تولید خودکار الگوهای نفوذ جدید با استفاده از طبقه‌بندهای تک کلاسی و روش‌های یادگیری استقرایی

مهدی آبادی[۱] و سعید جلیلی[*۲]

[۱]دانش آموخته دکتری مهندسی کامپیوتر- دانشکده فنی و مهندسی- دانشگاه تربیت مدرس

[۲]استادیار گروه مهندسی کامپیوتر- دانشکده فنی و مهندسی- دانشگاه تربیت مدرس

(تاریخ دریافت ۸۴/۱۲/۱۶، تاریخ دریافت روایت اصلاح شده ۸۶/۴/۱۰، تاریخ تصویب ۸۷/۱/۲۱)

چکیده

در این مقاله، روشی برای تولید خودکار الگوهای نفوذ جدید پیشنهاد می‌شود. از این روش می‌توان در سیستم‌های تشخیص نفوذ مبتنی بر شبکه و به منظور خودکارسازی فرآیند تولید الگوهای نفوذ استفاده کرد. در روش پیشنهادی، ابتدا با استفاده از ترکیب طبقه‌بندهای تک کلاسی نماهایی از ترافیک عادی شبکه مورد نظر ایجاد می‌شود. سپس در مرحله تشخیص، ترافیکی که با الگوهای نفوذ شناخته شده موجود مطابقت نکند و از نماهای ترافیک عادی شبکه انحراف داشته باشد، به عنوان نفوذ جدید تشخیص داده می‌شود. با استفاده از یک روش یادگیری استقرایی الگوی این نفوذ جدید تولید شده و پس از بررسی توسط مسئول امنیتی شبکه به پایگاه الگوهای نفوذ شناخته شده اضافه می‌شود. نتایج آزمایش‌های انجام شده بر روی مجموعه داده‌های فراهم شده توسط برنامه ارزیابی تشخیص نفوذ DARPA کارآیی روش پیشنهادی را برای تولید خودکار الگوهای نفوذ جدید نشان می‌دهد.

واژه‌های کلیدی: تشخیص نفوذ- الگوی نفوذ- طبقه‌بند تک کلاسی- یادگیری استقرایی

مقدمه

نفوذ، مجموعه اقدامات غیرقانونی است که صحت، محرمانگی و یا دسترسی به یک منبع را به خطر می‌اندازد. روش‌های تشخیص نفوذ به دو دسته تشخیص سوءاستفاده و تشخیص رفتار غیرعادی تقسیم می‌شوند. روش‌های تشخیص رفتار غیرعادی به دو دسته با نظارت و بدون نظارت تقسیم می گردند [۱]. با توجه به این واقعیت که همه نفوذها الزاماً رفتاری غیرعادی دارند، بنابراین روش‌های تشخیص رفتار غیرعادی قادر به تشخیص نفوذهای جدید می‌باشند [۲]. اما محدودیت اصلی این روش‌ها این است که معمولاً دارای نرخ هشدار نادرست نسبتاً بالا هستند.

در بسیاری از سیستم‌های تشخیص نفوذ موجود (از قبیل Snort) از الگوهای نفوذهای شناخته شده در فرآیند تشخیص نفوذ استفاده می‌شود. این سیستم‌های تشخیص نفوذ قادر به تشخیص نفوذهای جدید نمی‌باشند و در آنها با کشف هر نفوذ جدید پایگاه الگوهای نفوذ به صورت دستی به روز رسانده می‌شود. اغلب بین کشف هر نفوذ جدید، تولید الگوی آن نفوذ و به روز رسانی پایگاه الگوهای نفوذ تأخیر قابل ملاحظه‌ای وجود دارد. همچنین، تولید الگوهای نفوذ به صورت دستی کاری دشوار و زمان‌بر می‌باشد.

در این مقاله، روشی برای تولید خودکار الگوهای نفوذ جدید پیشنهاد می‌شود که با استفاده از آن علاوه بر تشخیص نفوذهای جدید، الگوهای این نفوذها به صورت خودکار تولید شده و به پایگاه الگوهای نفوذ شناخته شده اضافه می‌شود. در روش پیشنهادی، از ترکیب طبقه‌بندهای تک کلاسی برای مدل‌سازی ترافیک عادی و تشخیص ترافیک غیرعادی شبکه استفاده می‌گردد. روش پیشنهادی با استفاده از مجموعه داده‌های فراهم شده توسط برنامه ارزیابی تشخیص نفوذ DARPA مورد ارزیابی قرار می‌گیرد.

طبقه‌بندهای تک کلاسی

در مسائل طبقه‌بندی دو کلاسی، داده‌های مربوط به هر دو کلاس موجود است و مرز تصمیم از هر دو سمت توسط این داده‌ها پشتیبانی می‌شود. این طبقه‌بندها برای مسائلی از قبیل تشخیص رفتار غیرعادی، که در آن تنها یک کلاس از داده‌ها (رفتار عادی) موجود است، مناسب نمی‌باشند. برای حل این گونه مسائل می‌توان از طبقه‌بندهای تک کلاسی [۳] استفاده نمود.

* نویسنده مسئول : تلفن : ۸۲۸۸۳۳۷۴ ، فاکس : ۸۲۸۸۴۳۲۵ ، Email: sjalili@modares.ac.ir

الف – طبقه‌بند تک کلاسی PW

فرض کنید n نمونه $x_1,x_2,...,x_n$ از یک جمعیت با تابع چگالی $p(x)$ انتخاب شده باشند. تخمین چگالی PW[1] از $p(x)$ به صورت زیر محاسبه می‌شود:

$$\hat{p}(x)=\frac{1}{n\sigma^d}\sum_{i=1}^{n}k(\frac{x-x_i}{\sigma}) \qquad (۱)$$

که در آن $k(\cdot)$ پنجره یا تابع هسته، σ پهنای پنجره و d تعداد ابعاد فضای ویژگی است. در این مقاله، از هسته گوسی به عنوان تابع هسته استفاده می‌شود.

هنگام استفاده از روش تخمین چگالی PW برای مسائل طبقه‌بندی تک کلاسی، باید مقدار حد آستانه θ را به گونه‌ای تعیین کرد که نمونه x در صورتی به کلاس مورد نظر تعلق داشته باشد که $\hat{p}(x)>\theta$ باشد [۳]. در این مقاله، برای تعیین مقدار حد آستانه θ از نرخ پذیرش (AR[2]) استفاده می‌شود. AR به صورت کسری از داده‌های عادی که باید پذیرفته شوند، تعریف می‌شود:

$$\theta:\frac{1}{n}\sum_{i=1}^{n}I(\hat{p}(x_i)>\theta)=AR \qquad (۲)$$

که در آن $I(C)=1$ است اگر C درست باشد و $I(C)=0$ است اگر C نادرست باشد.

ب – طبقه‌بند تک کلاسی OCSVM

در طبقه‌بند تک کلاسی (OCSVM[3]) [۴]، ابتدا فضای داده ورودی X با استفاده از یک هسته مناسب به فضای ویژگی با تعداد ابعاد بالاتر H نگاشت می‌شود. سپس مبدأ به عنوان تنها عضو کلاس دوم در نظر گرفته می‌شود و سعی می‌شود تا ابرصفحه‌ای پیدا شود که بردارهای نگاشت شده را با بیشترین حاشیه از مبدأ جدا نماید.

مجموعه داده‌های آموزشی $x_1,x_2,...,x_n\in X$ را در نظر بگیرید. فرض کنید $\Phi:X\to H$ نگاشتی باشد که داده‌های آموزشی را به فضای ویژگی H تبدیل می‌نماید. به منظور جداسازی مجموعه داده‌ها از مبدأ باید مسأله برنامه‌ریزی درجه دوم زیر را حل کرد:

$$\min_{w,\xi,\rho}(\frac{1}{2}\|w\|^2+\frac{1}{nv}\sum_{i=1}^{n}\xi_i-\rho) \qquad (۳)$$

به شرط این که

$$(w\cdot\Phi(x_i))\geq\rho-\xi_i,\ \xi_i\geq 0, i=1,...,n \qquad (۴)$$

در روابط فوق، $v\in(0,1)$ عاملی است که بین به حداکثر رساندن فاصله از مبدأ و قرارگرفتن اکثر داده‌ها در ناحیه ایجاد شده توسط ابرصفحه توازن برقرار می‌کند.

در این مقاله، از OCSVM با هسته RBF استفاده می‌شود. این هسته به صورت زیر تعریف می‌گردد:

$$k(x,y)=\exp(-\gamma\|x-y\|^2) \qquad (۵)$$

ج – طبقه‌بند تک کلاسی GMM

متغیر تصادفی x دارای توزیع مخلوط متناهی است اگر تابع چگالی احتمال آن به صورت زیر نمایش داده شود:

$$p(x)=\sum_{i=1}^{C}\alpha_i f_i(x;\mu_i,\Sigma_i) \qquad (۶)$$

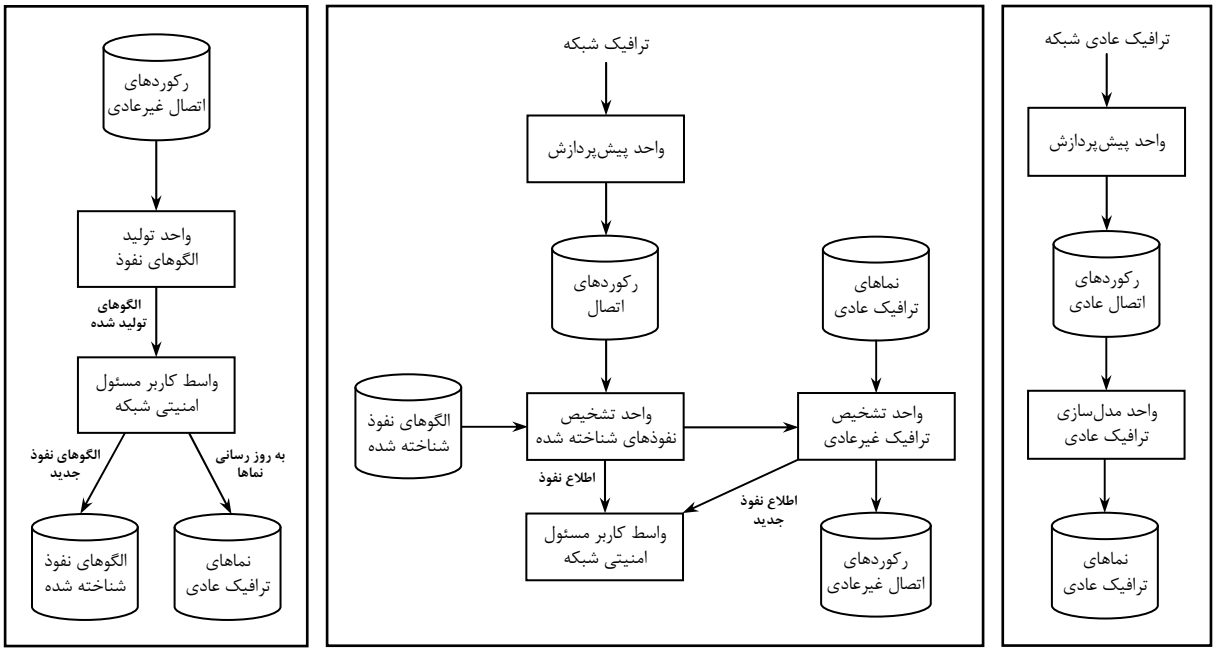
که در آن C تعداد مؤلفه‌های مخلوط، $f_i(x;\mu_i,\Sigma_i)$ چگالی iامین مؤلفه مخلوط و α_i وزن آن مؤلفه است.

اگر هر مؤلفه مخلوط دارای چگالی گوسی باشد، در این صورت اصطلاحاً گفته می‌شود که متغیر x از یک مدل مخلوط گوسی (GMM[4]) پیروی می‌کند. در هر GMM، تابع چگالی $f_i(x;\mu_i,\Sigma_i)$ می‌تواند یک گوسی تک متغیره $N(\mu_i,\sigma_i)$ یا یک گوسی چند متغیره $N(\mu_i,\Sigma_i)$ باشد. به منظور استفاده از روش تخمین چگالی GMM برای مسائل طبقه‌بندی تک کلاسی مشابه با روش تخمین چگالی PW عمل می‌شود [۳].

تولید خودکار الگوهای نفوذ جدید

روش پیشنهادی برای تولید خودکار الگوهای نفوذ جدید شامل سه مرحله *آموزش*، *تشخیص* و *یادگیری الگوهای نفوذ* است. در مرحله آموزش، با استفاده از ترکیب طبقه‌بندهای تک کلاسی (از قبیل PW با هسته گوسی، OCSVM با هسته RBF و GMM) نماهایی از ترافیک عادی شبکه مورد نظر ایجاد می‌شود. سپس در مرحله تشخیص، ترافیکی که با الگوهای نفوذ شناخته شده قبلی مطابقت ننماید و از نماهای ترافیک عادی شبکه انحراف داشته باشد، به عنوان نفوذ (احتمالی) جدید تشخیص داده می‌شود. در مرحله یادگیری الگوهای نفوذ، با استفاده از یک روش یادگیری استقرایی، الگوی این نفوذ جدید تولید شده و پس از بررسی توسط مسئول امنیتی شبکه به پایگاه الگوهای نفوذ شناخته شده اضافه می‌شود.

با استفاده از روش پیشنهادی می‌توان نفوذهای جدید را تشخیص داد و الگوهای آنها را به صورت خودکار تولید کرد. بنابراین، نیازی به کد کردن دستی الگوهای نفوذ جدید



(الف) مرحله آموزش (ب) مرحله تشخیص (ج) مرحله یادگیری الگوهای نفوذ

شکل ۱: معماری سیستم تشخیص نفوذ پیشنهادی .

وجود ندارد. همچنین، مسئول امنیتی شبکه می‌تواند از چگونگی انجام نفوذهای جدید اطلاع پیدا نموده و در صورت وقوع نفوذهای مشابه در آینده واکنش مناسبی نشان دهد.

معماری سیستم تشخیص نفوذ پیشنهادی

معماری سیستم تشخیص نفوذ پیشنهادی در شکل (۱) نمایش داده شده است. این سیستم تشخیص نفوذ از اجزاء زیر تشکیل می‌شود:

- واحد پیش‌پردازش
- واحد مدل‌سازی ترافیک عادی شبکه
- واحد تشخیص نفوذهای شناخته شده
- واحد تشخیص ترافیک غیرعادی شبکه
- واحد تولید الگوهای نفوذ

در سیستم تشخیص نفوذ پیشنهادی، در مرحله آموزش (شکل ۱ الف)، ابتدا ترافیک عادی شبکه مورد نظر در یک دورهٔ زمانی و تحت شرایط کنترل شده جمع‌آوری می‌شود. سپس در واحد پیش‌پردازش از ترافیک جمع‌آوری شده، رکوردهای اتصال استخراج می‌شود. از این رکوردها در واحد مدل‌سازی ترافیک عادی شبکه برای آموزش تعدادی طبقه‌بند تک کلاسی استفاده می‌شود. با ترکیب این طبقه‌بندهای تک کلاسی نماهای ترافیک عادی شبکه ایجاد می‌گردد. بنابراین، مرز تصمیمی پیدا می‌شود که قادر است ترافیک عادی را از ترافیک غیرعادی جدا نماید.

در مرحله تشخیص (شکل ۱ ب)، واحد پیش‌پردازش رکوردهای اتصال جدید را از ترافیک شبکه استخراج می‌کند. این رکوردهای اتصال به عنوان ورودی به واحد تشخیص نفوذهای شناخته شده داده می‌شوند. در این واحد، چنانچه هر یک از رکوردهای اتصال با یکی از الگوهای نفوذ شناخته شده منطبق گردد، بلافاصله موضوع به اطلاع مسئول امنیتی شبکه رسانده می‌شود. در غیر این صورت، رکوردهای اتصال به عنوان ورودی به واحد تشخیص ترافیک غیرعادی شبکه داده می‌شوند. در این واحد، رکوردهای اتصال ورودی براساس ترکیب نظرات طبقه‌بندهای تک کلاسی به دو دسته عادی و غیرعادی طبقه‌بندی می‌گردند. برای ترکیب نظرات طبقه‌بندهای تک کلاسی از استراتژی رأی اکثریت (MV[5]) استفاده می‌شود. در این استراتژی، ابتدا رکوردهای اتصال به عنوان ورودی به هرکدام از طبقه‌بندهای تک کلاسی داده می‌شوند. سپس، هر رکورد اتصال در صورتی به عنوان غیرعادی تشخیص داده می‌شود که توسط اکثر طبقه‌بندهای تک کلاسی به عنوان غیرعادی طبقه‌بندی شده باشد. چنانچه یک رکورد اتصال به عنوان غیرعادی طبقه‌بندی گردد، به پایگاه رکوردهای اتصال غیرعادی اضافه می‌شود. در مرحله یادگیری الگوهای نفوذ (شکل ۱ ج)، با توجه به این که

رکوردهای اتصال موجود در پایگاه رکوردهای اتصال غیرعادی ممکن است مربوط به چند نفوذ متفاوت باشند، بنابراین در واحد تولید الگوهای نفوذ، ابتدا رکوردهای اتصال غیرعادی با استفاده از یک الگوریتم خوشه‌بندی به تعدادی خوشه تقسیم می‌شوند. سپس با استفاده از یک روش یادگیری استقرایی، متناظر با هر خوشه یک الگو تولید می‌گردد.

در سیستم تشخیص نفوذ پیشنهادی از ترکیب هر دو روش‌های تشخیص سوءاستفاده و تشخیص رفتار غیرعادی برای تشخیص نفوذ به شبکه‌های کامپیوتری استفاده می‌شود. مزیت سیستم تشخیص نفوذ پیشنهادی نسبت به سیستم‌های تشخیص سوءاستفاده این است که سیستم تشخیص نفوذ پیشنهادی برخلاف این سیستم‌های تشخیص نفوذ قادر به تشخیص نفوذهای جدید می‌باشد. همچنین، مزیت سیستم تشخیص نفوذ پیشنهادی نسبت به سیستم‌های تشخیص رفتار غیرعادی این است که سیستم تشخیص نفوذ پیشنهادی علاوه بر تشخیص نفوذهای جدید، قادر به تولید خودکار الگوهای این نفوذها می‌باشد. بنابراین، مسئول امنیتی شبکه می‌تواند از چگونگی انجام نفوذهای جدید اطلاع پیدا کند و در صورت وقوع نفوذهای مشابه در آینده واکنش مناسبی نشان دهد.

ارزیابی کارآیی روش پیشنهادی

در این بخش، آزمایش‌های انجام شده برای ارزیابی کارآیی سیستم تشخیص نفوذ پیشنهادی شرح داده می‌شود.

الف. مجموعه داده‌ها

در آزمایش‌های انجام شده برای ارزیابی کارآیی سیستم تشخیص نفوذ پیشنهادی، از مجموعه داده‌های آموزشی فراهم شده توسط برنامه ارزیابی تشخیص نفوذ DARPA [۵] استفاده شد. این مجموعه داده‌ها شامل تقریباً پنج میلیون رکورد اتصال است. هر رکورد اتصال در این مجموعه داده‌ها شامل ۴۱ ویژگی و دارای برچسب عادی یا یک نوع حمله خاص است. این حملات را می‌توان به چهار دسته Probing، DoS، U2R و R2L تقسیم نمود. قبل از انجام آزمایش‌ها، مقدار هرکدام از ویژگی‌های رکوردهای اتصال فوق به بازه ۱- تا ۱ مقیاس داده شد.

برای ارزیابی کارآیی سیستم تشخیص نفوذ پیشنهادی، از دو معیار نرخ تشخیص (DR[۶]) و نرخ هشدار نادرست (FAR[۷]) استفاده گردید.

ب. ارزیابی واحدهای مدل‌سازی ترافیک عادی و تشخیص ترافیک غیرعادی شبکه

برای مدل‌سازی ترافیک عادی شبکه از ترکیب طبقه‌بندهای تک کلاسی PW با هسته گوسی، OCSVM با هسته RBF و GMM استفاده گردید. از مدل ایجاد شده فوق در واحد تشخیص ترافیک غیرعادی شبکه استفاده شد و با استفاده از آن کارآیی این واحد مورد ارزیابی قرار گرفت. بدین منظور، ابتدا مجموعه رکوردهای اتصال عادی به سه دسته تقسیم شد. از دسته اول برای آموزش هرکدام از طبقه‌بندهای تک کلاسی، از دسته دوم برای تعیین مقدار حد آستانه θ در طبقه‌بندهای تک کلاسی PW و GMM، و از دسته سوم برای تعیین نرخ هشدار نادرست (FAR) واحد تشخیص ترافیک غیرعادی شبکه استفاده شد.

برای تعیین نرخ تشخیص (DR) واحد تشخیص ترافیک غیرعادی شبکه، از رکوردهای اتصال با برچسب‌های Probing، DoS، U2R و R2L استفاده گردید.

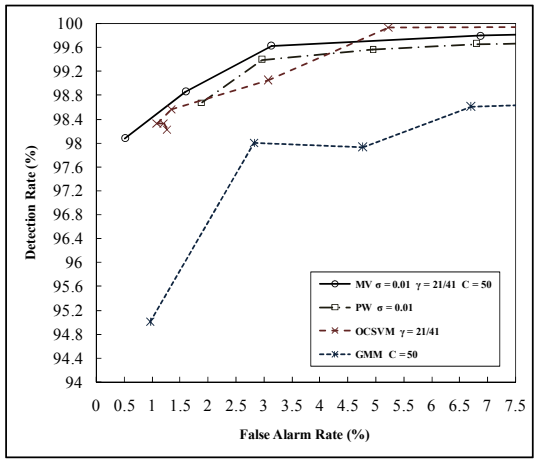
جدول ۱: نرخ تشخیص و نرخ هشدار نادرست ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM.

	Detection Rate (%)				False Alarm Rate (%)
	Probing	DoS	U2R	R2L	
$AR = 0.99$ $v = 0.005$	**98.08**	**99.51**	**59.61**	**28.95**	**0.51**
$AR = 0.97$ $v = 0.025$	**98.86**	**99.56**	**71.15**	**51.06**	**1.6**
$AR = 0.95$ $v = 0.05$	**99.63**	**99.59**	**82.69**	**95.11**	**3.13**
$AR = 0.91$ $v = 0.1$	**99.80**	**99.92**	**90.38**	**96.18**	**6.88**
$AR = 0.85$ $v = 0.15$	**99.90**	**100**	**100**	**98.40**	**11.92**
$AR = 0.70$ $v = 0.30$	**100**	**100**	**100**	**99.47**	**28.35**

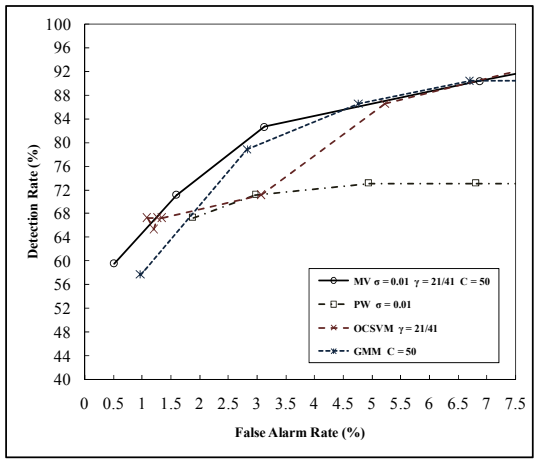
در جدول (۱) نرخ تشخیص و نرخ هشدار نادرست واحد تشخیص ترافیک غیرعادی شبکه به ازاء مقادیر مختلف عامل AR مربوط به طبقه‌بندهای تک کلاسی PW و GMM و عامل v مربوط به طبقه‌بند تک کلاسی OCSVM نمایش داده شده است.

در آزمایش‌های انجام شده، برای طبقه‌بند تک کلاسی PW عامل $\sigma = 0.01$، برای طبقه‌بند تک کلاسی OCSVM عامل $\gamma = 21/41$ و برای طبقه‌بند تک کلاسی GMM عامل $C = 50$ در نظر گرفته شد.

با ترکیب نظرات طبقه‌بندهای تک کلاسی می‌توان به نرخ‌های هشدار نادرست خیلی پایین دست پیدا نمود، در حالی که با استفاده از هرکدام از طبقه‌بندهای تک کلاسی به تنهایی این امکان وجود ندارد. در شکل‌های (۲) و (۳) با رسم منحنی‌های ROC کارآیی استراتژی رأی اکثریت برای ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM با کارآیی هرکدام از طبقه‌بندهای تک کلاسی فوق برای تشخیص ترافیک غیرعادی شبکه مقایسه شده است.



شکل ۲: مقایسه کارآیی ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM با کارآیی هرکدام از طبقه‌بندهای تک کلاسی فوق برای تشخیص حملات Probing.



شکل ۳: مقایسه کارآیی ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM با کارآیی هرکدام از طبقه‌بندهای تک کلاسی فوق برای تشخیص حملات U2R.

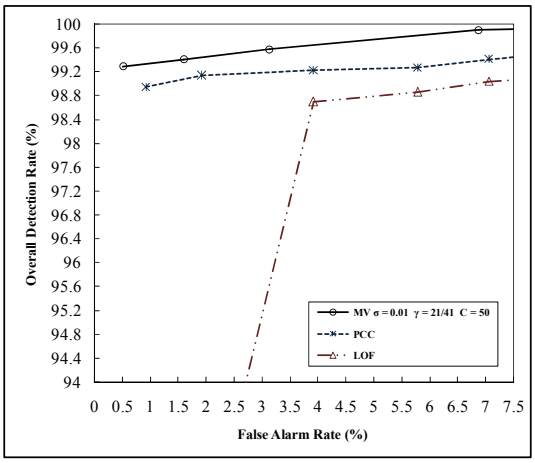
با مقایسه شکل‌های (۲) و (۳) مشخص می‌شود که با ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM با استراتژی رأی اکثریت توازن بهتری میان نرخ تشخیص و نرخ هشدار نادرست واحد تشخیص ترافیک غیرعادی شبکه برقرار می‌شود.

برای تشخیص با نظارت ترافیک غیرعادی شبکه روش‌های متعددی پیشنهاد شده است. Fan و همکارانش [۶] رویکرد متفاوتی به نام RIPPER-DBA2 را برای تشخیص با نظارت ترافیک غیرعادی شبکه پیشنهاد کرده‌اند. در جدول (۲) نرخ تشخیص و نرخ هشدار نادرست رویکرد فوق نمایش داده شده است.

جدول ۲: نرخ تشخیص و نرخ هشدار نادرست رویکرد RIPPER-DBA2 برای تشخیص ترافیک غیرعادی شبکه [۶].

Detection Rate (%)				False Alarm Rate (%)
Probing	DoS	U2R	R2L	
1.34	94.31	47.06	66.67	2.02

با مقایسه نتایج ارائه شده در جدول (۲) با نتایج ارائه شده در جدول (۱) مشخص می‌شود که ترکیب نظرات طبقه‌بندهای تک کلاسی با استراتژی رأی اکثریت از نرخ تشخیص خیلی بالاتری نسبت به رویکرد RIPPER-DBA2 [۶] برای تشخیص ترافیک غیرعادی شبکه برخوردار بوده و این در حالی است که نرخ هشدار نادرست نیز به شدت کاهش یافته است.



شکل ۴: مقایسه کارآیی ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM با کارآیی روش‌های PCC [۷] و LOF [۸] برای تشخیص ترافیک غیرعادی شبکه.

Shyu و همکارانش [۷] روشی به نام PCC را برای تشخیص با نظارت ترافیک غیرعادی شبکه پیشنهاد نموده‌اند. آنها کارآیی روش PCC برای تشخیص ترافیک غیرعادی شبکه را با کارآیی روش‌های KNN و LOF [۸] مقایسه کرده‌اند. این مقایسه تنها براساس نرخ تشخیص کلی حملات (بدون تفکیک هر دسته از حملات Probing، DoS، U2R و R2L) انجام شده است. نتایج آزمایش‌ها نشان

می‌دهد که روش PCC دارای کارآیی بالاتری نسبت به روش‌های KNN و LOF می‌باشد. در شکل (۴) کارآیی استراتژی رأی اکثریت برای ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM با کارآیی روش‌های PCC [۷] و LOF [۸] برای تشخیص ترافیک غیرعادی شبکه مقایسه شده است. با توجه به شکل (۴) مشخص می‌شود که با ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM با استراتژی رأی اکثریت نرخ تشخیص کلی بالاتری نسبت به روش‌های PCC [۷] و LOF [۸] به دست می‌آید.

ج. ارزیابی واحد تولید الگوهای نفوذ

برای ارزیابی واحد تولید الگوهای نفوذ، ابتدا ۶۰۰۰۰ رکورد اتصال با برچسب Normal به صورت تصادفی انتخاب گردید که از آنها برای آموزش طبقه‌بندهای تک کلاسی PW، OCSVM و GMM استفاده شد. برای مدل‌سازی ترافیک عادی و تشخیص ترافیک غیرعادی شبکه، ترکیب طبقه‌بندهای تک کلاسی فوق با استراتژی رأی اکثریت مورد استفاده قرار گرفت. سپس، ۶۰۰۰۰ رکورد اتصال دیگر با برچسب‌های Normal، Smurf و Neptune به صورت تصادفی انتخاب گردید. نفوذهای موجود در این مجموعه داده‌ها به عنوان نفوذهای جدید در نظر گرفته شد. مجموعه داده‌های فوق به عنوان ورودی به واحد تشخیص ترافیک غیرعادی شبکه داده شد. در این واحد، به هرکدام از رکوردهای اتصال ورودی برچسب عادی یا غیرعادی زده شد.

در آزمایش‌های انجام شده، برای طبقه‌بندهای تک کلاسی PW، OCSVM و GMM عامل‌های $\sigma = 0.01$، $\gamma = 21/41$، $v = 0.025$، $C = 50$ و $AR = 0.97$ در نظر گرفته شد.

رکوردهای اتصال غیرعادی تشخیص داده شده توسط واحد تشخیص ترافیک غیرعادی شبکه به عنوان ورودی به واحد تولید الگوهای نفوذ داده شد. در این واحد، ابتدا مجموعه داده‌های ورودی با استفاده از الگوریتم شبکه عصبی SOM خوشه‌بندی گردید. در آزمایش‌ها برای خوشه‌بندی رکوردهای اتصال غیرعادی، از یک SOM با شبکه خروجی ۲×۲ استفاده شد. آموزش شبکه در دو مرحله انجام گردید. در مرحله اول از یک نرخ یادگیری اولیه بزرگ ($\alpha = 0.5$) و در مرحله دوم از یک نرخ یادگیری اولیه کوچک ($\alpha = 0.05$) استفاده شد. در طی آموزش، نرخ یادگیری به صورت خطی به صفر کاهش داده شد.

پس از خوشه‌بندی، به داده‌های مربوط به هر خوشه برچسب نفوذ زده شد. این داده‌ها همراه با داده‌هایی که برچسب عادی داشتند، به عنوان ورودی به سیستم یادگیری قانون C4.5 [۹] داده شدند. با استفاده از این سیستم یادگیری قانون، برای هر کدام از خوشه‌ها یک قانون تولید گردید. این قوانین که در شکل (۵) نمایش داده شده‌اند، الگوهای نفوذهای فوق را توصیف می‌کنند. قانون اول بیانگر این مطلب است که در نفوذ با برچسب Intrusion1 تعداد زیادی بسته ICMP به میزبان مقصد ارسال می‌شود و قانون دوم هم بیان می‌کند که در نفوذ با برچسب Intrusion2 تعداد زیادی بسته SYN به درگاه خاصی از میزبان مقصد ارسال می‌گردد. بنابراین، با توجه به این قوانین می‌توان نتیجه گرفت که نفوذهای فوق از نوع جلوگیری از سرویس می‌باشند.

If Service = ecr_i **and**
SrvCount > 325
Then class = **Intrusion1**

تفسیر قانون: اگر سرویس اتصال جاری icmp echo request باشد و در ۲ ثانیه گذشته، تعداد اتصالاتی که سرویس یکسانی با اتصال جاری دارند بیشتر از ۳۲۵ باشد، آنگاه این رفتار نشان دهندهٔ نفوذ است.

If Flag = S0 **and**
SrvSYNErrRate > 0.5
Then class = **Intrusion2**

تفسیر قانون: اگر اتصال جاری با خطای SYN خاتمه یافته باشد و در ۲ ثانیه گذشته، درصد خطاهای SYN در اتصالاتی که سرویس یکسانی با اتصال جاری دارند بیشتر از ۵۰ درصد باشد، آنگاه این رفتار نشان دهندهٔ نفوذ است.

شکل ۵: الگوهای نفوذ تولید شده با استفاده از روش پیشنهادی.

د. ارزیابی واحد تشخیص نفوذهای شناخته شده

الگوهای (به عبارت دیگر، قوانین) تولید شده در بخش قبلی برای نفوذهای Intrusion1 و Intrusion2 به پایگاه الگوهای نفوذ شناخته شده اضافه گردید.

برای ارزیابی واحد تشخیص نفوذهای شناخته شده، ابتدا ۶۰۰۰۰ رکورد اتصال با برچسب‌های Normal، Smurf و Neptune به صورت تصادفی انتخاب گردید. در این مجموعه داده‌ها، ۳۰۰۰۰ رکورد اتصال دارای برچسب Normal، ۱۵۰۰۰ رکورد اتصال دارای برچسب Smurf و ۱۵۰۰۰ رکورد اتصال دارای برچسب Neptune بود. سپس از الگوهای نفوذ موجود در پایگاه الگوهای نفوذ شناخته شده برای طبقه‌بندی این رکوردهای اتصال استفاده گردید. نتایج به دست آمده در جدول (۳) نمایش داده شده است.

جدول ۳: طبقه‌بندی رکوردهای اتصال ورودی با استفاده از الگوهای نفوذ تولید شده .

	Normal	Intrusion1	Intrusion2
Normal	**29999**	**1**	
Smurf	**60**	**14940**	
Neptune	**2**		**14998**

با توجه به جدول (۳) مشخص می‌شود که با استفاده از الگوهای نفوذ تولید شده می‌توان نفوذهای Smurf و Neptune را با دقت بالا (۹۹/۶۰٪ و ۹۹/۹۸٪) تشخیص داد، در حالی که هشدار نادرست اعلام شده توسط سیستم تشخیص نفوذ بسیار ناچیز (۰/۰۰۳٪) است.

نتیجه‌گیری

در این مقاله، روشی برای تولید خودکار الگوهای نفوذ جدید پیشنهاد گردید. به منظور ارزیابی روش پیشنهادی از مجموعه داده‌های فراهم شده توسط برنامه ارزیابی تشخیص نفوذ DARPA استفاده گردید. در آزمایش‌های انجام شده، برای تشخیص ترافیک غیرعادی شبکه از ترکیب نظرات طبقه‌بندهای تک کلاسی PW با هسته گوسی، OCSVM با هسته RBF و GMM استفاده شد. برای تولید الگوهای نفوذ جدید از سیستم یادگیری قانون C4.5 استفاده گردید.

مراجع

1 - Leung, K. and Leckie, C. (2005). "Unsupervised anomaly detection in network intrusion detection using clusters." *Proc. 28th Australasian Conf. on Computer Science*, Newcastle, Australia, PP. 333-342.

2 - Denning, D. E. (1987). "An intrusion-detection model." *IEEE Trans. on Software Eng*., Vol. 13, No. 2, PP. 222-232.

3 - Tax, D. M. J. (2001). *One-Class Classification*. PhD Thesis, Delft University of Technology.

4 - Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J. and Williamson, R. C. (2001). "Estimating the support of a high-dimensional distribution." *Neural Computation*, Vol. 13, No. 7, PP. 1443-1471.

5 - Lippmann, R. P., Fried, D. J., Graf, I., et al. (2000). "Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation." *Proc. DARPA Information Survivability Conf. and Exposition (DISCEX)*, IEEE Computer Society Press, Los Alamitos, CA, USA, Vol. 2, PP. 12-26.

6 - Fan, W., Miller, M., Stolfo, S. J., Lee, W., and Chan, P. K. (2001). "Using artificial anomalies to detect unknown and known network intrusions." *Proc. 1st IEEE Int. Conf, on Data Mining*, San Jose, CA, USA, PP. 123-130.

7 - Shyu, M.-L., Chen, S.-C., Sarinnapakorn, K., and Chang, L.-W. (2003). "A novel anomaly detection scheme based on principal component classifier." *Proc. IEEE Foundations and New Directions of Data Mining Workshop*, Melbourne, FL, USA, PP. 172-179.

8 - Breunig, M. M., Kriegel, H. P., Ng, R. T., and Sander, J. (2000). "LOF: identifying density-based local outliers." *Proc. ACM SIGMOD Conf.*, Dallas, TX, USA, PP. 93-104.

9 - Quinlan, J. R. (1993). *C4.5 Programs for Machine Learning*, Morgan Kaufman, San Mateo, CA, USA.

واژه‌های انگلیسی به ترتیب استفاده در متن

1 - Parzen-Window
2 - Acceptance Rate
3 - One-Class Support Vector Machine
4 - Gaussian Mixture Model
5 - Majority Voting
6 - Detection Rate
7 - False Alarm Rate