیص نفوذ یک سیستم دفاعی است که تلاش می‌کند تا نفوذهای به شبکه و حملات روی سیستمهای رایانه‌ای را شناسایی کند. تشخیص نفوذها حملات را بوسیله انتخاب و تحلیل ترافیک شبکه و با استفاده از انواع گوناگونی از روش‌های موثر مانند: تکنیک‌های یادگیری ماشین (SVM[2]، RBF[3]، نگاشت خود خود سازمانده، Artificial Immune system و درختهای‌تصمیم گیری) شناسایی می‌کنند.

سیستمهای تشخیص نفوذ موجود بر اساس روشهای تشخیص به دو دسته طبقه بندی می‌شوند :

۱-تشخیص ناهنجاری

۲-تشخیص سوء استفاده یا تشخیص اثر و ردپا

تشخیص ناهنجاری روشی برای تشخیص نفوذها با استفاده از یادگیری اولیه می‌باشدکه بتوانند با یادگیری اولیه‌ی مدل رفتار و مشخصات و ویژگی‌های رفتارهای نرمال، دست به تشخیص الگوهای رفتاری غیرنرمال بزنند. در نتیجه هر رفتاری که دارای ناهنجاری از مدل اولیه باشد به عنوان رفتار غیرعادی[4] در نظر می‌گیرد. مهمترین عیب این رویکرد ایجاد تعداد زیادی اعلام تشخیص نفوذ اشتباه است. در مقابل نوع تشخیص سوءاستفاده سعی می‌کنند فعالیت کامپیوتر را با اثرات حملات یا دستکاریهای معلوم ذخیره شده مطابقت دهند. بعبارت دیگر سیستمهای تشخیص سوء استفاده از دانش قیاسی نسبت به حملات برای جستجوی ردپاها استفاده می‌کنند.در نتیجه این روش برای مقابله در برابر حملات ناشناخته نا کارآمد است، زیرا اثرات حملات در این روش باید به صورت دستی بروزرسانی شوند.

یک سیستم تشخیصی نفوذ می‌تواند به سه نوع طبقه‌بندی شود : تشخیص نفوذ مبتنی بر میزبان، تشخیص نفوذ مبتنی بر شبکه و تشخیص نفوذ هیبرید [2].

تشخیص نفوذ مبتنی بر میزبان الگوی رفتاری نرمال کاربر را که عامل تشخیص نفوذ مبتنی بر میزبان می‌باشد را ارزیابی می‌کند در دستگاههای میزبان بصورت نرم افزاری گسترش داده می‌شود. تشخیص نفوذ مبتنی بر شبکه، بسته‌هایی که در شبکه جریان دارند را بررسی می‌کنند. تشخیص نفوذ هیبرید از هردو روش استفاده می‌کند.

در این تحقیق، یک سیستم تشخیص نفوذ هیبریدی که از هر دو-نوع تشخیص ناهنجاری و سوءاستفاده بهره می‌بردارائه می‌شود مطلب اصلی این نوشتار توجه به عملکرد معماری تشخیص‌نفوذ هیبرید ارائه شده با استفاده‌از KDD Cup 99 است‌که این مجموعه داده‌ها توسط محققان تشخیص نفوذ تست وجمع آوری شده است [3].

این معماری سیستم تشخیص نفوذ هیبرید از ماژول تشخیص ناهنجاری، ماژول تشخیص سوء استفاده و یک ماژول کنترل به عنوان پشتیبان و تصمیم گیرنده که ترکیب نتایج این بلوک تشخیص می‌باشد تشکیل شده است.

هرچند هیچیک از این سیستم‌های دفاعی کامل نیستند و نفوذگران نیز پیوسته در حال تلاش برای طراحی حملات پیچیده‌تر برای گمراه نمودن سیستم‌های تشخیص هستند پژوهشگران زیادی به کارگیری شبکه‌های عصبی مصنوعی[5] را برای برای ایجاد تشخیص نفوذ اتوماتیک پیشنهاد و بررسی نموده اند. به طور سنتی شبکه‌های عصبی به دو دسته‌ی نظارتی[6] و غیر نظارتی[7]

[1] Distributed Denial of Service
[2] Support Vector Machine
[3] Radial Basis Function
[4] anomalous
[5] Artificial Neural Network
[6] Supervised

www.SID.ir

Archvie of SID

نظارتی[1] طبقه‌بندی می‌شوند و هر دو این دسته‌ها پس از آموزش شبکه با مشخصات و ویژگی‌های ترافیک شبکه می‌توانند برای تشخیص حملات به کار گرفته شوند. شبکه‌های عصبی نظارتی برای داشتن عملکرد مناسب در محیط‌های پویا نیازمند به بازآموزی پیوسته هستند، در حالی‌که شبکه‌های عصبی غیر نظارتی توانایی بهبود پویای عملکرد خود در محیطی متغیر با زمان را دارند. به علاوه ثابت شده که شبکه‌های عصبی غیر نظارتی به لحاظ محاسباتی سریعتر از نوع نظارتی هستند از این مهمتر، دارای زمان پاسخ‌دهی کوتاه‌تری در فاز به کارگیری می‌باشند. بیشتر شبکه‌های عصبی غیر نظارتی که تا به امروز برای یادگیری رفتار و ویژگی‌های نرمال و یا غیر نرمال ترافیک شبکه به کار گرفته شده‌اند از نوع نگاشت خود سازمانده بوده‌اند. نگاشت خود سازمانده یک الگوریتم خوشه‌بندی مشهور غیرنظارتی است که به طور گسترده‌ای برای سازماندهی داده‌هایی با ابعاد ورودی بالا و نگاشت آن به فضای خروجی با ابعاد کوچکتری باشد. در سال ۲۰۰۲ محققان شبکه نگاشت خود سازمانده دو لایه‌ی سلسله مراتبی را برای مساله تشخیص نفوذ به منظور بررسی اطلاعات نشست کاربران در یک سیستم UNIX به کار گرفته‌اند[4]. درسال ۲۰۰۳روش دیگری با نگاشت خود سازمانده چند لایه‌ی سلسله مراتبی برای مساله تشخیص نفوذ ارائه شده است که در مقایسه با دیگر روشهای ارائه شده، از کارایی بیشتری برخورداراست دراین روش با استفاده از بخش کوچکی از مجموعه ویژگی‌ها، شش ویژگی اصلی، بررسی وتشخیص نفوذ بر اساس آنها صورت می‌گیرد [5]. در سال ۲۰۰۵ نیز روش دیگری با نگاشت خود سازمانده چند لایه‌ی سلسله مراتبی ارائه داده‌اند که در آن هر لایه وظیفه بررسی ویژگیهای مشخصی را بر عهده داشته و نسبت به شناسایی بخشی از حملات اقدام می‌نماید[6]. در سال ۲۰۰۵ محققان روش معماری ترکیبی ارائه نموده اند که دو نوع تشخیص ناهنجاری و سوء استفاده را به کار گرفته است. آنها از نگاشت خود سازمانده برای مدلسازی رفتار نرمال برای طبقه‌بندی نمودن انواع متنوعی از حملات استفاده نموده‌اند[7] . در سال۲۰۰۶ سیستم تشخیص نفوذ مرکبی به نام RT_UNNID ارائه نموده‌اند و در آن (عملکرد) سه نوع متفاوت طبقه‌بندی کننده غیرنظارتی، نگاشت خود سازمانده و دو گونه مشتق از (ART)[2]، را ارزیابی نموده‌اند[8] برای تشخیص نفوذ ناهنجاری درسال ۲۰۰۲ از شبکه‌های غیر نظارتی با نگاشت هندسی برای پردازش اطلاعات بدون برچسب‌گذاری و تشخیص نقاط واقع شده در نواحی تنک فضای ویژگی‌ها به عنوان ناهنجاری استفاده نموده اند [9].

[1] Unsupervised

[2] Adaptive Resonance Theory

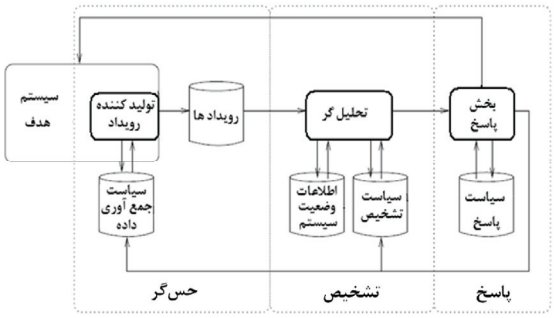
۲- برخی چالشها در سیستم‌های تشخیص نفوذ

هر یک از روش‌های تشخیص نفوذ دارای مزایا و معایب خاص خود هستند و سیستم تشخیص نفوذ به تنهایی یک راه حل امنیتی کامل و جامع نیست. در ادامه به صورت فهرست‌وار، برخی از چالش‌های موجود در زمینه سیستمهای تشخیص نفوذ ارائه می‌شود:

- حملات بسیار جدید[3]
- همبستگی وارتباط وانتخاب داده‌ها[4]
- ترافیک عبوری رمزنگاری شده
- IPv6
- حمله نفوذ یا حمله قطعه قطعه کردن بسته‌های شبکه[5]
- حمله از نوع Evasion یا TCP Reassembly
- حمله ممانعت از سرویس
- حمله ممانعت از سرویس توزیع شده[6]
- کارایی بسیار ضعیف در سرعت‌های بسیار زیاد
- اشتباهات یا نقایص ناشی از خطای پیکربندی یا اشتباه در ایجاد الگوهای امضای حملات توسط نیروی انسانی

۳- ارائه روش پیشنهادی

در این مقاله، یک سیستم تشخیص نفوذ هیبریدی که ترکیبی از دو نوع معماری تشخیص نفوذ (تشخیص ناهنجاری و سوء استفاده) بهره می‌برد ارائه می‌شود دراین روش به منظور تشخیص نفوذ ازسه ماژول استفاده شده است در فاز اول از مجموعه داده KDD 99 به منظور آموزش و یادگیری شبکه عصبی استفاده شده است. بعد از آموزش با استفاده از ابزارهای داده کاوی ترافیک شبکه استخراج و جهت تجزیه و تحلیل وارد ماژول‌های مورد نظر می‌شود. به طور کلی اجزای اصلی یک سیستم تشخیص نفوذ به صورت شکل ۱ می‌باشد.



شکل۱: اجزای یک سیستم تشخیص نفوذ

[3] Zero-day

[4] Data collection and correlation

[5] IP Fragmentation Attack or Insertion Attack

[6] Distributed Denial-of-Service Attack

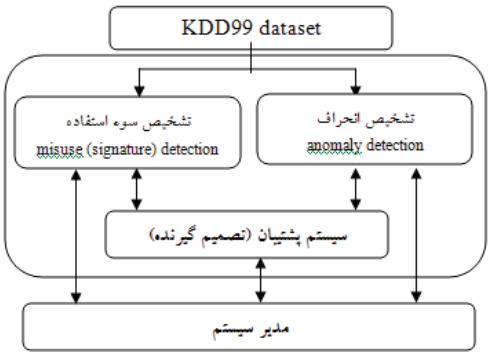
www.SID.ir

Archive of SID

همانطور که در شکل ۲ نشان داده شده، معماری تشخیص نفوذ ارائه شده از یک ماژول تشخیص ناهنجاری، یک ماژول تشخیص سوء استفاده و یک سیستم پشتیبان تصمیم گیری که ترکیب نتایج این دو ماژول تشخیص می‌باشد تشکیل شده است. مزیت این روش استفاده از دو ماژول به عنوان تشخیص نفوذ است که این موضوع باعث کاهش درصد خطای ناشی از تشخیص نفوذ اشتباه وافزایش سرعت تشخیص نفوذ می‌باشد مزیت دیگر این روش نسبت به روشهای مشابه [7] استفاده از پیش پردازنده در بخش تشخیص نفوذ وتعیین نوع پروتکل ارتباطی دربخش پیش پردازنده و اعمال داده‌های مورد نظر باتوجه به نوع پرتوکل به لایه‌های زیرین است با انجام این روش به جای تحلیل کل داده‌های ورودی تنها تحلیل بر اساس نوع سرویسهای شبکه صورت گرفته و باعث افزایش سرعت پردازش وکاهش حجم حافظه مورد نیاز جهت تجزیه و تحلیل می‌گردد.

۳-۱ ماژول تشخیص ناهنجاری

تشخیص ناهنجاری، بخش کلیدی تشخیص نفوذ می‌باشد که در آن رفتارغیر نرمال دلالت بر وجود حملات یا خطاهای عمدی یا سهوی تحریک شده دارد. روشهای تشخیص ناهنجاری براساس ایجاد مدلهای داده‌های نرمال و کشف میزان انحراف صورت گرفته از مدل نرمال در داده‌های ورودی می‌باشند. الگوریتمهای تشخیص ناهنجاری این مزیت را دارند که می‌توانند انواع جدید نفوذها را بعنوان ناهنجاری از مدل نرمال کشف کنند.



شکل ۲: معماری سیستم تشخیص نفوذ هیبریدی

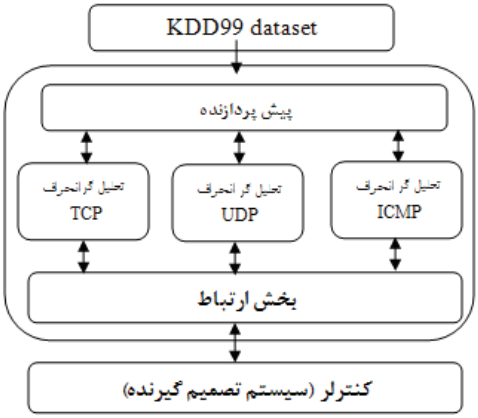
در این مقاله، هر رکورد اتصال بررسی شده و ویژگیهای ترافیک استخراج می‌شوند. هدف الگوریتمهای تشخیص نفوذ، آموزش سیستم با داده‌های نرمال و مدلسازی ترافیک شبکه با مجموعه داده‌های نرمال موجود خواهد بود سپس وظیفه بعدی تعیین این مطلب می‌باشد که آیا داده‌های تست در یک داده تست جدید متعلق به رفتار نرمال هستند یا غیر نرمال. ماژول تشخیص ناهنجاری ارائه شده از سه بخش تشکیل شده است.

۱ – بخش پیش پردازنده

۲ – بخش‌های تحلیل‌گر ناهنجاری

۳- بخش ارتباطی

بخش تحلیل‌گر (تحلیل‌گر ناهنجاری TCP [1]، تحلیل‌گر ناهنجاری UDP [2]، تحلیلگر ناهنجاری ICMP [3]) از الگوریتم نگاشت خود سازمانده به منظور ساختن پروفایلهای ترافیک نرمال استفاده می‌کند از پروفایل ساخته شده در ماژول تحلیل‌گر ناهنجاری به منظور تعیین اینکه اتصال شبکه نرمال است یا غیر نرمال استفاده خواهد شد. بخش ارتباط، به منظور ارتباط با بخش سیستم پشتیبان تصمیم گیری (DSS) استفاده شده است. شکل ۳ بلوک دیاگرام ماژول تشخیص ناهنجاری را نشان می‌دهد.



شکل ۳: بلوک دیاگرام معماری ماژول تشخیص انحراف

۳-۱-۱ پیش پردازنده

مجموعه‌داده KDD 99 که بوسیله مسابقه بین المللی ابزارهای داده کاوی و کشف دانش تولید شده است. معیار قابل قبول موجودبرای ارزیابی روشهای پیشنهادی‌درزمینه‌هوش محاسباتی - می‌باشد که برای مسئله تشخیص نفوذ بکار می‌روند.[2]

این مجموعه داده‌ها شامل ۲۴ نوع حمله شناخته شده مختلف در داده‌های آموزشی و همچنین ۱۴ نوع حمله ناشناخته اضافی دیگر است که فقط در داده‌های تست گنجانده شده اند.کل این حملات به ۴ دسته زیر قابل تقسیم می‌باشند.

۱-حملات انکار سرویس(DOS): که در آن درخواستهای مشروع کاربر به دلیل اعمال بار بیش از حد توان پاسخگویی سیستم برآورده نمی شوند.

۲-حملات از راه دور(R2L) : که در آن از یک ماشین راه دور دسترسیهای غیرمعتبر به یک سیستم محلی صورت می‌پذیرد.

[1] Transmission Control Protocol
[2] User Datagram Protocol
[3] User Datagram Protocol

www.SID.ir

Archvie of SID

۳-حملات کاربر به ریشه(U2R) :که در آن با تصاحب مجوزهای کاربر ریشه، دسترسیهای غیر معتبر و غیر مجاز به سیستم صورت می‌پذیرد.

۴- حملات پویش (Probe): که شامل بررسی و پویش بر روی سیستم برای یافتن راههای نفوذ به آن می‌باشد.

به هر حال در مقالات به چندین اشکال اساسی این مجموعه داده اشاره شده است. در سال ۲۰۰۴ نشان دادند که از موانع و محدودیتهای این مجموعه داده این است که نباید برای آموزش الگوریتمهای یادگیری ماشین برای شناسایی حملات ناشی از سوءاستفاده از نوع (U2R) [1] و (R2L)[2] استفاده گردد.

آنها بررسی گسترده‌ای‌را انجام دادند که نشان دهنده این مسئله بود که هیچ الگوریتم یادگیری‌ماشینی در صورتی که از مجموعه داده مذکور برای فرآیند آموزش آن استفاده شده باشد، قابلیت شناسایی حملات R2LوU2R را نخواهد داشت. [10] همچنین تاکنون کارهای محدودی برای ارائه یک مبنای دیگر به جز KDD انجام شده است.

در این مقاله به منظور بررسی رفتار کاربران از ۶ ویژگی اصلی استفاده شده که عبارتند از: [11]

۱ - مدت اتصال

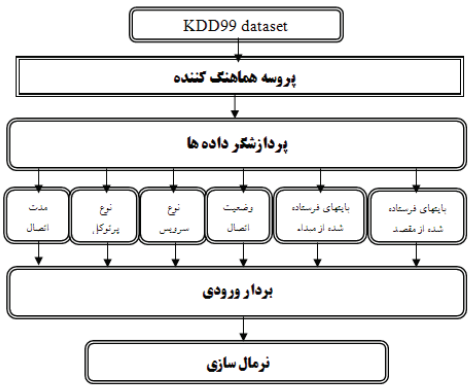
۲ – نوع پروتکل از قبیل TCP,UDP,ICMP

۳ – نوع سرویس از قبیل FTP, HTTP, Telnet

۴ – پرچم وضعیت اتصال

۵ – کل بایتهای فرستاده شده به مقصد

۶ – کل بایتهای فرستاده شده به مبدا



شکل ۴: بلوک دیاگرام پیش پردازشگر

درشکل ۴ نحوه مدل‌سازی رفتار هر کاربر برای تشخیص نفوذ نمایش داده شده است. پروسه هماهنگ کننده مسئول برچسب‌گذاری اطلاعات سیستم به شبکه‌های عصبی است. هر کدام از این مشخصه‌های رفتاری هم توسط شبکه نگاشت خود سازمانده مدلسازی شده و هم توسط یک فیلتر استاتیک محدود چک می‌شود. اطلاعات بدست آمده از logهای سیستم برای فیلتر کردن توسط پیش پردازشگر (شکل ۳) با جداکردن داده‌های منتخب از داده‌های ممیزی استفاده می‌شوند. قبل از پردازش بردار ورودی، لازم است داده‌های ورودی نرمالیزه شوند. ورودی شبکه عصبی یک بردارداده است که دربردارنده ۶ ویژگی می‌باشد بمنظور آموزش معماری نگاشت خود سازمانده چندین مرحله نرمال‌سازی ضروری است. نگاشت خود سازمانده معمولا بطور مستقل رفتار می‌کند و روی متغیرهای نرمالیزه شده عددی کار می‌کند. بنابراین متغیرهای کاراکتری در مجموعه داده باید شمرده شده و سپس همگی نرمالیزه شوند. در مرحله اول نوع پروتکل ارتباطی با توجه به سرویس شبکه مشخص و در مرحله بعد بر این اساس ویژگیهای ذکر شده در تحلیل‌گر مورد نظر دسته بندی شده که ساختار نگاشت خود سازمانده در هر ویژگی مستقل عمل می‌کند هر نمونه از یک کاراکتر به مقادیر صحیح متوالی نگاشته می‌شوند. به عنوان نمونه مدت اتصال، نوع پروتکل، نوع سرویس وپرچم وضعیت اتصال، کاراکتری هستندو بعداز عملیات شمارش، نرمال‌سازی انجام می‌شود. هدف از نرمال‌سازی داده‌ها آن است که هیچ کدام از مولفه‌های بردارهای ورودی تاثیری روی نتیجه آموزش نداشته باشند. نرمال‌سازی استاندارد [1 0] در این جا استفاده می‌شود. نتایج پیش شبیه‌سازی آموزش نگاشت خود سازمانده با استفاده از نرمال‌سازی [1 0] یا [1 -1] نتایج قابل قبولی ارائه نمی‌کنند. چون ویژگیهای عددی (مانند مدت اتصال، کل بایتهای اختصاص داده شده به میزبانهای مبدا / مقصد) بردار ویژگی اتصال مقادیری با طیف دینامیک دارند.

همانطورکه ویژگیهای اتصال نرمالیزه شدند مقادیر ویژگیها نزدیکتر شده و نمی توانند توسط ساختار نگاشت خود سازمانده مشخص‌گردند. برای مثال در حملات DoS، مقدار بایتهای مقصد ۰ و مقدار بایتهای مبدا ۴۰- ۵۰ بایت می‌باشند. به هر حال در اتصالات نرمال هر دو ویژگی ۴۰-۵۰ بایت دارند. برای این مورد اگر یک نرمال‌سازی [1 0] انجام شود داریم

$$50/5000000 = 10^{-5} \quad and \quad 0/5000000 = 0$$

ما دو مقدار خیلی نزدیک داریم. این دو مقدار ممتاز، نمی‌توانند توسط ساختار نگاشت خود سازمانده از هم تشخیص داده شوند. اگر ۴ پارامتر باقی مانده یکسان باشند که اغلب در حملات DoS اینگونه است، این نوع حملات بعنوان اتصالات نرمال تفسیر می‌شوند و نمی توانندمشخص شوند. بنابراین این دو پارامتر (بایت مبدا و بایت مقصد) باید مفصل تر بررسی شوند. برای انجام این کار، برای هر دو پارامتر اتصال، الگوریتم k-means که مثل

[1] User-to-Root

[2] Remote to local

www.SID.ir

Archive of SID

نگاشت خود سازمانده یک الگوریتم یادگیری غیر نظارتی می‌باشد استفاده می‌شود

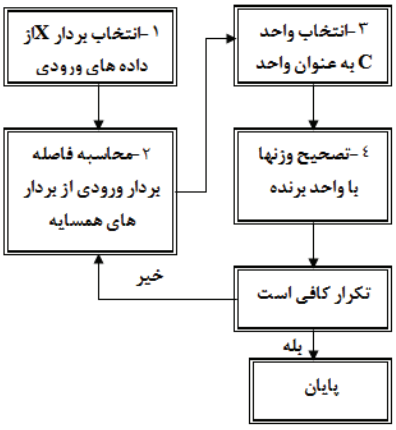
بعنوان یک نتیجه، برای هر مقدار بایت منبع، احتمالات متعلق بودن به هر مرکز خوشه محاسبه می‌شود. با استفاده از روش فوق، مشکل نرمالیزه کردن که در بالا تعریف شد حل می‌شود بنابراین مقدار بایت منبعی که تشخیص آن بعد از نرمالیزه‌سازی سخت است می‌تواند توسط ساختار نگاشت خود سازمانده تفکیک شود. حال طول پارامترهای اتصال۱۶ می‌شود.

۳-۱-۲ تحلیل‌گر ناهنجاری

باتوجه به نوع پرتوکل ارتباطی که توسط ماژول پیش پردازنده مشخص گردید است ماژول تحلیل‌گر ناهنجاری مورد نظر فعال می‌گردد این حالت باعث می‌شود دیگر نیازی به تحلیل کل داده‌های ورودی نباشد هرچند این موضوع باعث از بین رفتن قابلیت شناسایی برخی از سناریوهای ترکیبی می‌شود لیکن وجود ماژول تشخیص سوء استفاده این مشکل را تا حدی کاهش می‌دهد.

در این روش باتوجه به اینکه هر ماژول تحلیل‌گر ناهنجاری (تحلیل‌گر ناهنجاری TCP، تحلیل‌گر ناهنجاری UDP، تحلیل‌گر ناهنجاری ICMP) داده‌های مربوط به خود را تجزیه وتحلیل می‌نماید، سرعت پردازش افزایش وفضای حافظه مورد نیازکاهش می‌یابد.

هر ماژول تحلیل‌گر ناهنجاری از الگوریتم نگاشت خود سازمانده برای ایجاد پروفایلهای رفتار نرمال استفاده می‌کند. هر ساختار نگاشت خود سازمانده با داده‌های ترافیک نرمال متناظرآموزش داده می‌شود و پروفایل رفتار نرمال مدل‌سازی می‌شود. فرض ما این است که ترافیک نرمالی که بیانگر رفتار نرمال است حول یک یا چند مرکز خوشه روی شبکه نگاشت خود سازمانده خوشه بندی می‌شود و هر ترافیک غیر عادی که بیانگر رفتار غیرعادی و یا احتمالا مشکوکی است باید خارج از خوشه بندی نرمال یا داخل خوشه بندی نرمال با خطای کوانتیزاسیون بالا تقسیم بندی شود. پس پروفایلی که از داده‌ها ساخته شده برای تعیین اینکه آیا یک اتصال شبکه نرمال است یا غیر نرمال استفاده می‌شود (شکل۵).



شکل ۵: خلاصه الگوریتم SOM

۳ –۲ ماژول تشخیص سوء استفاده

تکنیک تشخیص سوء استفاده با مقایسه فعالیتهای کاربر با رفتارهای شناخته شده حمله کننده‌هایی که تلاش می‌کنند به سیستم نفوذ کنند درگیر است. تکنیکهای تشخیص سوء استفاده بیشتر اوقات از روش مبتنی بر قاعده بهره می‌برد وقتی تشخیص سوء استفاده اعمال شود این قواعد برای حملات شبکه‌ای بصورت یک روال در می‌آید. دراین مکانیسم تشخیص نفوذ اگر فعالیتهای کاربر با قواعد ایجاد شده سازگار باشد یک حمله بالقوه را تعیین می‌کند. استفاده از قواعد فراگیر در کاربرد سیستمهای خبره برای تشخیص نفوذ حیاتی است. در روش تشخیص سوء استفاده، یک حمله و مشخصه‌های آن حمله که این حمله را از داده‌های نرمال یا ترافیک تمیز می‌دهد تعریف می‌شوند. این مشخصه‌ها بعنوان اثرات یک حمله شناخته می‌شوند و این اثرات بخشی از مجموعه داده اثرات حمله می‌شوند. وقتی سیستم تشخیص نفوذ یکی‌از این اثرات را کشف می‌کند یک آلارم ایجاد می‌شود تشخیص نفوذ سوء استفاده نیاز به این دارد که حمله قبل از اینکه بتواند اجرا شود مورد بررسی قرارگیرد. سیستمهایی که توسط یک سیستم محافظت شده‌اند تا زمانی که پایگاه داده تشخیص نفوذ بروزسانی نشده، نسبت به حملات جدید آسیب پذیر هستند. بنابراین یک مکانیسم هیبریدی که تشخیص ناهنجاری و تشخیص سوء استفاده را تجزیه وتحلیل می‌نماید برای دفع اغلب حملات در یک شبکه تحت نظارت مورد انتظار است.

در اینجا ازنوعی‌الگوریتم درختی تصمیم گیری بعنوان ماژول تشخیص سوء استفاده می‌شود. قواعدی که از این درخت تصمیم‌گیری تولید می‌شوند برای طبقه بندی حملات مورد استفاده قرار می‌گیرند.

www.SID.ir

Archvie of SID

۳-۲-۱ درختهای تصمیم گیری برای فراگیری تحت نظارت

الگوریتم‌های درختی تصمیم گیری الگوریتم‌های فراگیری تحت نظارت هستند که بطور بازگشتی داده‌ها را براساس مشخصه‌هایشان شاخه بندی می‌کنند تا زمانی که شرایط توقف بوجود آید این شاخه بندی بازگشتی تحت یک ساختار شبیه درخت عمل می‌کند. هدف‌شاخه بندی نهایی است برگ درخت‌ها با توجه به کلاسهایشان همگن هستند و شاخه‌های داخلی درخت تصمیماتی در باره مشخصه‌هایی است که برای رسیدن به برگها استفاده شده‌اند. این‌تصمیم‌گیریها معمولا تستهای مشخصه ساده هستند که از یک مشخصه در یک زمان برای تمیز قائل شدن داده‌ها استفاده می‌کنند.

داده‌های جدید می‌توانند با تبعیت از شرایط تعریف شده در پایین شاخه‌ها دسته بندی شوند روش پیاده‌سازی در حوزه درخت تصمیم گیری C4.5 است. بسته دسته بندی کننده Weka نسخه C4.5 خودش را دارد که به J48 معروف است. Weka کد جاوایی است که توسط محققان دانشگاه وایکاتودر نیوزیلند ثبت شده است [12].

الگوریتم فوق برای داده‌های آموزش اعمال می‌شود. درخت تصمیم گیری ایجاد شده معمولا روی مجموعه داده‌ها تست و آزمایش می‌شود و یک مورد را فراهم می‌کند. اگر داده تست موجود نباشد j48 یک اعتبارسنجی مقطعی را با استفاده از داده‌های آموزش انجام می‌دهد و یا مجموعه داده‌ها را به ۳ بخش داده‌های آموزش، داده‌های اعتبارسنجی و داده‌های تست تقسیم می‌کند. مهمترین پارامتر الگوریتم درخت تصمیم گیری J48، مقدار اطمینان است. این مقدار وقتی در حال هرس کردن درخت هستیم استفاده می‌شود. (حذف شاخه‌هایی که تصور می‌شود هیچ بهره یا حداقل بهره‌ای در دقت آماری مدل دارند). مقدار پیش فرض آن ۲۵% است که در اغلب موارد بخوبی کار می‌کند اما قابل اصلاح می‌باشد. به هر حال اگر نرخ خطای حقیقی روی داده‌های واقعی (یا نرخ خطا روی اعتبار سنجی مقطعی) بطور قابل ملاحظه‌ای بزرگتر از نرخ خطا روی داده‌های آموزش باشد، فاکتور اطمینان می‌تواند برای ایجاد هرس قوی تر و جامع تر شدن مدل داده‌ها کاهش داده شود. اگر یک مدلسازی خاص‌تر مبتنی بر داده‌های آموزش مورد نیاز باشد، فاکتور اطمینان می‌تواند افزایش داده شود که در این صورت میزان هرس کردن کاهش خواهد یافت.

۳-۳ماژول پشتیبان وتصمیم گیری

ماژول پشتیبان و تصمیم گیری قاعده مند (DSS) نسبت به تفسیر نتایج ماژولهای تشخیص ناهنجاری و سوء استفاده پاسخگوست ماژول نهایی ارائه شده در معماری فعالیت تشخیص نفوذ را برای کاربر انتهایی گزارش می‌کند. انواع مختلف ماژول پشتیبان و تصمیم گیری قاعده مند می‌توانند برای انجام این کار پیاده‌سازی شوند. ماژول پشتیبان و تصمیم گیری قاعده مند مبتنی برقاعده‌که در این مقاله استفاده شده از قواعد کاربری ساده برای تصمیم گیری تشکیل شده است. این براساس قواعد ابتکاری تعریف شده توسط کاربرنهایی می‌باشد. مهمترین مزیت آن عبارتست از اینکه ساده و سریع می‌باشد. مجموعه قواعد متعددی قابل تعریف هستند. قواعدی‌که در این ماژول استفاده می‌شوند در زیر مطرح خواهند شد.

۳-۳-۱ قواعد

۱ – اگر ماژول ناهنجاری حمله‌ای را کشف کند و ماژول سوء استفاده نیز حمله‌ای را کشف کند آنگاه آن، حمله بوده و ماژول سوء استفاده این حمله را طبقه بندی خواهد کرد.

۲ - اگر ماژول ناهنجاری حمله‌ای را کشف نکند و ماژول سوء استفاده حمله‌ای را کشف کند آنگاه آن، حمله بوده و ماژول سوء استفاده این حمله را طبقه بندی خواهد کرد.

۳- اگر ماژول ناهنجاری حمله‌ای را کشف کند و ماژول سوء استفاده حمله‌ای را کشف نکند آنگاه آن، حمله بوده و بعنوان یک حمله غیر طبقه بندی شده تعریف می‌شود.

۴- جمع‌بندی و نتیجه‌گیری

با توجه به اینکه حجم انبوهی‌ازداده‌ها وگزارشات‌درسیستمهای اطلاعاتی تولیدوانبار می‌شود یافتن روشی که با استفاده ازداده کاوی بتواند در تحلیل این حجم زیاد داده‌ها و در نهایت تشخیص نفوذوآسیب‌پذیریهای‌سامانه‌ها موثرواقع شوداهمیت فراوانی دارد. از جمله محدودیتهای استفاده از شبکه‌های عصبی در تشخیص وجلوگیری از نفوذ عبارتند از:

- محدود وغیر واقعی بودن مجموعه داده‌های تست
- عدم امکان شناسایی حملات خیلی جدید وعدم امکان بروزرسانی فوری سیستمهای تشخیص نفوذ
- عدم شناسایی بسته‌های رمز شده
- عدم امکان پاسخگویی مناسب در سرعتهای بالا وروی بسترهای پرترافیک
- محرمانه بودن بسیاری از دستاوردها از جنبه دفاعی وتجاری

در این روش پیشنهادی استفاده از دو ماژول به عنوان تشخیص نفوذ باعث کاهش درصد خطای ناشی از تشخیص نفوذ اشتباه ونیز افزایش‌نرخ تشخیص نفوذ و افزایش سرعت تشخیص نفوذ (بدلیل استفاده از پیش پردازنده) خواهد شد. مشاهده می‌گردد که روش

www.SID.ir

Archive of SID

هیبریدی ارائه شده عملکرد بهتری را نسبت به روشهای انفرادی ازخود نشان می‌دهد.

۵- کارهای آینده

مهمترین مساله درشبکه‌های عصبی غیر نظارتی با یادگیری (آموزش) online یا life-long مشکل نحوه مواجه با سازگاری(تطبیق‌پذیری با محیط) در مقابل پایداری است. شبکه‌های عصبی سنتی یکی از دو راهکار زیر را برای مواجه با این مشکل انتخاب می‌کنند: یا از دانش آموخته شده در گذشته بهره می‌جویند (حالت شبکه پایدار) و یا در محیط‌های در حال تغییر به سرعت خود رابا الگوی جدید ورودی منطبق می‌کنند (حالت شبکه تغییرپذیر و قابل تحول و تغییر). شبکه‌های پایدار توانایی یادگیری موثر الگوهای جدید را ندارند، در حالیکه شبکه‌های تغییرپذیر و قابل تحول و تغییر نیز دانش آموخته شده قبلی را از یاد می‌برند یا فرم قابل استفاده بودن آن را از بین می‌برند. در نتیجه برای اینکه بتوان به نحوه مناسبی مساله تشخیص نفوذ را آدرس‌دهی نمود، نیازمند توسعه‌ی یک یادگیر life-long با توانایی یادگیری الگوهای جدید هستیم که در عین حال دانش قبلی بدست آمده را نیز از دست ندهد و حفظ نماید. ما بر این باوریم که هر الگوریتم خوشه‌بندی غیرنظارتی که نتواند به صورت مناسبی یادگیری life-long با اثر تخریبی کم در یادگیری‌های قبلی را به خدمت گیرد، برای تشخیص نفوذهای جدید، zero-day، و به کارگیری در شبکه‌های در حال کار مناسب نیست. نگاشت خود سازمانده یک مدل شبکه عصبی است که برای تحلیل و متصور ساختن داده‌های با ابعاد بالا ارائه شده است. این به طبقه مدلهای یادگیری رقابتی متعلق است که معمولا برای مشکلات متنوع دسته بندی بطور موفقیت آمیزی استفاده می‌شوند. نگاشت خود سازمانده براساس یادگیری غیر نظارتی برای نگاشت روابط آماری غیرخطی بین داده‌های ورودی با ابعاد بالا در شبکه دو بعدی که فضای خروجی نامیده می‌شود می‌باشد.

نگاشتهای خود سازمانده بطور موثری الگوهای مشابه را برای موقعیت‌های همجوار در فضای خروجی قرار داده و گزینه‌های ویژوال‌سازی و پیش‌بینی را برای داده‌ها با ابعاد بالا را فراهم می‌کند. با توجه به موارد ذکر شده، تحقیقات به منظور ارائه یک الگوریتم بهبود یافته شبکه عصبی غیر نظارتی خود سازمانده توسط نویسندگان مقاله در حال انجام می‌باشد.

۶- مراجع

[1] Bishop computer security, pearson Education, Addison Wesley, 2003

[2] Haykin,Neural networks: a comprehensive foundation, second Edition, Prentice Hall Inc. ,1999

[3] Peddisetty , Statoof-the-artIntrusion Detection :Technologies ,Challenges , and Evaluation ,2005

[4] Lichodzijewski , P.,zincir –heywood , A. , M.Hostbased intrusion detection using self-organizing maps proceedings of the 2002

[5] Kayacik H.G. Kayacik , A.N. Zincir –Heywood,M.1.Heywood ,on the Capability of an som based Intrusion Detection system ,IEEE-INNS international joint conference on neural nehvorks ,pp.1808-1813 , 2003

[6] S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchical Kohonenen Net for Anomaly Detection in Network Security," In IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, Vol. 35, No. 2, APRIL 2005.

[7] Ozgur Depren An intelligent intrusion detection system (IDS)for anomaly ,2005

[8] Morteza Amini,rasool jalili , hamid Reza Shahriari , RT-UNNID:A practical solution to real time network –based intrusion detection using unsupervised neural network2004

[9] Eskin , Ageometric framework for unsupervised anomaly detection ,detecting intrusions in unlabaled data , 2002

[10] Kohonen , T, Self organization map (3rd ed) Berlin :springer –verlag .2001

[11] kayacik and Zincir –Heywood , Training the SOFM Efficiently :An Intrusion detection 2005

[12] J.R.Quinlan, Decision trees as probabilistic classifiers, in proceedings of the fourth international workshop on Machine Learning Morgan Kaufmann ,pp 3437 ,June 1987.

www.SID.ir