اولین همایش ملی پیشرفت های تکنولوژی در مهندسی برق، الکترونیک و کامپیوتر

First National Conference of Technology Developments on Electronical, Electronics and Computer Engineering

. . . W W W . T D E C O N F . I R . . .

سیستم تشخیص نفوذ ترکیبی ART و MLP مبتنی بر شبکه های عصبی

رضا خدابنده لو ،مجید خلیلیان

دانشجوی کارشناسی ارشد دانشگاه آزاد اسلامی بویین زهرا

عضو هیئت علمی دانشگاه آزاد اسلامی کرج

taninrayaneh@yahoo.com

چکیده

در حوزه شبکه ،امنیت ،کنترل دسترسی و تشخیص به موقع با دقت بالا از ترافیک شبکه از مباحث اصلی و مهم میباشد.عملا هیچ سیستمی امنیت کامل ندارد.سیستم IDSبرای تشخیص نفوذ به موقع در ساختار شبکه بسیار جای خود را باز کرده و نیاز اساسی در هر شبکه ای میباشد .در این میان محققان به دنبال روش های مختلف برای بر آورده کردن این نیاز به کشف و طراحی انواع سیستم های خبره ،تغییر گذر حالات ،شبکه پتری ،روشهای آماری ،داده کاوی و شبکه های عصبی میپردازند. روشهای IDSشبکه های عصبی به دو دسته ۱- با ناظر مانند پیشخور چند لایه ،بازگشتی ۲- بدون ناظر مانند همینگ ،کوهنن و Artتقسیم می شوند .مزیت شبکه های عصبی بدون ناظر در این است که حملات شناخته نشده جدید را نیز می تواند شناسایی کند و نیاز به آموزش مجدد ندارند .در این مقاله سیستم AM با استفاده از شبکه های عصبی ART1,MLP با دسته بندی گروهی از ویژگیهای KDD-CUP ارائه گردیده است که کارایی بسیار بالایی دارد

کلید واژه :شبکه های عصبی نظارت شده ،تشخیص نفوذ AM ،شبکه های عصبی MLP وART

۱-مقدمه

گسترش روز افزون ارتباطات کامپیوتری وترافیک ایجاد شده تامین امنیت در برابر حملاتی نظیر دستکاری اطلاعات ، افزودن اطلاعات، استراق سمع ، قطع ارتباط کاربر DOSیاDDOS با استفاده از IP واطلاع از پورت های باز امری اجتناب ناپذیر می باشد.باتوجه به نفوذ هکرها از دیواره آتش وحتی ویروس یاب ها ، IDS ها ابزاری مناسب جهت تشخیص نفوذ واعلام هشدارها به مدیر شبکه می باشد.راههای نفوذ به کامپیوتر میزبان یا شبکه ویا به صورت ترکیبی وتوامان به دسته های زیر تقسیم می شوند:

حمله از طریق IP،حمله به TCP،جعل اطلاعات ،حمله به کلمات عبور ،حمله به برنامه های کاربردی ،استراق سمع(sniffer)،حملات اختلال در سرویس دهی،قطع ارتباط باDOS وDDOS ،ویروس ها واسب تروا ،پورت های باز(عبور بدون مرز)،حمله به سیستم عامل(ROOT KIT).

مقابله با نفوذ در دو سطح زیر انجام می گیرد:۱-کنترل واعتبارسنجی۲-سیستم های IDS

اهداف IDS :

۱-تشخیص گستره وسیعی از حملات

۲-تشخیص نفوذ به موقع

۳-تجزیه وتحلیل سریع وآسان

۴-به حداقل رساندنFNRو PPR [5]

استفاده از شبکه های عصبی باعث میشود دسته بندی خوب،تعمیم پذیری بالا،انعطاف پذیری،سرعت مناسب،کاهش نرخ اعلان خطا داشته باشیم.

روشهای تشخیص نفوذ به شبکه های کامپیوتری به دو دسته تقسیم میشوند:

۱- سوء استفاده (Misuse):در این روش یک سری الگوی شناخته شده به سیستم داده می شود که اگر ترافیک مانند اینالگو رفتار کند تشخیص نفوذ انجام می شود.این الگوها معمولا توسط افراد خبره به سیستم داده می شود.

۲-روش رفتار غیر نرمال(Anonaly): در این حالت براساس رفتار غیر عادی کاربران تشخیص نفوذ صورت می گیرد که روش های آماری خوشه بندی داده کاوی شبکه های عصبی جزء این روش ها می باشد.

طبقه بندی سیستم های تشخیص نفوذ IDS :

۱-مبتنی بر میزبان (Host Based IDS (HIDS: که در سمت Client انجام می شود.
2-مبتنی برشبکه (Network Based IDS (NIDS :در سمت سرور نصب وتشخیص انجام می شود.
۳- توزیع شده هیبریدی (Distributed IDS (DIDS :
در هر دو سمت Client وسرور نصب وتشخیص صورت می گیرد.(تشخیص ونفوذ توزیع شده).از چندینNIDS یا HIDS یا ترکیبی از این دونوع با مدیریت مرکزی تشکیل می شود.یعنی گزارشات هرIDS به مرکز ارسال می شود.[۹]
ارزیابی تشخیص نفوذ[۱۳]
۱- درصد تشخیص حمله (۱) $TPR = \frac{TP}{TP+FN}$
(۲) $TPR = \frac{\text{حملات درست تشخیص داده شده}}{\text{کل حملات}} \times 100$

اگر TP=TP+FN باشد ونسبت TPR به یک نزدیکتر باشد سیستم کاراتر است.
۲-درصد هشدار خطا
(۳) $FPR = \frac{FP}{FT+TN} = \frac{\text{رویدادهای های عادی که حمله محسوب شده اند}}{\text{تشخیص رویداد های نرمال صحیح+حملاتی که عادی گزارش اند}}$
3-درصد خطای منفی نادرست
(۴) $FNR = \frac{\text{کل ترافیک=}(\text{کل حملات درست و نادرست تشخیص داده شده})}{TN+TP+FN+FP} \times 100$ [3]
TN= True Negative کاربر عادی به درستی شخیص داده شده
TP= True positive حمله عادی به درستی نشخیص داده شده
FN=False Negative کاربر عادی حمله نشخیص داده شده
FP=False Positive حمله کاربر عادی تلقی شده
معمولاً این خطاها زمانی اتفاق می افتد که IDS طراحی شده براساس تنظیمات اشتباه ویا بسیار سختگیرانه ویا بسیار ساده کاربر عادی ،حمله وحمله کاربر عادی تلقی می شود.

۲-داده های تشخیص نفوذ

جهت شبیه سازی ،تست وتعیین کارایی سیستم های IDS باید از داده های استاندارد استفاده شود.اولین داده های استاندارد ترافیک شبکه-KDD CUP99 توسط گروه IST از آزمایشگاه MITزیرنظر DARPA وAFRL/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 IDSهای بدون ناظر مورد استفاده قرار می گیرد.
حملات گنجانده شده در داده های تست عبارتنداز:
۱-حملاتDOS انکار سرویس
2-حملاتPROBE بررسی وپویش برای یافتن راههای نفوذ
۳-حملات R2L دسترسی غیر مجاز از یک ماشین راه دور
۴-حملات U2R 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 KDD2014 معمولا مورد استفاده طراحان IDS جدید قرار می گیرد که داده های تکراری بسیار کمتری دارند.[۱]
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 [۹]
(۵) $xi = \frac{Xi - Xi\,min}{Xi\,max - Xi\,min}$

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 ،ICMP،UDP می باشد که شماره های ۱تا۳ را برای آنها در نظر می گیریم.

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

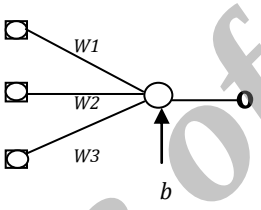
2-شبکه عصبی بازگشتی مانند CMAC و ELMANکه با بازگشت خروجی به ورودی تغییرات انجام می گیرد.

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.

3-شبکه های عصبی

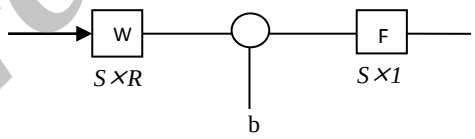
شبکه های عصبی در مقیاس تکنولوژیکی بسیار کوچک مدل های الکترونیکی از ساختار عصبی مغز برپایه فعالیت های سلول عصبی به نام نرون بنا نهاده شده بعبارتی یک شبکه عصبی یک ساختار توزیع شده موازی به فرم یک گراف جهت دار است هر گره (شکل ۱)یک واحد پردازشگر یایک نرون که ساده ترین واحد ساختاری سیستم های عصبی است می نامند.



شکل ۱:ساختار نرون

3-۱پرسپترون

این شبکه ها قادرند با انتخاب مناسب تعداد لایه ها و سلولهای عصبی ، یک نگاشت غیر خطی را با دقت دلخواه انجام دهند .فرمول۶ مرز تصمیم گیری را مشخص میکند.مرز جداسازی نواحی درحالت دوبعدی یک خط راست است.

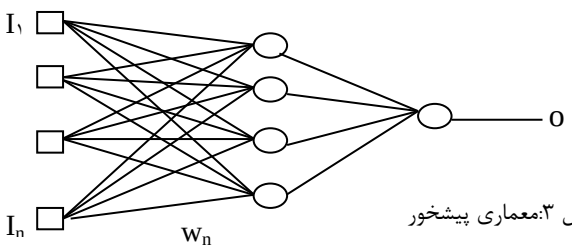


شکل ۲: ساختار پرسپترون

$$\sum \alpha_n + b = IW + b \qquad (۶)$$

۳-۲معماری شبکه عصبی پیشخور(Bp)

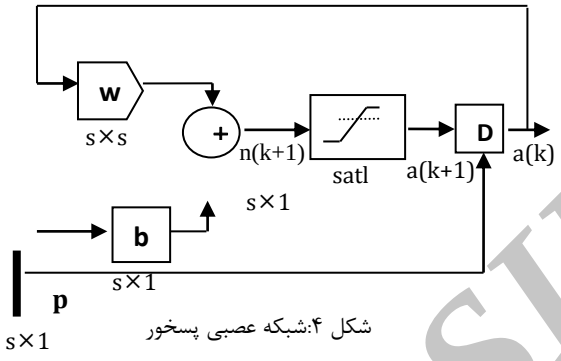
در این نوع شبکه ها(شکل ۳) پاسخ رو به جلو بوده و از لایه بعد باز خوردی نداردوخروجی به ورودی اعمال نمی شود.



شکل ۳:معماری پیشخور

3-۳معماری شبکه عصبی پسخور[15]

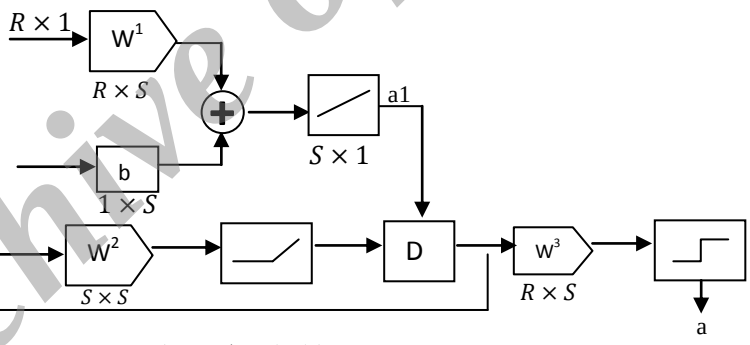
تفاوت شبکه های انتشار به عقب (شکل ۴) با شبکه های انتشار به جلو در این است که در شبکه های انتشاربه عقب حداقل یک سیگنال برگشتی از یک نرون به همان نرون یا نرون های همان لایه قبل وجود دارد.این شبکه ها پویا هستند.وضعیت آنها پیوسته در حال تغییر است تا اینکه به یک نقطه تعادل برسند.



شکل ۴:شبکه عصبی پسخور

۳-۴شبکه عصبی همینگ

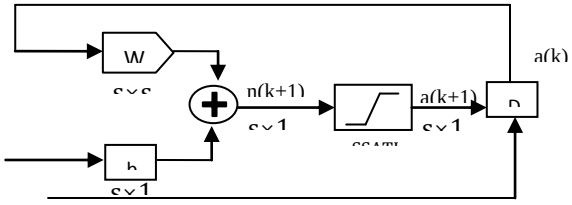
این شبکه تشخیص میدهد که کدام الگوی مرجع بیشترین نزدیکی را به الگوی ورودی دارد ونهایتا آنرا به خروجی هدایت میکند .از سه لایه تشکیل شده است.



شکل ۵:معماری شبکه

برای شناسایی الگوهای باینری بکار می رود(شکل ۵) از دو ساختار پیشخورو پسخور تشکیل شده وهدف اصلی تشخیص این است که کدام الگو بیشترین نزدیکی را به الگوی ورودی دارد.

۳-۵ شبکه عصبی هاپفیلد



$\underline{a}(o)=p, \underline{a}(k+1)=ssatl(w\underline{a}(k)+b)$

شکل ۶: معماری شبکه هاپفیلد

این شبکه(شکل ۶) مانند لایه میانی همینگ دارای فیدیک است بااین تفاوت که شبکه همینگ را جهت حل مسئله شناسایی الگو استفاده میکنند

۳-۶شبکه عصبی SOM

این شبکه بدون ناظر بوده و نرون ها بصورت صفحات مشبک در نظر گرفته میشوند نرون انتخاب شده بهمراه همسایگانش آموزش میبینند و ضریب یادگیری به فاصله نرون های همسایه با نرون انتخاب شده بستگی دارد $N_i(d)=\{j,d_{ij}\leq d\}$ ،d شعاع حداکثر همسایگی و $N_i(d)$ اعضاء همسایگی میباشند .بروز رسانی وزن های نرون ها در محدوده شعاع d با فرمول زیر انجام میگیرد. برای هر j عضو Nj(n)

$$W_{ij}(n+1) = W_{ij}(n) + \eta(X_{ij}(n) + W_{ij}(n) \quad (۸)$$

شعاع همسایگی و نرخ آموزش بمرور زمان تغییر میکند و میتوان از تابع همسایگی گوسین نیز استفاده کرد .

۳- ۷ شبکه عصبی ART

با این شبکه میتوان دسته بندی را بنحو مطلوب انجام داد نزدیکترین فاصله میان ورودی و بردار شاخص مشخص میکند ورودی به کدام گروه تعلق دارد اگر داده ورودی با دسته های موجود وفق داده نشود (شباهت نسبی) کلاس جدیدی بر آن ایجاد میشود که مشکل شبکه عصبی SOM را در مورد نرون مرده حل میکند این کار با پارامتر احتیاط (ρ) انجام میگردد میتوان گفت کار پایداری و انعطاف پذیری را نیز انجام میدهد.

ART1 برای مقادیر دودویی (گسسته) بوده و ART2 جهت مقادیر پیوسته بکار برده میشود یعنی ابتدا باید نرمالیزه و کاهش نویز انجام داد و در مرحله بعد مانند ART1 عمل میکند.

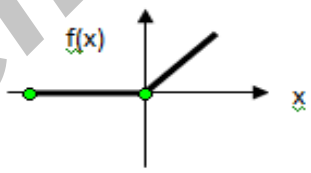
۳-۸ شبکه عصبی MAXNET

نمونه ای از شبکه های مبتنی بر رقابت است که فقط یکی از خروجی ها برنده میشود از این شبکه میتوان به عنوان زیر شبکه ای برای انتخاب واحدی که ورودی آن بزرگ ترین مقدار را در بین واحدهای شبکه دارد استفاده کرد (ماکزیمم یابی) .

در معماری این شبکه با M نرون ، کلیه M نرون دو طرفه به هم از جمله به خودشان وصل میشوند و وزن های متقارن دارند .

تابع فعال ساز آن بصورت زیر است :

$$f(x) = \begin{cases} x & if\ x > 0 \\ 0 & \text{درغیراین صورت} \end{cases} \quad (۷)$$



شکل7:تابع شبکه عصبی ماکس نت

مراحل تست این شبکه

مرحله یک : وزن ها تعیین میشوند $0 < \epsilon < \frac{1}{m}$ که mتعداد نرون هاست

مرحله دو : تا زمانی که شرایط توقف حاصل نشده مراحل ۳ تا ۵ تکرار شود

مرحله ۳: مقدار جدید هر گره بصورت زیر محاسبه میشود:

(۸)

$$a_j(new) = f\left(a_j(old) - \epsilon \sum_{j \neq k} a_k(old)\right)$$

مرحله ۴ : مقادیر گره ها را برای استفاده در تکرار بعدی ذخیره میکنیم :

(۹)

$$a_j(old) = a_j(new)$$

مرحله ۵: بررسی شرط توقف : اگر بیش از یک گره مقدار غیر صفر دارد ، ادامه والا توقف.

۴-کارهای انجام شده

[2,4] در بررسی های انجام شده IDS ترکیبی از مدل شبکه عصبی وبردار پشتیبان (SVM,SOM)جهت شناسایی حملات ناشناخته وتغییر یافته واستفاده از KDD-CUD DATASET بازدهی تشخیص صحیح درحملات Anomalyبه تنهایی در شبکه عصبی مخصوصاً در PROBE ٪۸۲/۴ و SVM به ۸۳/۸ بوده که با ترکیب این دو روش به کارایی ۴ /۹۷ رسیده است.

[3] در بررسی IDS بروش شبکه های عصبی HAMMING برای شناسایی حملات با پروتکل TCP نشان داده است که تعداد رکوردهای مورد بررسی کمتر از ۱۰۰۰ باشد بازدهی درست ۱۰۰٪ دارد ولی وقتی تعداد رکوردهای مورد بررسی به ۵۲۰۸ میرسد بازدهی تشخیص درست ٪۸۸.۷ میشود بنظر میرسد که خطای این روش با افزایش تعداد رکوردهای مورد بررسی افزایش میبابد و میتوان گفت که این روش برای تشخیص حملات DOS,DDOS اصلا مناسب نیست . DATASET بکار رفته در این روش NDIS میباشد.

[6] در بررسی تشخیص نفوذ بروش شبکه های عصبی همینگ در ترافیک غیر نرمال و استفاده از داده های استاندارد KDD-CUP با آزمایش ۶۱۸۶ رکورد با زمان تقریبی ۷ میلی ثانیه نتیجه ۹۵٪ تشخیص درست و ۴.۹۴٪ تشخیص نادرست بدست آمده است.

[7] در این روش که از شبکه عصبی بدون ناظر ART تحت عنوان UNNID از داده های DD-CUP99 استفاده شده است و نرمال سازی توسط پیش پردازنده انجام میگیرد طی مقایسه شبکه عصبی SOM و سیستم پیشنهادی برای تشخیص حملات DOS,PROB, R2L,U2R با تعیین پارامتر احتیاط ۰.۹ برای ART1 و ۰.۹۹۹ برای ART2 ، در کارایی بدست آمده نشان میدهد که سیستم ART1 بهتر از SOM عمل کرده و ART2 نسبت به ART1,SOM نتیجه مطلوبی ندارد.

[9] از روش طراحی موازی وشبکه های عصبی RBF برای شناسایی حملات اکثریتDOS وPROBING و از شبکه عصبی MLP برای شناسایی حملات اقلیت U2Rو R2L شناسایی را دسته بندی نمودند واز مجموع ۴۱ ویژگی برای هر نوع حمله تعداد ویژگی تاثیر گذار راانتخاب نمودند. در سیستم پردازش تشخیص نفوذ همزمان با چندین پردازنده نیز مقایسه گردیده است مثلاً تشخیص نفوذ با تقسیم بندی کار به ۴ پردازنده زمان تشخیص را تقریباً کمتر از 1/2 کاهش می دهد.

[10] از سیستم تشخیص انتشار به عقب MLP با نرمالیزه نمودن داده ها ودسته بندی استفاده شده است. لایه ورودی با ۴۱ نود و لایه میانی با ۲۰ نود و لایه خروجی بسته به نوع خروجی هدف ۱ یا ۵ نود تعیین شده است.

[11] از روش های سرمایش شبیه سازی شده بصورت فازی جهت تشخیص بهره گرفته شد.

[12] از شبکه های عصبی SOM در کاهش نرخ خطا مثبت و بالا بردن نرخ تشخیص درست استفاده شده است.

[13] از روش کاهش ویژگی ها به همراه شبکه عصبی PBH استفاده گردید. در بررسی های بعمل امده ۸ ویژگی زیر با، بالاترین تاثیر انتخاب شد.
هشت ویژگی استفاده شده عبارتند از:

service,src-byte,dst-byte,count,dst-hostcount,dst-host-srv-count,
dst-host-diff-srv-rate,dst-host-srv-diff-host-rate

برای هر نوع حمله تعداد ویژگی تاثیر گذار راانتخاب نمودند. در سیستم پردازش تشخیص نفوذ همزمان با چندین پردازنده نیز مقایسه گردیده است مثلاً تشخیص نفوذ با تقسیم بندی کار به ۴ پردازنده زمان تشخیص را تقریباً کمتر از 1/2 کاهش می دهد.

جدول ۱: نتایج بدست آمده شبکه عصبی PBH با ۸و۴۱ ویژگی

Probe	R2Ll	U2R	Dos	
94/26%	73/11%	49/27%	96/60%	41
99/48%	88/69%	76/25%	99/14%	8

نرخ تشخیص حمله و نرخ خطای مثبت نادرست و نرخ دقت ۷۳/۳۱ به ۹۱/۱۶ و۱۲/۶۷ به ۵/۲۸و۸۲/۵۳ به ۸۹/۲۱ ارتقاپیدا کرده است(جدول ۱) .برای پیدا کردن این ۸ ویژگی با استفاده از نرم افزار rosetta با الگوریتم Generic عمل شده است.

[14] از یک روش ترکیبی غیر نظارتی با استفاده از شبکه SOM وبررسی ۶ روش اصلی رفتار کاربران استفاده گردید.

۵- سیستم پیشنهادیAM

این سیستم دارای ۵ قسمت میباشد

۱- قسمت تامین داده

داده ها از منبع اطلاعاتی NSL-KDD-CUP استخراج گردیده که نسبت به KDD-CUP99 داده های تکراری کمتری دارد .

۲- قسمت نرمالیزاسیون

در این پیش پردازنده عمل نرمال سازی داده های بسته اطلاعاتی که دارای ۴۱ ویژگی میباشد در محدوده [0,1] قرار میگیرد

۳- قسمت تعیین دسته داده

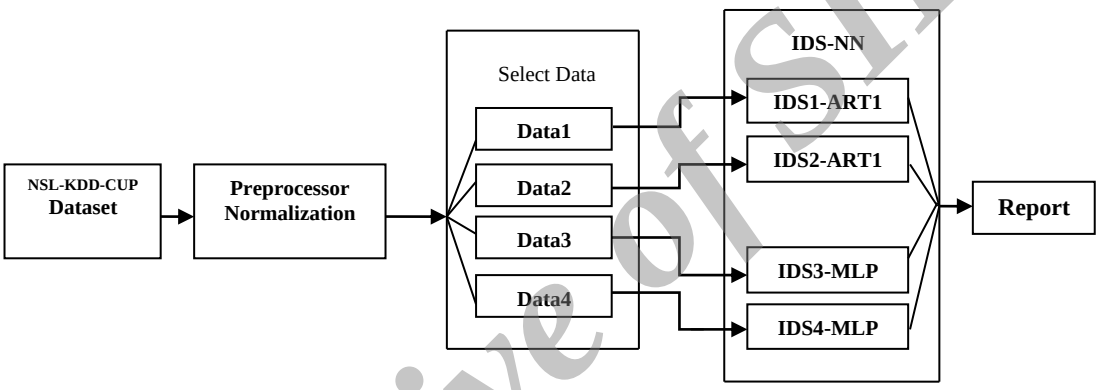
در این قسمت داده ها بر اساس نوع ویژگی و اهمیت آن در نوع حمله به ۴ دسته داده تقسیم میشود برای حمله DOS از شش ویژگی ،حمله PROBE چهار ویژگی ،حمله U2R شش ویژگی و حمله R2L از هفت ویژگی استفاده شده است

۴- قسمت پردازش تشخیص شبکه عصبی

از دو شبکه عصبی ART1 برای تشخیص حملات DOSو PROBE و شبکه عصبی MLP برای تشخیص حملات U2R و R2L استفاده شده است

۵- قسمت گزارش

گزارش تشخیص حمله را در اختیارمدیر شبکه و یا در فایل اطلاعاتی ثبت وقایع قرار میدهد



شکل ۸: معماری سیستم پیشنهادی AM

داده ها از منبع استاندارد KDD-CUP ابتدا نرمالیزه شده و در محدوده [0,1] قرار میگیرند سپس ویژگیهای مهم در ۴ دسته مختلف قرار میگیرند این ۴ دسته بر اساس ویژگیهای مهم نوع حمله با تست حالت ها تعیین گردیده است با انتخاب این ویژگیها به دقت و سرعت بیشتری رسیده ایم سپس در قسمت تشخیص حمله دو دسته اول از نوع حملات DOSو PROBE از شبکه عصبی ART1 و دو دسته دیگر از نوع حملات U2R و R2L از شبکه عصبی MLP استفاده گردید

جدول ۲: ویژگیهای انتخابی بر اساس اهمیت نوع حمله

نوع داده	نوع ویژگی انتخابی برای نوع حمله	نوع حمله
۱	Ipsweep,nmap,port sweep,satan	PROBE
۲	Back,Land,NepTune,pod,smurt,Teardrop	DOS
۳	Buffer-over flow-loadmodule,MulTihop,perl,rootkit	U2R
۴	ftp-write,guess-passwd,Limap,phf,spy,ware zclient ,warezmaster	R2L

پس از بررسیهای انجام شده تشخیص صحیح حمله با استفاده از IDS ART1 نتیجه ۱۰۰٪ برای نوع حمله DOS و ۹۹.۴۸٪ برای نوع حمله PROBE بدست آمد و همینطور با استفاده از IDS MLP نتیجه ۹۹.۹٪ برای حمله U2R و ۹۹.۳ % برای نوع حمله R2L طبق جدول بدست آمد

جدول ۳ : تشخیص صحیح حمله

نوع IDS	نوع حمله	تشخیص صحیح حمله
IDS ART1	DOS	100%
IDS ART1	PROB	99.48%
IDS MLP	U2R	99.9%
IDS MLP	R2L	99.3%

6- نتیجه گیری

با توجه به نیاز به تشخیص نفوذ در سیستم های کامپیوتری و بالا بردن قدرت صحت تشخیص در گونه های مختلف IDS ،شبکه های عصبی یکی از انواع مدل های تشخیص است دسته بندی نوع حملات واستفاده از مدل های مختلف شبکه عصبی از انواع BPH-BP، SOM وART و. . . که هر کدام دارای ویژگی خاص خود است ما را به این نتیجه می رساند که مدل های ترکیبی برای شناسایی حملات از انواع پویش، از راه دور و U2R باید توسعه بیشتری بیابد تا بتواند حداکثر تشخیص صحیح وحداقل تشخیص نادرست را به مسئول شبکه اعلام کند.

7-مراجع

[۱]s.revathi,dr.a. malathi, 2014 ”a detailed analysis on nsl-kdd dataset using various machine learning techniques for intrusion detection”,ijert
[2] Roshani Gaid hane ,M.Raghuwanshi 2014 “Leavnin Techigues for intrusion Detection system (IDS)” ,ijafrc ,vol 1
[۳] reyadh naom,Abdullah al-jaouni,narwan shaker, 2013 “ a hybrid intrusion detection system using hamming and maxnet neural nets using ndis dataset “ , cis jurnal,vol4
[4]Bhavin shah, Bhushan H Trived , 2012 ”Aytificial Neural Network based intrusion Detction system :Asurvey “, international journal of computer Applications ,vol39 –No.6
[5].madjid khalilian,norwati Mustapha,md nasir soliman,ali mamat, 2011”intusion detection system with data mining approach”,global journal of computer science&technology ,vol 11
[6]muna m.taher jawaher,monica mehrotra , 2010 “anomaly intrusion detection system using hamming network approach” , ijsc,vol1,165-169
[7] m.Amini and R.jalili , 2004 ”Net work-based in trusion Detection using unsupervised adaptive resonance theory (art) ” , proceedings of th 4th confercrence EIS 2004 , madria , Portugal

[8] رضا خدابنده لو ،مجید خلیلیان، ۲۰۱۴" بررسی سیستم های تشخیص نفوذ مبتنی بر شبکه های عصبی نظارت نشده"،مشهد،نهمین همایش ملی علوم و مهندسی کامپیوتر
[9] مهدی جانی نسب صلحدار،حمیده بابایی، مرتضی رموزی، ۲۰۱۳" ارائه یک روش جدید لایه ای برای سیستم های تشخیص نفوذ با استفاده از طراحی موازی و شبکه عصبی "، رودسر، اولین کنفرانس ملی رویکردهای نوین در مهندسی کامپیوتر و بازیابی اطلاعات
[10] حامد رجبی قمی ، محمد بهزادی ، ۲۰۱۲"سیستم تشخیص نفوذ مبتنی بر شبکه های عصبی انتشار به عقب " ،امل، ICNMO
[11] حمید محمدی ، جعفر حبیبی ، محمد صنیعی آباده ، حمید سعدی، ۲۰۱۲" تشخیص نفوذ در شبکه های کامپیوتری به کمک الگوریتم سرمایش شبیه سازی شده " ، اولین کنفرانس بین المللی شهر الکترونیک
[12] زهرا اخلاقی ، محمد قاسم زاده ، مهدی رضائیان، 2012" تشخیص نفوذ از نوع آنومالی با استفاده از شبکه های عصبی بدون ناظر ،" همایش ملی فن آوری اطلاعات و شبکه های کامپیوتری ،دانشگاه پیام نور طبس
[13] ربابه علیش زاده ، ۲۰۱۲" تشخیص نفوذ مبتنی بر تئوری مجموعه های نا هموار و شبکه های عصبی "، دومین کنفرانس ملی مهندسی نرم افزار ، لاهیجان
[14] سعید بخشایش خانیکی ، علیرضا رحمانی ، حمید رضا اسکندری ، ۲۰۰۸" ارتقاء یک سیستم تشخیص نفوذ ترکیبی با استفاده از شبکه های عصبی غیر نظارتی "، ششمین کنفرانس بین المللی رمز ایران
[15] محمد باقر منهاج، ۱۳۹۲" مبانی شبکه های عصبی "،دانشگاه صنعتی امیر کبیر،تهران،کتابشناسی ملی۱۱۶۲۱۱۷