# توليد خودكار الگوهاي نفوذ جديد با استفاده از طبقه‌بندهاي تك كلاسي و روش‌هاي يادگيري استقرايي

مهدي آبادي[۱] و سعيد جليلي*[۲]

[۱]دانشجوي دكتري گروه مهندسي كامپيوتر- دانشكده فني و مهندسي- دانشگاه تربيت مدرس

[۲]استاديار گروه مهندسي كامپيوتر- دانشكده فني و مهندسي- دانشگاه تربيت مدرس

(تاريخ دريافت ۸٤/۱۲/۱٦، تاريخ دريافت روايت اصلاح شده ۸٦/٤/۱۰، تاريخ تصويب ۸۷/۱/۲۱)

## چكيده

در اين مقاله، روشي براي توليد خودكار الگوهاي نفوذ جديد پيشنهاد مي‌شود. از اين روش مي‌توان در سيستم‌هاي تشخيص نفوذ مبتني بر شبكه و به منظور خودكارسازي فرآيند توليد الگوهاي نفوذ استفاده كرد. در روش پيشنهادي، ابتدا با استفاده از تركيب طبقه‌بندهاي تك كلاسي نماهايي از ترافيک عادي شبكه مورد نظر ايجاد مي‌شود. سپس در مرحله تشخيص، ترافيكي كه با الگوهاي نفوذ شناخته شده موجود مطابقت نكند و از نماهاي ترافيك عادي شبكه انحراف داشته باشد، به عنوان نفوذ جديد تشخيص داده مي‌شود. با استفاده از يك روش يادگيري استقرايي الگوي اين نفوذ جديد توليد شده و پس از بررسي توسط مسئول امنيتي شبكه به پايگاه الگوهاي نفوذ شناخته شده اضافه مي‌شود. نتايج آزمايش هاي انجام شده بر روي مجموعه داده‌هاي فراهم شده توسط برنامه ارزيابي تشخيص نفوذ DARPA كارآيي روش پيشنهادي را براي توليد خودكار الگوهاي نفوذ جديد نشان مي‌دهد.

**واژه‌هاي كليدي**: تشخيص نفوذ- الگوي نفوذ- طبقه‌بند تک كلاسي- يادگيري استقرايي

## مقدمه

نفوذ، مجموعه اقدامات غيرقانوني است كه صحت، محرمانگي و يا دسترسي به يك منبع را به خطر مي‌اندازد. روش‌هاي تشخيص نفوذ به دو دسته تشخيص سوء استفاده و تشخيص رفتار غيرعادي تقسيم مي‌شوند. روش‌هاي تشخيص رفتار غيرعادي به دو دسته با نظارت و بدون نظارت تقسيم مي گردند [۱]. با توجه به اين واقعيت كه همه نفوذها الزاماً رفتاري غيرعادي دارند، بنابراين روش‌هاي تشخيص رفتار غيرعادي قادر به تشخيص نفوذهاي جديد مي‌باشند [۲]. اما محدوديت اصلي اين روش‌ها اين است كه معمولاً داراي نرخ هشدار نادرست نسبتاً بالا هستند.

در بسياري از سيستم‌هاي تشخيص نفوذ موجود (از قبيل Snort) از الگوهاي نفوذهاي شناخته شده در فرآيند تشخيص نفوذ استفاده مي‌شود. اين سيستم‌هاي تشخيص نفوذ قادر به تشخيص نفوذهاي جديد نمي‌باشند و در آنها با كشف هر نفوذ جديد پايگاه الگوهاي نفوذ به صورت دستي به روز رسانده مي‌شود. اغلب بين كشف هر نفوذ جديد، توليد الگوي آن نفوذ و به روز رساني پايگاه الگوهاي نفوذ تأخير قابل ملاحظه‌اي وجود دارد. هم چنين، توليد الگوهاي نفوذ به صورت دستي كاري دشوار و زمان‌بر مي باشد.

در اين مقاله، روشي براي توليد خودكار الگوهاي نفوذ جديد پيشنهاد مي‌شود كه با استفاده از آن علاوه بر تشخيص نفوذهاي جديد، الگوهاي اين نفوذها به صورت خودكار توليد شده و به پايگاه الگوهاي نفوذ شناخته شده اضافه مي‌شود. در روش پيشنهادي، از تركيب طبقه‌بندهاي تك كلاسي براي مدل‌سازي ترافيك عادي و تشخيص ترافيك غيرعادي شبكه استفاده مي گردد. روش پيشنهادي با استفاده از مجموعه داده‌هاي فراهم شده توسط برنامه ارزيابي تشخيص نفوذ DARPA مورد ارزيابي قرار مي‌گيرد.

## طبقه‌بندهاي تک كلاسي

در مسائل طبقه‌بندي دو كلاسي، داده‌هاي مربوط به هر دو كلاس موجود است و مرز تصميم از هر دو سمت توسط اين داده‌ها پشتيباني مي‌شود. اين طبقه‌بندها براي مسائلي از قبيل تشخيص رفتار غيرعادي، كه در آن تنها يک كلاس از داده‌ها (رفتار عادي) موجود است، مناسب نمي‌باشند. براي حل اين گونه مسائل مي‌توان از طبقه‌بندهاي تک كلاسي [۳] استفاده نمود.

* نويسنده مسئول : تلفن : ۸۸۰۱۱۰۰۱ , فاكس : ۸۸۰۰۵۰۴۰ , Email: sjalili@modares.ac.ir

الف - طبقه‌بند تک کلاسي **PW**

فرض کنيد $n$ نمونه $x_1, x_2, ..., x_n$ از يك جمعيت با تابع چگالي $p(x)$ انتخاب شده باشند. تخمين چگالي PW[1] از $p(x)$ به صورت زير محاسبه مي‌شود:

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

که در آن $k(\cdot)$ پنجره يا تابع هسته، $\sigma$ پهناي پنجره و $d$ تعداد ابعاد فضاي ويژگي است. در اين مقاله از هسته گوسي به عنوان تابع هسته استفاده مي‌شود.

هنگام استفاده از روش تخمين چگالي PW براي مسائل طبقه‌بندي تک کلاسي، بايد مقدار حد آستانه $\theta$ را به‌گونه‌اي تعيين کرد که نمونه $x$ در صورتي به کلاس مورد نظر تعلق داشته باشد که $\hat{p}(x) > \theta$ باشد [۳]. در اين مقاله، براي تعيين مقدار حد آستانه $\theta$ از نرخ پذيرش ($AR$[2]) استفاده مي‌شود. $AR$ به صورت کسري از داده‌هاي عادي که بايد پذيرفته شوند، تعريف مي‌شود:

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

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

ب - طبقه‌بند تک کلاسي **OCSVM**

در طبقه‌بند تک کلاسي (OCSVM[3]) [۴]، ابتدا فضاي داده ورودي $X$ با استفاده از يک هسته مناسب به فضاي ويژگي با تعداد ابعاد بالاتر $H$ نگاشت مي‌شود. سپس مبدأ به عنوان تنها عضو کلاس دوم در نظر گرفته مي‌شود و سعي مي‌شود تا ابرصفحه‌اي پيدا شود که بردارهاي نگاشت شده را با بيشترين حاشيه از مبدأ جدا نمايد.

مجموعه داده‌هاي آموزشي $x_1, x_2, ..., x_n \in X$ در نظر گرفته مي شود. فرض بر اين است $\Phi : X \to H$ نگاشتي باشد که داده‌هاي آموزشي را به فضاي ويژگي $H$ تبديل مي‌نمايد. به منظور جداسازي مجموعه داده‌ها از مبدأ بايد مسئله برنامه‌ريزي درجه دوم زير 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 اين که

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

در روابط فوق، $v \in (0, 1)$ عاملي است که بين به حداکثر رساندن فاصله از مبدأ و قرارگرفتن اکثر داده‌ها در ناحيه ايجاد شده توسط ابرصفحه توازن برقرار مي‌کند.

در اين مقاله، از OCSVM با هسته RBF استفاده مي‌شود که به صورت زير تعريف مي گردد:

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

ج - طبقه‌بند تک کلاسي **GMM**

متغير تصادفي $x$ داراي توزيع مخلوط متناهي است اگر تابع چگالي احتمال آن به صورت زير نمايش داده شود:

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

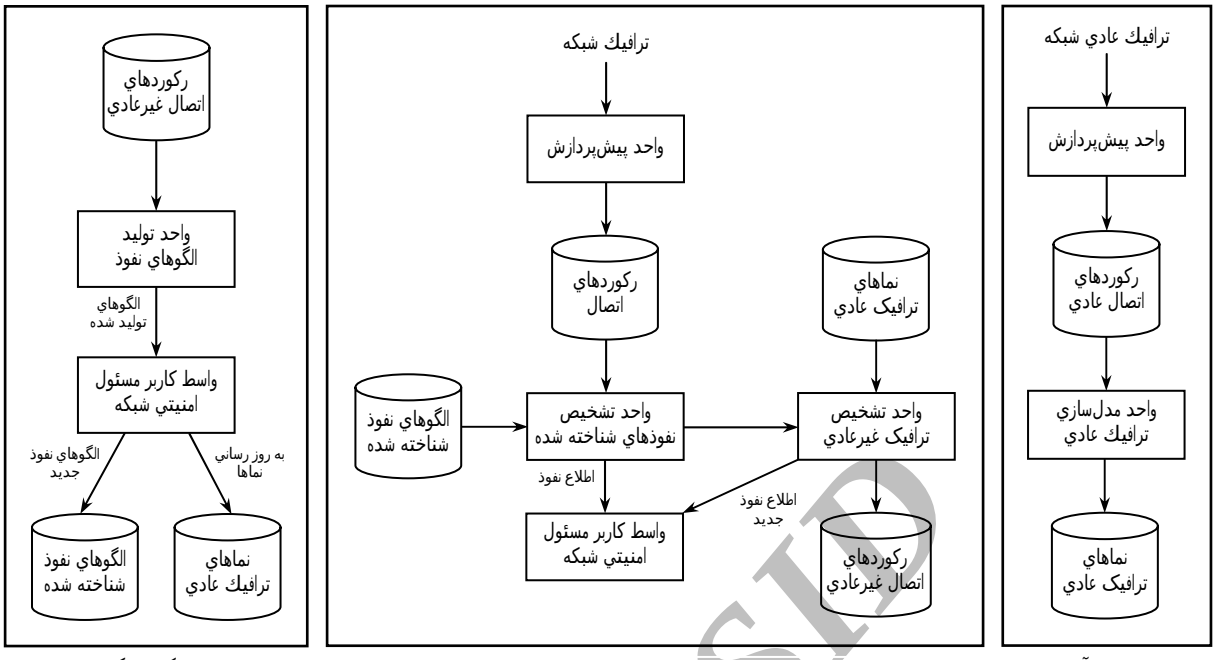
که در آن $C$ تعداد مؤلفه‌هاي مخلوط، $f_i(x; \mu_i, \Sigma_i)$ چگالي $i$ امين مؤلفه مخلوط و $\alpha_i$ وزن آن مؤلفه است.

اگر هر مؤلفه مخلوط داراي چگالي گوسي باشد، در اين صورت اصطلاحاً گفته مي‌شود که متغير $x$ از يك مدل مخلوط گوسي (GMM[4]) پيروي مي‌کند. در هر GMM، تابع چگالي $f_i(x; \mu_i, \Sigma_i)$ مي‌تواند يك گوسي تك متغيره $N(\mu_i, \sigma_i)$ يا يك گوسي چند متغيره $N(\mu_i, \Sigma_i)$ باشد. به منظور استفاده از روش تخمين چگالي GMM براي مسائل طبقه‌بندي تک کلاسي مشابه با روش تخمين چگالي PW عمل مي‌شود [۳].

## توليد خودکار الگوهاي نفوذ جديد

روش پيشنهادي براي توليد خودکار الگوهاي نفوذ جديد شامل سه مرحله *آموزش*، *تشخيص* و *يادگيري الگوهاي نفوذ* است. در مرحله آموزش، با استفاده از ترکيب طبقه‌بندهاي تک کلاسي (از قبيل PW با هسته گوسي، OCSVM با هسته RBF و GMM) نماهايي از ترافيک عادي شبکه مورد نظر ايجاد مي‌شود. سپس در مرحله تشخيص، ترافيکي که با الگوهاي نفوذ شناخته شده قبلي مطابقت ننمايد و از نماهاي ترافيك عادي شبکه انحراف داشته باشد، به عنوان نفوذ (احتمالي) جديد تشخيص داده مي‌شود. در مرحله يادگيري الگوهاي نفوذ، با استفاده از يك روش يادگيري استقرايي، الگوي اين نفوذ جديد توليد شده و پس از بررسي توسط مسئول امنيتي شبکه به پايگاه الگوهاي نفوذ شناخته شده اضافه مي‌شود.

با استفاده از روش پيشنهادي مي‌توان نفوذهاي جديد را تشخيص داد و الگوهاي آنها را به صورت خودکار توليد کرد. بنابراين، نيازي به کد کردن دستي الگوهاي نفوذ جديد




شكل ۱: معماري سيستم تشخيص نفوذ پيشنهادي .

وجود ندارد. هم چنين، مسئول امنيتي شبكه مي‌تواند از چگونگي انجام نفوذهاي جديد اطلاع پيدا نموده و در صورت وقوع نفوذهاي مشابه در آينده واكنش مناسبي نشان دهد.

## معماري سيستم تشخيص نفوذ پيشنهادي

معماري سيستم تشخيص نفوذ پيشنهادي در شكل (۱) نمايش داده شده است. اين سيستم تشخيص نفوذ از اجزاء زير تشكيل مي‌شود:

- واحد پيش‌پردازش
- واحد مدل‌سازي ترافيك عادي شبكه
- واحد تشخيص نفوذهاي شناخته شده
- واحد تشخيص ترافيک غيرعادي شبكه
- واحد توليد الگوهاي نفوذ

در سيستم تشخيص نفوذ پيشنهادي، در مرحله آموزش (شكل ۱ الف)، ابتدا ترافيك عادي شبكه مورد نظر در يك دورة زماني و تحت شرايط كنترل شده جمع‌آوري مي‌شود. سپس در واحد پيش‌پردازش از ترافيک جمع‌آوري شده، رکوردهاي اتصال استخراج مي‌شود. از اين رکوردها در واحد مدل‌سازي ترافيك عادي شبكه براي آموزش تعدادي طبقه‌بند تک كلاسي استفاده مي‌شود. با تركيب اين طبقه‌بندهاي تك كلاسي نماهاي ترافيك عادي شبكه ايجاد مي گردد. بنابراين مرز تصميمي پيدا مي‌شود كه قادر است ترافيك عادي را از ترافيك غيرعادي جدا نمايد.

در مرحله تشخيص (شكل ۱ ب)، واحد پيش‌پردازش رکوردهاي اتصال جديد را از ترافيک شبكه استخراج مي‌كند. اين رکوردهاي اتصال به عنوان ورودي به واحد تشخيص نفوذهاي شناخته شده داده مي‌شوند. در اين واحد، چنانچه هر يك از رکوردهاي اتصال با يكي از الگوهاي نفوذ شناخته شده منطبق گردد، بلافاصله موضوع به اطلاع مسئول امنيتي شبكه رسانده شده, در غير اين صورت، رکوردهاي اتصال به عنوان ورودي به واحد تشخيص ترافيک غيرعادي شبكه داده مي‌شوند. در اين واحد، رکوردهاي اتصال ورودي براساس تركيب نظرات طبقه‌بندهاي تك كلاسي به دو دسته عادي و غيرعادي طبقه‌بندي مي گردند. براي تركيب نظرات طبقه‌بندهاي تك كلاسي از استراتژي رأي اكثريت ($MV^0$) استفاده مي‌شود. در اين استراتژي، ابتدا رکوردهاي اتصال به عنوان ورودي به هركدام از طبقه‌بندهاي تك كلاسي اختصاص يافته سپس، هر رکورد اتصال در صورتي به عنوان غيرعادي تشخيص داده مي‌شود كه توسط اكثر طبقه‌بندهاي تك كلاسي به عنوان غيرعادي طبقه‌بندي شده باشد. چنانچه يك رکورد اتصال به عنوان غيرعادي طبقه‌بندي گردد، به پايگاه رکوردهاي اتصال غيرعادي اضافه مي‌شود. در مرحله يادگيري الگوهاي نفوذ (شكل ۲ ج)، با توجه به

اين كه ركوردهاي اتصال موجود در پايگاه ركوردهاي اتصال غيرعادي ممكن است مربوط به چند نفوذ متفاوت باشند، بنابراين در واحد توليد الگوهاي نفوذ، ابتدا ركوردهاي اتصال غيرعادي با استفاده از يك الگوريتم خوشه‌بندي به تعدادي خوشه تقسيم شده سپس با استفاده از يك روش يادگيري استقرايي، متناظر با هر خوشه يك الگو توليد مي گردد.

در سيستم تشخيص نفوذ پيشنهادي از تركيب هر دو روش‌هاي تشخيص سوءاستفاده و تشخيص رفتار غيرعادي براي تشخيص نفوذ به شبكه‌هاي كامپيوتري استفاده مي‌شود. مزيت سيستم تشخيص نفوذ پيشنهادي نسبت به سيستم‌هاي تشخيص سوء استفاده اين است كه سيستم تشخيص نفوذ پيشنهادي برخلاف اين سيستم‌هاي تشخيص نفوذ قادر به تشخيص نفوذهاي جديد مي‌باشد. هم چنين، مزيت سيستم تشخيص نفوذ پيشنهادي نسبت به سيستم‌هاي تشخيص رفتار غيرعادي اين است كه سيستم تشخيص نفوذ پيشنهادي علاوه بر تشخيص نفوذهاي جديد، قادر به توليد خودكار الگوهاي اين نفوذها مي باشد. بنابراين، مسئول امنيتي شبكه مي‌تواند از چگونگي انجام نفوذهاي جديد اطلاع پيدا كند و در صورت وقوع نفوذهاي مشابه در آينده واكنش مناسبي نشان دهد.

## ارزيابي كارآيي روش پيشنهادي

در اين بخش، آزمايش هاي انجام شده براي ارزيابي كارآيي سيستم تشخيص نفوذ پيشنهادي شرح داده مي‌شود.

### الف. مجموعه داده‌ها

در آزمايش هاي انجام شده براي ارزيابي كارآيي سيستم تشخيص نفوذ پيشنهادي، از مجموعه داده‌هاي آموزشي فراهم شده توسط برنامه ارزيابي تشخيص نفوذ DARPA [۵] استفاده شد. اين مجموعه داده‌ها شامل تقريباً پنج ميليون ركورد اتصال است. هر ركورد اتصال در اين مجموعه داده‌ها شامل ۴۱ ويژگي و داراي برچسب عادي يا يک نوع حمله خاص است. اين حملات را مي‌توان به چهار دسته Probing، DoS، U2R و R2L تقسيم نمود. قبل از انجام آزمايش ها، مقدار هركدام از ويژگي‌هاي ركوردهاي اتصال فوق به بازه ۱- تا ۱ مقياس داده شد.

براي ارزيابي كارآيي سيستم تشخيص نفوذ پيشنهادي، از دو معيار نرخ تشخيص (DR[۶]) و نرخ هشدار نادرست (FAR[۷]) استفاده گرديده است.

### ب. ارزيابي واحدهاي مدل‌سازي ترافيك عادي و تشخيص ترافيک غيرعادي شبكه

براي مدل‌سازي ترافيك عادي شبكه از تركيب طبقه‌بندهاي تك كلاسي PW با هسته گوسي، OCSVM با هسته RBF و GMM استفاده گرديد. سپس از مدل ايجاد شده فوق در واحد تشخيص ترافيك غيرعادي شبكه استفاده گرديد و با استفاده از آن كارآيي اين واحد مورد ارزيابي قرار گرفت.

بدين منظور، ابتدا مجموعه ركوردهاي اتصال عادي به سه دسته تقسيم شد. از دسته اول براي آموزش هركدام از طبقه‌بندهاي تك كلاسي، از دسته دوم براي تعيين مقدار حد آستانه $\theta$ در طبقه‌بندهاي تك كلاسي PW و GMM، و از دسته سوم براي تعيين نرخ هشدار نادرست (*FAR*) واحد تشخيص ترافيك غيرعادي شبكه استفاده شد.

براي تعيين نرخ تشخيص (DR) واحد تشخيص ترافيك غيرعادي شبكه، از ركوردهاي اتصال با برچسب‌هاي Probing، DoS، U2R و R2L استفاده گرديد.

جدول ۱: نرخ تشخيص و نرخ هشدار نادرست تركيب نظرات طبقه‌بندهاي تک كلاسي **PW**، **OCSVM** و **GMM** .

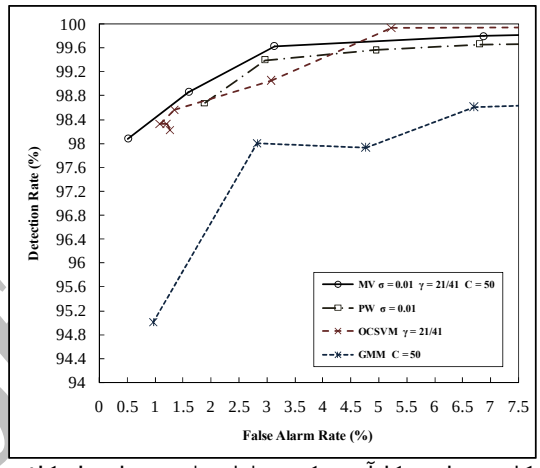
| | **Detection Rate (%)** | | | | **False Alarm Rate (%)** |
|---|---|---|---|---|---|
| | **Probing** | **DoS** | **U2R** | **R2L** | |
| $AR = 0.99$ $v = 0.005$ | **98.08** | **99.51** | **59.61** | **28.95** | **0.51** |
| $AR = 0.97$ $v = 0.025$ | **98.86** | **99.56** | **71.15** | **51.06** | **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 تشخيص و نرخ هشدار نادرست واحد تشخيص ترافيك غيرعادي شبكه به ازاء مقادير مختلف عامل *AR* مربوط به طبقه‌بندهاي تك كلاسي PW و GMM و پارامتر $v$ مربوط به طبقه‌بند تك كلاسي OCSVM نمايش داده شده است.

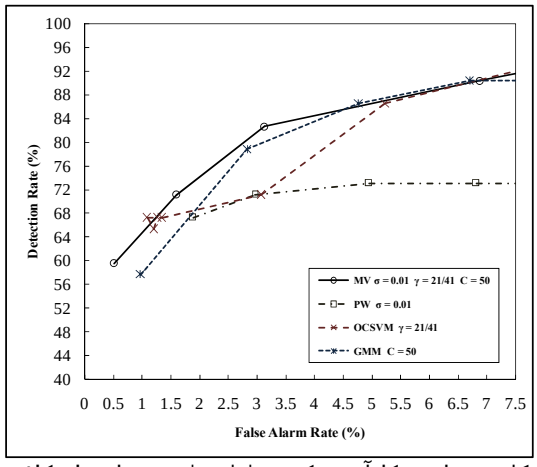
در آزمايش هاي انجام شده، براي طبقه‌بند تك كلاسي PW عامل $\sigma = 0.01$، براي طبقه‌بند تك كلاسي OCSVM عامل $\gamma = 21/41$ و براي طبقه‌بند تك كلاسي GMM

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** .

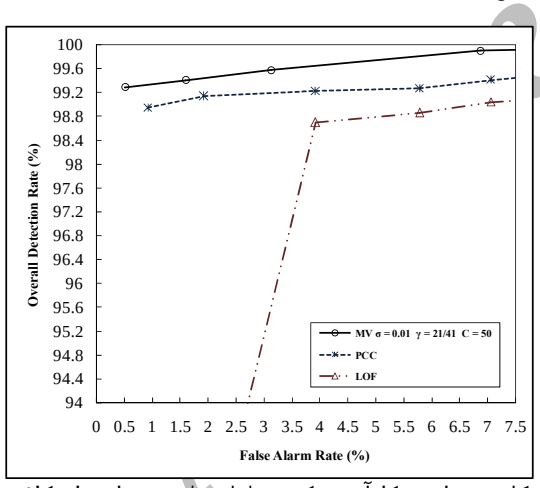
با مقایسه شکل‌های (۲) و (۳) مشخص می‌شود که با ترکیب نظرات طبقه‌بندهای تک کلاسی PW، OCSVM و GMM با استراتژی رأی اکثریت توازن بهتری میان نرخ تشخیص و نرخ هشدار نادرست واحد تشخیص ترافیک غیرعادی شبکه برقرار می‌شود.

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 نموده اند. 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. نتايج آزمايش ها نشان مي‌دهد كه روش PCC داراي كارآيي بالاتري نسبت به روش‌هاي KNN و LOF مي باشد. در شكل (۴) كارآيي استراتژي رأي اكثريت براي تركيب نظرات طبقه‌بندهاي تك كلاسي PW، OCSVM و GMM با كارآيي روش‌هاي PCC [۷] و LOF [۸] براي تشخيص ترافيك غيرعادي شبكه مقايسه شده است. با توجه به شكل (۴) مشخص مي‌شود كه با تركيب نظرات طبقه‌بندهاي تك كلاسي PW، OCSVM و GMM با استراتژي رأي اكثريت نرخ تشخيص كلي بالاتري نسبت به روش‌هاي PCC [۷] و LOF [۸] به دست مي‌آيد.

ج. ارزيابي واحد توليد الگوهاي نفوذ

براي ارزيابي واحد توليد الگوهاي نفوذ، ابتدا ۶۰۰۰۰ ركورد اتصال با برچسب Normal به صورت تصادفي انتخاب گرديد كه از آنها براي آموزش طبقه‌بندهاي تك كلاسي PW، OCSVM و GMM استفاده شد. براي مدل‌سازي ترافيك عادي و تشخيص ترافيك غيرعادي شبكه، تركيب طبقه‌بندهاي تك كلاسي فوق با استراتژي رأي اكثريت مورد استفاده قرار گرفته است. سپس، ۶۰۰۰۰ ركورد اتصال ديگر با برچسب‌هاي Normal، Smurf و Neptune به صورت تصادفي انتخاب گرديد. نفوذهاي موجود در اين مجموعه داده‌ها به عنوان نفوذهاي جديد در نظر گرفته شده و مجموعه داده‌هاي فوق به عنوان ورودي به واحد تشخيص ترافيک غيرعادي شبكه داده شد. در اين واحد، به هركدام از ركوردهاي اتصال ورودي برچسب عادي يا غيرعادي الصاق گرديد.

در آزمايش هاي انجام شده، براي طبقه‌بندهاي تك كلاسي PW، OCSVM و GMM عامل هاي $\sigma = 0.01$، $\gamma = 21/41$، $\nu = 0.025$، $C = 50$ و $AR = 0.97$ در نظر گرفته شد.

ركوردهاي اتصال غيرعادي تشخيص داده شده توسط واحد تشخيص ترافيک غيرعادي شبكه به عنوان ورودي به واحد توليد الگوهاي نفوذ داده شد. در اين واحد، ابتدا مجموعه داده‌هاي ورودي با استفاده از الگوريتم شبكه عصبي SOM خوشه‌بندي گرديد. در آزمايش ها براي خوشه‌بندي ركوردهاي اتصال غيرعادي، از يك SOM با شبكه خروجي ۲*۲ استفاده شد. آموزش شبكه در دو مرحله انجام گرديد. در مرحله اول از يك نرخ يادگيري اوليه بزرگ ($\alpha = 0.5$) و در مرحله دوم از يك نرخ يادگيري اوليه كوچك ($\alpha = 0.05$) استفاده شد. در طي آموزش، نرخ يادگيري به صورت خطي به صفر كاهش يافته است.

پس از خوشه‌بندي، به داده‌هاي مربوط به هر خوشه برچسب نفوذ زده شد. اين داده‌ها همراه با داده‌هايي كه برچسب عادي داشتند، به عنوان ورودي به سيستم يادگيري قانون C4.5 [۹] داده شد. با استفاده از اين سيستم يادگيري قانون، براي هر كدام از خوشه‌ها يک قانون توليد گرديد. اين قوانين كه در شكل (۵) نمايش داده شده‌اند، الگوهاي نفودهاي فوق را توصيف مي‌كنند. قانون اول بيانگر اين مطلب است كه در نفوذ با برچسب Intrusion1 تعداد زيادي بسته ICMP به ميزبان مقصد ارسال مي‌شود و قانون دوم هم بيان مي‌كند كه در نفوذ با برچسب Intrusion2 تعداد زيادي بسته SYN به قسمت خاصي از ميزبان مقصد ارسال مي گردد. بنابراين با توجه به اين قوانين مي‌توان نتيجه گرفت كه نفوذهاي فوق از نوع جلوگيري از سرويس مي‌باشند.

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

تفسير قانون: اگر سرويس اتصال جاري icmp echo request باشد و در ۲ ثانيه گذشته، تعداد اتصالاتي كه سرويس يكساني با اتصال جاري دارند بيشتر از ۳۲۵ باشد، آنگاه اين رفتار نشان دهندة نفوذ است.

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

تفسير قانون: اگر اتصال جاري با خطاي SYN خاتمه يافته باشد و در ۲ ثانيه گذشته، درصد خطاهاي SYN در اتصالاتي كه سرويس يكساني با اتصال جاري دارند بيشتر از ۵۰ درصد باشد، آنگاه اين رفتار نشان دهندة نفوذ است.

شكل ۵: الگوهاي نفوذ توليد شده با استفاده از روش پيشنهادي.

د. ارزيابي واحد تشخيص نفوذهاي شناخته شده

الگوهاي (به عبارت ديگر، قوانين) توليد شده در بخش قبلي براي نفوذهاي Intrusion1 و Intrusion2 به پايگاه الگوهاي نفوذ شناخته شده اضافه گرديد. براي ارزيابي واحد تشخيص نفوذهاي شناخته شده، ابتدا ۶۰۰۰۰ ركورد اتصال با برچسب‌هاي Normal، Smurf و Neptune به صورت تصادفي انتخاب گرديد. در اين مجموعه داده ها، ۳۰۰۰۰ ركورد اتصال داراي برچسب Normal، ۱۵۰۰۰ ركورد اتصال داراي برچسب Smurf و ۱۵۰۰۰ ركورد اتصال داراي برچسب Neptune بود. سپس از الگوهاي نفوذ موجود در پايگاه الگوهاي نفوذ شناخته شده براي طبقه‌بندي اين ركوردهاي اتصال استفاده گرديد. نتايج به دست آمده در

جدول (۳) نمايش داده شده است.

جدول ۳: طبقه‌بندي رکوردهاي اتصال ورودي با استفاده از الگوهاي نفوذ توليد شده .

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

با توجه به جدول (۳) مشخص مي‌شود که با استفاده از الگوهاي نفوذ توليد شده مي‌توان نفوذهاي Smurf و Neptune را با دقت بالا (۹۹/۶۰% و ۹۹/۹۸%) تشخيص داد، در حالي که هشدار نادرست اعلام شده توسط سيستم تشخيص نفوذ بسيار ناچيز (۰/۰۰۳%) است.

## نتيجه‌گيري

در اين مقاله، روشي براي توليد خودکار الگوهاي نفوذ جديد پيشنهاد گرديد. به منظور ارزيابي روش پيشنهادي از مجموعه داده‌هاي فراهم شده توسط برنامه ارزيابي تشخيص نفوذ DARPA استفاده گرديد. در آزمايش هاي انجام شده، براي تشخيص ترافيك غيرعادي شبکه از ترکيب نظرات طبقه‌بندهاي تك کلاسي PW با هسته گوسي، OCSVM با هسته RBF و GMM استفاده شد. براي توليد الگوهاي نفوذ جديد از سيستم يادگيري قانون C4.5 استفاده گرديد.

## 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