سیستم تشخیص نفوذ آنومالی مبتنی بر جریان با استفاده از طبقه‌بندی جمعی و مقیاس تأثیر ویژگی

۱. سپیده حیدرپور

دانشجوی کاردانی فناوری اطلاعات دانشکده ملی مهارت ولیعصر(عج) تهران

۲. دکتر نسترن بیرانوند

مدرس گروه کامپیوتر دانشکده ملی مهارت ولیعصر(عج) تهران

چکیده

با افزایش حجم ترافیک شبکه و تنوع حملات، تشخیص دقیق حملات به یک چالش بزرگ تبدیل شده است. روش‌های سنتی مبتنی بر ویژگی‌های سطح بسته، به دلیل تغییرات مداوم در رفتار شبکه، کارایی کافی ندارند. این مقاله روشی جدید برای تشخیص حملات شبکه مبتنی بر یادگیری ماشین ارائه می‌دهد. در این روش، ویژگی‌های ترافیک در سطح جریان (به جای سطح بسته) استخراج می‌شوند. این ویژگی‌ها مستقل از تغییرات شبکه هستند و عملکرد سیستم را بهبود می‌بخشند. مجموعه‌ای از ویژگی‌های منحصر به فرد جریان تعریف شده و از داده‌های ترافیک استخراج می‌شود.از آزمون کولموگروف-اسمیرنوف برای آموزش مدل و شناسایی تفاوت‌های بین رفتار جریان‌های عادی و حملات استفاده می‌شود. برای طبقه‌بندی جریان‌ها، از طبقه‌بندهای جمعی و ارزیابی مقیاس متاهیوریستیک استفاده می‌شود. نتایج آزمایش‌ها نشان می‌دهد که روش پیشنهادی دقت تشخیص بالاتری نسبت به روش‌های قبلی دارد و نرخ هشدار کاذب کمتری تولید می‌کند. همچنین، زمان پردازش این روش نیز کمتر است. این روش جدید می‌تواند به طور موثر در تشخیص انواع مختلف حملات شبکه مورد استفاده قرار گیرد و امنیت شبکه‌ها را افزایش دهد.

کلیدواژه‌ها :سیستم‌های تشخیص نفوذ آنومالی، طبقه‌بندهای جمعی، رویکردهای یادگیری ماشین، مقیاس متاهیوریستیک،

آزمون کولموگروف-اسمیرنوف(K–S Test) .

۱. مقدمه

در دنیای امروز، تعداد دستگاه‌های متصل به اینترنت به طور فزاینده‌ای در حال افزایش است. این دستگاه‌ها برای ارتباط در برنامه‌های تجاری و فردی استفاده می‌شوند. اگرچه استاندارد زندگی ما با ارتباطات بین دستگاه‌ها بهبود یافته است، اما حملات سایبری به طور فزاینده‌ای پیچیده‌تر و بزرگ‌تر شده‌اند. رایج‌ترین حملات سایبری، حملات Denial of Service (DoS) و Distributed Denial of Service (DDoS) هستند. در عصر مدرن، مهاجمان/هکرها از ابزارهای پیچیده‌تری برای ایجاد حملات سیلابی در شبکه، لایه انتقال و لایه کاربرد مدل مرجع استفاده می‌کنند. حملات سیلابی بار شبکه را افزایش می‌دهند و ترافیک مخرب با حجم بالا را به طور مجازی تولید می‌کنند که حداکثر پهنای باند را مصرف می‌کند. بنابراین، سیستم هدف نمی‌تواند خدمات را به کاربران مجاز خود ارائه دهد و این منجر به حمله Denial-of-Service (DoS) می‌شود. مهاجمان DDoSنه تنها هدفشان این است که خدمات را غیرقابل دسترسی کنند، بلکه ممکن است به دنبال دسترسی نامحدود به سیستم قربانی باشند که می‌تواند منجر به آسیب‌های بیشتری شود. در لایه کاربرد، رفتار حملات DoS/Ddos با سایر لایه‌ها متفاوت است. بنابراین، سیستم‌های تشخیص نفوذ (IDS) نقش حیاتی در شناسایی حملات DoS و DDoS ایفا می‌کنند.

۱.۱ انگیزه

سیستم تشخیص نفوذ (IDS) یک ابزار مدیریت امنیتی است که اطلاعات را از شبکه‌ها جمع‌آوری کرده و سوابق را برای بررسی رفتار غیرعادی در شبکه تحلیل می‌کند. بر اساس اطلاعات جمع‌آوری‌شده برای تحلیل، IDSبه دو کلاس اصلی تقسیم می‌شود IDS مبتنی بر میزبان و IDSمبتنی بر شبکه علاوه بر این دسته‌بندی، IDS به دو نوع تشخیص تقسیم می‌شود: ۱.تشخیص سوءاستفاده ۲.تشخیص انحراف یا ترکیبی بر اساس استراتژی تشخیص

تشخیص مبتنی بر سوءاستفاده که به آن سیستم تشخیص مبتنی بر امضا نیز گفته می‌شود، از الگوهای از پیش تعریف‌شده حملات در یک پایگاه داده استفاده می‌کند. این تکنیک سوابق را بر اساس الگوها یا امضاهای خاص ذخیره‌شده در پایگاه داده تحلیل می‌کند و فقط می‌تواند الگوهای حملاتی را که در پایگاه داده ذخیره شده‌اند، شناسایی کند. این روش نمی‌تواند حملات جدید یا روز صفر را شناسایی کند.

تشخیص مبتنی بر انحراف رفتار عادی سیستم یا شبکه را تخمین می‌زند. وقتی رکوردی وارد می‌شود، انحراف رفتار آن رکورد با رفتار عادی بررسی می‌شود. اگر این انحراف از مقدار آستانه از پیش تعیین‌شده فراتر رود، به عنوان انحراف پیش‌بینی می‌شود. این روش می‌تواند حملات جدید و روز صفر را شناسایی کند.

منبع داده‌ای که برای تحلیل IDS مبتنی بر شبکه (NIDS) استفاده می‌شود، به دو دسته تقسیم می‌شود: مبتنی بر بسته و مبتنی بر جریان. بررسی ویژگی‌های کامل ترافیک به عنوان NIDS مبتنی بر بسته (PNIDS) شناخته می‌شود،

در حالی که بررسی اطلاعات تجمعی مربوط به سوابق ترافیک به صورت جریان به NIDS مبتنی بر جریان (FNIDS) معروف است.

اگرچه PNIDS دقت تشخیص بالایی با نرخ‌های پایین هشدار کاذب تولید می‌کند، این فرآیند زمان‌بر است. انجام یک رویکرد مبتنی بر بسته در نرخ‌های چند گیگابایت در ثانیه (GBPS) دشوار و گاهی غیرممکن است FNIDS .به دلیل حجم کمتری از داده‌ها برای پردازش، به طور منطقی برای شبکه‌های با سرعت بالا انتخاب می‌شود.

برای یادگیری رفتار جریان‌های ترافیک عادی، بهترین الگوریتم‌های مناسب، الگوریتم‌های یادگیری ماشین (ML) هستند. معمولاً برای اندازه‌گیری انحرافات، یک مقدار آستانه تعیین می‌شود تا رفتار عادی و حمله را تفکیک کند. با توجه به اینکه روش‌های DDoS به طور مداوم در حال افزایش هستند، تعیین دستی مقادیر آستانه در تکنیک‌های تشخیص مبتنی بر رفتار به شدت ضروری است. به طور کلی، تکنیک‌های تشخیص مبتنی بر رفتار به چهار دسته تقسیم می‌شوند: خوشه‌بندی، آماری، نظریه اطلاعات و تکنیک‌های طبقه‌بندی که برای شناسایی حملات DoS/DDoS استفاده می‌شوند.

از سال ۲۰۰۰، مطالعات زیادی در زمینه شناسایی حملات DoS/DDoS انجام شده است. بیشتر این مطالعات به تحلیل رفتارهای سطح شبکه یا ترافیک برای دسته‌بندی عادی و نفوذها وابسته هستند.ترافیک اینترنت شامل بسته‌های داده‌ای است که بین دو طرف برای ارتباط برقرار می‌شود و جریان‌های ترافیکی عظیمی را در شبکه‌ها تولید می‌کند. ویژگی‌های استخراج‌شده از جریان ترافیک بسته‌ها نقش حیاتی در تعریف راه‌حل‌ها برای شناسایی و کاهش حملات سایبری ایفا می‌کند. ویژگی‌های مربوط به جریان‌های ترافیک بر روش‌های استفاده‌شده برای شناسایی و دفاع در برابر حملات DDoS تأثیر می‌گذارد. خواص مرتبط با درخواست‌ها مانند زمان‌های بین‌جلسه یا جلسات، جریان ترافیک را تعریف می‌کند. در شبکه‌های یک‌طرفه، ویژگی‌های مورد استفاده برای بسته‌های داده معمولاً شامل شماره پورت، IPمنبع و IP مقصد است.

درIPFIX ، نویسندگان یک انتخاب انعطاف‌پذیر از عملکردها با اطلاعات اضافی متفاوت از ویژگی‌های موجود در بسته‌های داده پیشنهاد کرده‌اند. در هسته تحلیل یا جریان بسته، سطوح دسترسی به داده‌ها ویژگی‌های اصلی تمایز هستند. وقتی به تمام داده‌های ارتباطی دسترسی کامل وجود داشته باشد، تحلیل بسته‌ها مؤثرترین حالت است که در آن لاگ‌های جریان متاداده‌ای برای ارتباط فراهم می‌کنند. آمارهای اصلی مورد استفاده شامل تعداد بسته‌ها، پروتکل ترافیک، و مدت زمان جریان و آدرس‌های نقاط انتهایی است.جریان ترافیک ورودی در فایروال‌ها یا سیستم‌های تشخیص نفوذ (IDS) نیاز به استراتژی‌های بازرسی عمیق بسته‌ها برای تحلیل حملات در لایه کاربرد دارد. فعالیت‌های مخرب مانند نفوذهای شبکه و آسیب‌پذیری‌های حمله از جریان ترافیک ورودی شناسایی می‌شوند. با این حال، استراتژی‌های بازرسی عمیق در شناسایی نفوذها و حملات ناشی از سیلاب درخواست‌ها ناکام مانده‌اند.

این مقاله عمدتاً بر روی کاهش و شناسایی انواع مختلف حملات از حجم بالای ترافیک تمرکز دارد. سیلاب حجم بالای ترافیک به سمت سیستم هدف منجر به ازدحام در لینک‌های ارتباطی می‌شود و کانال را مسدود می‌کند و مانع از انتقال ترافیک به سیستم هدف می‌شود.

۱.۲فرموله‌سازی مشکل و هدف

تشخیص ترافیک به عنوان عادی یا حمله در سطح جریان بسیار دشوار است و چندین محقق این مشکل را با استفاده از الگوریتم‌های مختلف یادگیری ماشین مورد بررسی قرار داده‌اند. با این حال، این الگوریتم‌های یادگیری ماشین ویژگی‌ها را از بسته‌های کنترل یا داده استخراج می‌کنند تا ترافیک را به عنوان عادی یا حمله تأیید کنند.

این الگوریتم‌ها بیشتر به ویژگی‌های سنتی مانند سرعت انتقال، اندازه متوسط بسته‌ها و زمان ورود بسته‌ها وابسته هستند. در سناریوهای واقعی، ترافیک از منابع متنوعی تولید می‌شود و تنوع در تراکنش‌ها یا ویژگی‌های مرتبط با تراکنش‌ها وجود دارد که نمایانگر عادی یا حمله است. تنوع عملکردها یا ویژگی‌های خاص فرصتی برای حمله‌کنندگان ایجاد می‌کند تا حملات را بر روی قربانی انجام دهند. الگوریتم‌های سنتی یادگیری ماشین نتوانسته‌اند این رفتار متنوع تراکنش‌ها را برای تشخیص ترافیک به عنوان عادی یا حمله مدیریت کنند. این امر نیاز به طبقه‌بندهای

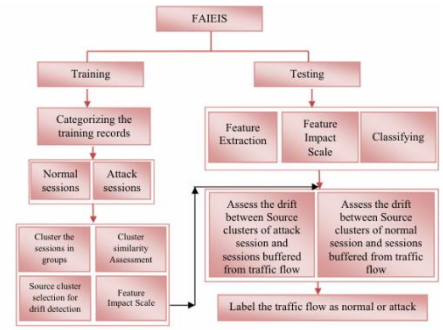
ترکیبی یا روش‌های یادگیری پیشرفته را ایجاب می‌کند، اما این روش‌های یادگیری پیچیدگی فرآیند را به دلیل ویژگی‌های پیوسته و متنوع به جای ویژگی‌های دسته‌ای افزایش می‌دهند.

برای پاسخ به این نیاز، این مقاله ویژگی‌های منحصر به فرد جریان را تعریف کرده است تا ترافیک را در سطح جریان به جای سطح بسته مدیریت کند و از وابستگی به ویژگی‌ها برای مدیریت ترافیک متنوع از محیط‌های توزیع‌شده جلوگیری کند. استدلال اصلی در این مقاله این است که افزایش حجم ترافیک منجر به افزایش میانگین فاصله مربعی مورد نیاز برای ویژگی‌های خاص می‌شود و همچنین ویژگی‌ها به دلیل ماهیت احتمالی به جای ماهیت قطعی بی‌اهمیت می‌شوند.

۲.کارهای مرتبط

تحلیل جریان ترافیک یا تحلیل داده‌ها یا منبع داده‌ها، سیاست اصلی تشخیص است که توسط اکثر روش‌ها برای شناسایی هرگونه ناهنجاری در شبکه یا سیستم استفاده می‌شود. در این بخش، قوت‌ها و ضعف‌های روش‌های موجود در وضعیت کنونی مورد بحث قرار می‌گیرد.

۳.مدل پیشنهادی در این مقاله، فرآیند تشخیص حمله در دو مرحله پیشنهاد شده است: آموزش و تشخیص. در مرحله آموزش، ترافیک به صورت جلساتی که به عنوان دسته‌های عادی و حمله برچسب‌گذاری شده‌اند، استفاده می‌شود. علاوه بر این، جلسات در مرحله آموزش که به عنوان عادی یا حمله دسته‌بندی شده‌اند، گروه‌بندی شده و ویژگی‌های گروه‌های جلسه استخراج می‌شود. مراحل دیگر شامل یافتن شباهت بین توزیع گروه‌ها، شناسایی رهبر در میان گروه و در نهایت تعریف مقیاسی برای پیش‌بینی به عنوان حمله یا عادی است. توضیحات دقیق‌تری از فرآیند پیشنهادی در بخش‌های بعدی ارائه شده است. جریان عملکرد/فرآیند مدل پیشنهادی، FAIEISدر شکل ۱ نشان داده شده است.



شکل ۱

FAIEIS با استفاده از تکنیک‌های خوشه‌بندی، الگوهای رفتاری نرمال و حملات را در شبکه شناسایی می‌کند. در مرحله آموزش، این الگوها مدل‌سازی می‌شوند و در مرحله تست، داده‌های جدید با این مدل مقایسه شده و برچسب‌گذاری می‌شوند. این سیستم به ویژه برای تشخیص حملات جدید و ناشناخته مفید است، زیرا می‌تواند انحرافات از الگوهای نرمال را شناسایی کند.(شکل۱)

۳.۱گروه‌بندی جلسات به خوشه‌ها ترافیک از شبکه جمع‌آوری شده و با فواصل زمانی ثابت به عنوان جلسات تعریف می‌شود. جلسات به خوشه‌ها گروه‌بندی می‌شوند، زیرا ترافیک از شبکه یا محیط‌های توزیع شده به صورت جلسات جمع‌آوری می‌شود و جلسات با فواصل زمانی همپوشانی در یک خوشه قرار می‌گیرند و این کار با خوشه‌بندی انجام می‌شود. خوشه‌بندی جلسات به طور مستقل به هر دو نوع ترافیک عادی و حمله در مرحله آموزش اعمال می‌شود تا خوشه‌ها تعریف شوند. فرآیند خوشه‌بندی در الگوریتم خوشه‌بندی-جلسات تعریف شده و نمادهای استفاده شده در این الگوریتم ۱ در جدول ۱ نشان داده شده است.

```
Algorithm Clustering-Sessions ( )
Begin
    Loop 1: while(|TS| > 0)
    Begin
        cl_k = {s_1 ∃ s_1 ∈ TS} scl_k ← cl_k
        ncl_k ← cl_k
        Loop 2: ∀_{i=1}^{|TS|}{s_i ∃ s_i ∈ TS ∧ s_i ≠ cl_k} begin
            if(bt(s_i) < et(cl_k))Begin
            scl_k ← s_i
                if(et(s_i) < et(cl_k))Begin
                ncl_k ← s_i
                End
            End
        End
        if(cl_k ≠ ncl_k)Begin
                cl_k = ncl_k
        scl_j = null
            Go to loop 2
        End
        elseif(cl_k ≡ ncl_k)Begin
        TS = {TS \ scl_k}
        k = k + 1
        End
    End
End
```

۳.۲ویژگی‌های تعریف شده برای اعتبارسنجی شباهت خوشه در سطح جریان ترافیک ورودی از شبکه یا محیط‌های توزیع شده به خوشه‌های عادی یا حمله تبدیل می‌شود با گروه‌بندی جلسات به عنوان خوشه‌ها بر اساس فواصل زمانی همپوشانی آن‌ها.

تنوع ویژگی‌ها یا خصوصیات با شباهت خوشه اندازه‌گیری می‌شود. برای مدیریت این موضوع در سطح جریان، در این مقاله مجموعه‌ای منحصر به فرد از ویژگی‌ها تعریف شده و داده‌ها از خوشه‌ها با استفاده از این ویژگی‌ها استخراج می‌شود. فهرست ویژگی‌های منحصر به فرد برای نمایندگی جریان ترافیک در زیر نشان داده شده است.

- فواصل شروع جلسه :این ویژگی از یک جریان جلسات به عنوان زمان سپری شده بین زمان شروع اولین جلسه و زمان شروع دومین جلسه ارزیابی می‌شود. این ویژگی فراوانی جلسات تشکیل شده در خوشه را از ترافیک ورودی تعریف می‌کند.
- فواصل پایان جلسه :این ویژگی از یک جریان جلسات به عنوان زمان سپری شده بین زمان پایان اولین جلسه و زمان پایان دومین جلسه ارزیابی می‌شود. این ویژگی مدت زمان جلسات در خوشه را تعریف می‌کند.
- زمان شروع دسترسی به صفحه :در یک توالی از صفحات، زمان شروع دسترسی به صفحه به عنوان فاصله زمانی بین دسترسی به یک صفحه و صفحه دیگر محاسبه می‌شود. این ویژگی فراوانی تغییر صفحات با درخواست دسترسی توسط یک مهاجم را تعریف می‌کند.
- زمان پایان دسترسی به صفحه :در یک توالی از صفحات، زمان پایان دسترسی به صفحه به عنوان فاصله زمانی بین زمان پایان دسترسی به یک صفحه و صفحه دیگر محاسبه می‌شود. این ویژگی مهم است زیرا مقدار زمانی که مهاجم در هر صفحه یا خدمات با درخواست ورودی صرف می‌کند را تعریف می‌کند.
- مصرف پهنای باند در سطح جلسه :مقدار پهنای باند مصرف شده توسط تمام درخواست‌ها در یک جلسه مشخص محاسبه می‌شود. این ویژگی نوع ترافیک را بر اساس مقدار پهنای باند مصرف شده توسط تراکنش‌های عادی یا حمله در یک جلسه مشخص از خوشه تعریف می‌کند. وقتی تعداد جلسات افزایش یابد، این امر منجر به سیل درخواست‌ها برای مسدود کردن هدف یا خدمات می‌شود.
- تعداد مطلق جلسات :میانگین تعداد جلسات موجود در یک خوشه با استفاده از این ویژگی ارزیابی می‌شود و بار متوازن‌سازی بر روی سرورها را تعریف می‌کند.
- تعداد مطلق دسترسی به صفحات :این ویژگی تعداد متوسط صفحات دسترسی یافته در یک خوشه مشخص را تعریف می‌کند. این ویژگی به تعیین تعداد قربانیان یا خدمات هدف‌گذاری شده با درخواست‌های هدایت شده به صفحات مختلف در یک برنامه وب کمک می‌کند.

- نسبت تنوع منبع :(SR) اگر ترافیک از محیط توزیع شده باشد، این ویژگی میانگین تعداد سیستم‌های منبع مربوط به تولید جریان ترافیک در یک خوشه مشخص را شناسایی می‌کند. این یک ویژگی مهم برای تحلیل رفتار متنوع مهاجم با خصوصیات ترافیک متنوع از محیط‌های توزیع شده است.

- نسبت فواصل بین تراکنش‌ها :وقتی توالی تراکنش‌ها در یک دوره زمانی خاص تکرار می‌شود، این ویژگی برای ارزیابی زمان دسترسی الگوهای خاص یا جفتی از چنین تراکنش‌ها در یک جلسه مشخص از هر خوشه استفاده می‌شود.

جدول نمادگذاری الگوریتم خوشه‌بندی جلسات

$SL = \{s_1, s_2, ...s_{\|SL\|}\}$: Sorted list contains sessions in ascending order of session begin time.
$TS \leftarrow SL$: Clone to sorted sessions list.
$bt(s_i)$: begin time of the session s_i
$et(s_i)$: completion time of the session s_i
scl_k: k^{th} cluster, that to be formed, where, the initial value of k is 1

جدول ۱

۳.۳ ارزیابی شباهت خوشه

ترافیک از شبکه به‌صورت جلسات جمع‌آوری می‌شود و این جلسات بر اساس زمان‌های همپوشانی به خوشه‌ها گروه‌بندی می‌شوند تا جریان را تعریف کنند. داده‌ها از این خوشه‌ها با ویژگی‌های جریانی که در بخش ۳.۲ تعریف شده‌اند استخراج می‌شوند. این ویژگی‌ها نسبت به استخراج داده‌ها در سطح بسته، وابستگی کمتری دارند. زمانی که ویژگی‌ها مستقل از شبکه یا ویژگی‌های جریان ترافیک باشند، تأثیر کمتری بر فرآیند شناسایی یا اعتبارسنجی خواهند داشت. شباهت خوشه‌ها با استفاده از آزمون کولموگروف-اسمیرنوف (K–S Test) محاسبه می‌شود تا رفتارهای مشابه را در یک بسته واحد گروه‌بندی کند. آزمون K–S خوشه‌ها را بر اساس شباهت رفتار یا توزیع به چندین گروه تقسیم می‌کند که رفتارهای مختلف جریان ترافیک را نشان می‌دهد. شباهت توزیع خوشه‌ها دارای خاصیت متقارن) اگر x = y ، آنگاه (y = x و خاصیت انتقالی) اگر x = y و y = z، آنگاه (x = z است. الگوریتم ارزیابی شباهت در الگوریتم ۲ ارائه شده و نمادهای استفاده شده در آن در جدول ۲ فهرست شده‌اند.

۳.۴ انتخاب خوشه منبع از گروه‌های خوشه

الگوریتم شباهت خوشه، خوشه‌ها را به گروه‌های جداگانه بر اساس شباهت توزیع نگه می‌دارد، که مشخص می‌کند خوشه‌ها در یک گروه مشترک قرار دارند و رفتار یکسانی دارند. تعداد این رفتارها یا ویژگی‌های مختلف جریان، بر اساس تعداد گروه‌های تشکیل شده از جلسات جریان ترافیک ورودی به گروه‌های خوشه تعیین می‌شود. با این حال، خاصیت انتقالی (اگر x = y و y = z ، آنگاه (x = z و خاصیت متقارن توزیع)اگر x = y ، آنگاه y = x) در آزمون شباهت خوشه بین خوشه‌ها در یک گروه یا بین گروه‌های خوشه، پیچیدگی فرآیند را با انتخاب یک منبع از هر گروه خوشه برای نمایندگی رفتار آن گروه کاهش می‌دهد. این سرخوشه‌های انتخاب شده به عنوان منبعی برای شناسایی در میان جریان‌های ترافیک استفاده می‌شوند.

۳.۵ شناسایی نفوذ با استفاده از مقیاس تأثیر ویژگی

مقیاس ارتباط متا-هوریستیک که به عنوان مقیاس تأثیر ویژگی نیز شناخته می‌شود، بر اساس ویژگی‌های استخراج شده از خوشه‌ها که در بخش ۳.۲ تعریف شده‌اند، محاسبه می‌شود. برای تشکیل مجموعه داده‌های معاملات شبکه، فرض کنید.

۴.مطالعه تجربی

۴.۱مجموعه داده‌های حمله

مدل پیشنهادی دفاع و شناسایی حمله با استفاده از انواع مختلف مجموعه داده‌های لاگ حملات مانند حمله انکار سرویس(DoS) ، حمله پروب (Probe)، حمله محلی به وعده‌ها (R۲L) و حمله کاربر به ریشه (U۲R) از KDD۹۹ ، NSL-KDD، CIDIAو غیره اعتبارسنجی شده است. مجموعه داده KDD۹۹ شامل تعداد زیادی تکرار، درخواست‌های خراب و درخواست‌های جعلی به دلیل تکرار گسترده درخواست‌ها در این مجموعه داده است و مجموعه داده NSL-KDD برای اعتبارسنجی مدل پیشنهادی استفاده می‌شود. با این حال، یکی از چالش‌های اصلی برای اعتبارسنجی هر سیستم شناسایی نفوذ (IDS) کمبود مجموعه داده‌های مناسب یا مناسب است.

آموزش و آزمایش مدل با استفاده از مجموعه داده NSL-KDD انجام می‌شود، جایی که ۳۰٪ یا ۲۷،۹۴۰،۲۰ درخواست نرمال یا حمله برای آموزش مدل استفاده می‌شود و ۷۰٪ باقی‌مانده برای آزمایش در نظر گرفته می‌شود. درخواست‌هایی که رفتار نرمال دارند به عنوان "نرمال" فرض می‌شوند و معاملاتی که از این نرمال منحرف شده‌اند به عنوان "حمله" شناخته می‌شوند.مجموعه داده NSL-KDD شامل چهار دسته اصلی حمله زیر است:

- حمله انکار سرویس :(DoS) هدف اصلی مهاجم در این دسته، مسدود کردن درخواست‌های قانونی است که پردازش نمی‌شوند. برخی از مثال‌ها شامل حملات"tear" ، "death ping"، "Neptune"، "mail bomb"، "earth"و "smurf" هستند.
- حمله پروب :(PROBE) هدف مهاجم این است که به عنوان یک کاربر مخفی عمل کند و اطلاعاتی از شبکه کاربر قانونی یا سیستم فردی جمع‌آوری کند. مثال‌هایی از این دسته شامل"satan" ، "nmap"، "port sweep"و "sweep" هستند.
- حمله کاربر به ریشه :(U۲R) هدف مهاجم این است که با بهره‌برداری از آسیب‌پذیری‌ها و با استفاده از اعتبارنامه‌های جعلی، به دسترسی ریشه دست یابد. مثال‌هایی شامل"Buffer overflow" ، "rootkit"، "perl"و "load module" هستند.

نتایج ارزیابی عملکرد یک مدل تشخیص نفوذ به نام FAIS

Total number of attack prone requests	307,292
Total number of salubrious or normal requests	307,544
Positives used in training	215,281
Negatives used in training	215,280
Positives used in testing	92,188
Negatives used in testing	92,263
TP (true positives)	80,480
FP (false positives)	10,702
TN (true negatives)	81,561
FN (false negatives)	11,708
PPV (positive predict value)	0.8826
TPR (true positive rate)	0.873
TNR (true negative rate)	0.8745
DA (detection accuracy)	0.8785
FAR (false alarming rate)	0.1174

جدول ۳

نتایج ارزیابی عملکرد مدل تشخیص نفوذ BIFAD

Number of absolute time intervals (ATI)	435,936 (222,987:RTF, 212,949:RTN)
Number of ATIs used in training	302,813 (154,872:RTF, 147,941:RTN)
Number of ATIs used in testing	133,123 (68,115:RTF, 65,008:RTN)
Records showed as attack prone	69,549
Records showed as normal	63,574
TP (true positives)	61,423
FP (false positives)	8126
TN (true negatives)	56,882
FN (false negatives)	6692
PPV (positive predict value)	0.88562
TPR (true positive rate)	0.90879
TNR (true negative rate)	0.89686
DA (detection accuracy)	0.88867
FAR (false alarming rate)	0.11788

جدول ۲

حملات از جمله مثال‌هایی هستند که در این دسته قرار می‌گیرند.

حمله محلی از راه دور (R۲L): برای به‌دست آوردن دسترسی به سیستم محلی، مهاجم از طریق ارسال بسته‌های جعلی به شبکه یا سیستم فردی سوءاستفاده می‌کند، جایی که او اجازه دسترسی به آن سیستم محلی را ندارد. این دسته از حملات شامل«ftp write» ، «spy»، «warez master»، «imap»و «phf» است. برای بررسی دامنه و عملکرد مدل پیشنهادی، آزمایش‌ها با استفاده از مجموعه داده NSL-KDD انجام شد و نتایج با روش‌های معاصر مانندBIFAD، ECDDو FAIS مقایسه شد. عملکرد مدل پیشنهادی با مدل‌هایBIFAD،ECDDو FAIS مقایسه شده است.

BIFAD اولین مدل مبتنی بر جریان است که در آن نویسندگان از الگوریتم جستجوی CUCKOO الهام‌گرفته از طبیعت برای شناسایی جریان ورودی به عنوان نرمال یا حمله استفاده کردند، اما این مدل دقت بهتری برای ترافیک همگن دارد.

ECDD یک گسترش برای BIFAD است که در آن از طبقه‌بندهای انبوه برای رسیدگی به رفتار تنوع در ویژگی‌های جریان ترافیک استفاده می‌شود، اما زمانی که تعداد انحرافات در ترافیک ورودی افزایش می‌یابد، این روش‌ها نیاز به پیچیدگی پردازش بالایی دارند.

مدل FAIS یک رویکرد مبتنی بر آمار است که در آن نفوذها با مقیاس تأثیر ویژگی‌ها اعتبارسنجی می‌شوند، اما این روش برای شبکه‌های ثابت عملکرد بهتری دارد و در حفظ ثبات در جریان‌های ترافیکی افزایش‌یافته ناکام می‌ماند.

روش پیشنهادی از مجموعه‌ای منحصر به فرد از ویژگی‌های جریان ترافیک با طبقه‌بند انتخابی و مقیاس تأثیر ویژگی‌ها استفاده می‌کند تا این محدودیت‌ها را برطرف کرده و دقت شناسایی مؤثری با نرخ‌های کاذب پایین برای ترافیک متغیر ارائه دهد. این مقایسه با روش‌های معاصر که مشخص شده‌اند، انجام شده است.

۴.۲ نتایج تجربی

تجربیات با استفاده از مجموعه داده NSL-KDD انجام شده است تا مدل پیشنهادی با معیارهای عملکرد تعریف شده مانند مثبت واقعی(TP) ، منفی واقعی(TN) ، مثبت کاذب(FP) ، منفی کاذب (FN) و دقت تشخیص ارزیابی شود.

- مثبت واقعی :(TP) تعداد درخواست‌ها یا تراکنش‌هایی که به درستی به عنوان جلسات مستعد حمله پیش‌بینی شده‌اند.
- مثبت کاذب :(FP) تعداد درخواست‌ها یا تراکنش‌هایی که به اشتباه به عنوان جلسات مستعد حمله پیش‌بینی شده‌اند.
- منفی واقعی :(TN) تعداد درخواست‌ها یا تراکنش‌هایی که به درستی به عنوان جلسات عادی پیش‌بینی شده‌اند.
- منفی کاذب :(FN) تعداد درخواست‌ها یا تراکنش‌هایی که به اشتباه به عنوان جلسات عادی پیش‌بینی شده‌اند.

فرمول دقت تشخیص به صورت زیر است:دقت تشخیصTN+TP+FNTP+FP+TN=

مقدار دقت به نسبت کل جلسات جریانی که واقعاً مستعد حمله هستند و جلسات جریانی که واقعاً عادی هستند نسبت به کل جلسات جریانی که به عنوان مستعد حمله و عادی توسط مدل شناسایی شده‌اند، اشاره دارد. نرخ هشدار کاذب به نسبت جلسات جریانی عادی اشاره دارد که مدل مربوطه به عنوان مستعد حمله شناسایی کرده است. مدل پیشنهادی به نام FAIEIS نامگذاری شده ،جایی که ۷۰٪ داده‌ها برای آموزش و ۳۰٪ برای آزمایش در نظر گرفته شده است. تعداد طبقه‌بندها، سرمنبع خوشه و آستانه برای هر طبقه‌بند به همراه انحراف معیار ریشه مربع (RMSD)و مقادیر عملکرد برای FAIEIS لیست شده است.

این بخش به بررسی مقادیر معیار عملکرد برای مدل FAIEIS می‌پردازد، به طوری که دقت تشخیص مدل پیشنهادی ۹۶٪ با نرخ هشدار کاذب ۶٪ است. دقت تشخیص FAIEIS بیشتر از دقت محاسبه شده با روش‌هایBIFAD ، ECDDو FAIS است. روش پیشنهادی FAIEIS مقیاس‌پذیری و ثبات در عملکرد را برای ترافیک همگن یا متنوع دریافتی از محیط توزیع شده حفظ می‌کند، زیرا FAIEIS به ویژگی‌های سطح بسته وابسته نیست و از مجموعه‌ای منحصر به فرد از ویژگی‌های جریان استفاده می‌کند که مستقل از ویژگی‌های سطح بسته هستند.تحلیل روش FAIEIS در بخش بعدی بررسی می‌شود.

F-Measureیک تکنیک برای ارتباط دادن دقت و یادآوری مدل است و به عنوان میانگین هارمونیک دقت و یادآوری FAIEIS نمایش داده می‌شود. دقت تشخیص برای انواع مختلف حملات مانند پروب، U۲R، R۲Lو DoS است.هشدار کاذب نرخ خطای مدل FAIEIS را تعریف می‌کند. هشدارهای کاذب شامل مثبت کاذب و منفی کاذب به ترتیب هستند.

۴.۳دقت تشخیص و تحلیل

برای ارزیابی عملکرد مدل پیشنهادیFAIEIS ، این مدل با معیارهای عملکرد سه روش معاصر مانندBIFAD ، ECDDو FAIS تحلیل می‌شود.

مدل BIFAD اولین مدل مبتنی بر جریان است که ویژگی‌های مشخصی برای مدیریت ترافیک ورودی در سطح جریان به جای سطح بسته دارد و از الگوریتم جستجوی CUCKOO سلسله‌مراتبی برای آموزش و آزمایش داده‌ها در سطح جریان استفاده می‌کند.این روش عملکرد فوق‌العاده‌ای برای ترافیک همگن نشان می‌دهد اما در حفظ عملکرد برای ترافیک متنوع و مدیریت حجم بالای ترافیک ناکام است. دقت تشخیص در سطح ترافیک تصادفی ۸۸٪ با نرخ هشدار کاذب ۰،۱۲٪ است. مدل FAIS برای تشخیص حملات با مقیاس تأثیر ویژگی‌ها پیشنهاد شده است.

این روش یک مدل مبتنی بر آمار است که در آن مقادیر مقیاس برای دسته‌های مختلف حمله با رویکردی هنجاری محاسبه می‌شود. ترافیک با استفاده از این مقیاس برای تعریف آن به عنوان کلاس عادی یا حمله اعتبارسنجی می‌شود.این رویکرد دقت بالایی در تشخیص حملات برای شبکه‌های ثابت ارائه می‌دهد، اما در حفظ ثبات در دقت تشخیص برای جریان‌های متنوع شبکه و حملات جدید ناکام است. این روش دقت ۸۷٪ با نرخ هشدار کاذب ۱۲٪ را نشان می‌دهد.. عملکرد ضعیف FAIS به دلیل فرآیند آموزشی است که با تنوع قابل توجهی از برنامه‌ها در تعداد زیادی از نمونه‌ها تصور شده است.

در نهایت، یک روش مبتنی بر مجموعه ECDD که از ویژگی‌های جریان استفاده می‌کند و به تنوع ویژگی‌ها و خصوصیات ترافیک پرداخته و یک طبقه‌بند مجموعه‌ای با تشخیص انحراف برای اعتبارسنجی ترافیک در سطح جریان به عنوان عادی یا حمله تعریف کرده است. این مدل مقیاس‌پذیری و دقت تشخیص نسبتاً خوبی برای ترافیک همگن و متنوع نشان می‌دهد، اما زمانی که حجم ورودی افزایش می‌یابد، تعداد طبقه‌بندها نیز افزایش می‌یابد و زمان پردازش بیشتری مصرف می‌کند. دقت تشخیص این مدل ۹۱٪ ECDD با نرخ هشدار کاذب ۸٪ است که بهتر از مدل‌های BIFAD و FAIS است..

مدل پیشنهادی FAIEIS ثبات در عملکرد برای جریان‌های متنوع ترافیکی را نشان می‌دهد و مقیاس‌پذیری بهتری نسبت به مدل‌های معاصر ارائه می‌دهد. دقت تشخیص مدل FAIEIS را برای کلاس‌های مختلف حمله و ترافیک عادی با تعداد متغیر خوشه‌ها نشان می‌دهد. نرخ‌های هشدار کاذب مانند مثبت‌های واقعی، منفی‌های واقعی، مثبت‌های کاذب و منفی‌های کاذب نسبت به مدل‌هایBIFAD ، ECDDو FAIS بهبود یافته است. روش پیشنهادی FAIEIS عملکرد بهتری نسبت به روش‌های رقیب ارائه می‌دهد و دقت ثابتی معادل ۹۴٪ برای ترافیک عادی و بیش از ۹۵٪ برای ٤ کلاس حمله حفظ می‌کند. دقت تشخیص برای جریان‌های عادی و ٤ کلاس ترافیک در شکل ٦ نشان داده شده است. نرخ هشدار کاذب FAIEIS نسبت به روش‌های رقیب برای ترافیک عادی و کلاس‌های مختلف حملات بسیار کمتر است. FAIEIS نسبت به روش‌های BIFAD، FAISو ECDD مثبت‌های کاذب و منفی‌های کاذب کمتری را نشان می‌دهد. مدل BIFAD از جستجوی CUCKOO سلسله‌مراتبی با ویژگی‌های جریان برای تشخیص ترافیک ورودی به عنوان عادی یا حمله در سطح جریان برای داده‌های همگن استفاده می‌کند. زمانی که حجم ترافیک ورودی افزایش می‌یابد، زمان پردازش نیز افزایش می‌یابد و دقت تشخیص کاهش می‌یابد. افزایش حجم ترافیک به طور مؤثری با دقت تشخیص برای ویژگی‌های همگن و توزیع‌شده ترافیک در ECDD اعتبارسنجی می‌شود. اما زمانی که تنوع ترافیک افزایش می‌یابد، نیاز به افزایش تعداد طبقه‌بندها و فرآیند آموزش و آزمایش زمان بیشتری برای پردازش نیاز دارد. مدل پیشنهادی FAIEIS به هر دو جریان متغیر ترافیک و ویژگی‌های متنوع پرداخته و دقت تشخیص ثابتی را حفظ کرده و زمان پردازش کمتری نسبت بهBIFAD ، ECDDو FAIS مصرف می‌کند.

انواع مختلف حملات و ترافیک عادی با تعداد متغیر خوشه

نرخ‌های هشدار کاذب مانند True Positive، True Negative، False Positive و False Negative در مقایسه با مدل‌های BIFAD، ECDD و FAIS بهبود یافته است. روش پیشنهادی FAIEIS عملکرد بهتری نسبت به روش‌های رقیب داشته و دقت تشخیص بالاتری را ارائه می‌دهد. این روش دقت ثابتی حدود ۹٤٪ برای ترافیک عادی و بیش از ۹۵٪ برای ٤ کلاس حمله حفظ می‌کند..نرخ هشدار کاذب FAIEIS در مقایسه با روش‌های رقیب برای ترافیک عادی و انواع مختلف حملات بسیار کمتر است. FAIEIS خطاهای مثبت کاذب و منفی کاذب کمتری نسبت به رویکردهای BIFAD، FAIS و ECDD نشان می‌دهد. مدل BIFAD از جستجوی سلسله‌مراتبی CUCKOO با ویژگی‌های جریان غیر دوستانه برای تشخیص ترافیک ورودی به عنوان عادی یا حمله در سطح جریان برای داده‌های همگن استفاده می‌کند. هنگامی که حجم ترافیک ورودی افزایش می‌یابد، زمان پردازش نیز افزایش می‌یابد و دقت تشخیص کاهش می‌یابد. افزایش حجم ترافیک با دقت تشخیص برای ویژگی‌های همگن و توزیع شده

ترافیک در ECDD به طور موثر تأیید می‌شود. اما هنگامی که تنوع ترافیک افزایش می‌یابد، نیاز به افزایش تعداد طبقه‌بندها و فرآیند آموزش و آزمایش به زمان پردازش بیشتری نیاز دارد. مدل پیشنهادی FAIEIS هم جریان متغیر ترافیک و هم ویژگی‌های متنوع متغیر را با دقت تشخیص ثابت و زمان پردازش کمتر نسبت به BIFAD، ECDD و FIAS برطرف می‌کند.

نتیجه‌گیری

با رشد سریع و توسعه فناوری‌های مدرن، استفاده از اینترنت افزایش یافته است که زندگی انسان را پیچیده‌تر کرده است. در عین حال، این امر باعث ایجاد آسیب‌پذیری‌های متعددی در شبکه شده که حملات مختلفی را به دنبال دارد. محققان رویکردهای مختلفی را برای مقابله با این حملات تعریف کرده‌اند که اکثر آن‌ها در سطح بسته اعمال می‌شوند. ویژگی‌های سطح بسته به داده‌های تراکنش یا درخواست وابسته هستند. هنگامی که تنوع ویژگی‌ها در ترافیک ورودی وجود دارد، این روش‌ها هشدارهای کاذب بالایی با نرخ تشخیص پایین ایجاد می‌کنند.

این مقاله رویکرد مبتنی بر جریان را معرفی می‌کند که کاملاً مستقل از ویژگی‌های ترافیک است و ترافیک را از شبکه‌های همگن و توزیع‌شده با ویژگی‌های متنوع مدیریت می‌کند. یک مجموعه منحصر به فرد از ویژگی‌های جدید برای آدرس‌دهی جریان تعریف شده است و هر ویژگی از جریان متنوع به عنوان یک طبقه‌بند مستقل تعریف می‌شود و هر رفتار حمله با یک آستانه مقیاس متا ابتکاری نشان داده می‌شود. تنوع ترافیک با استفاده از آزمون KS با توزیع شباهت خوشه‌ها ارزیابی می‌شود. آزمایش برای اعتبارسنجی رویکرد پیشنهادی بر روی حجم زیادی از ترافیک با تنوع قابل توجه توزیع از مجموعه داده NSL-KDD انجام شده است. با این وجود، مدل‌های معاصر BIFAD و ECDD تشخیص حمله در سطح جریان را برطرف می‌کنند، اما آن‌ها در حفظ انسجام در تشخیص حمله و نرخ‌های هشدار کاذب ناکام هستند. علاوه بر این، این مدل‌ها زمانی که حجم ترافیک ورودی افزایش می‌یابد، زمان محاسباتی بالایی را نشان می‌دهند. مدل پیشنهادی FAIEIS نتایج بهتری نسبت به این مدل‌های BIFAD، ECDD و FAIS در سطح جریان برای ترافیک متنوع حجم‌های بزرگ با نرخ‌های هشدار کاذب کمتر تولید می‌کند. با این حال، مدل پیشنهادی با تکنیک‌های یادگیری عمیق برای آموزش کارآمد مدل با سربار پردازش کمتر برای دستیابی به دقت تشخیص بهتر با هشدارهای کاذب کم در هر شبکه‌ای ساده‌تر شده است.

منابع

Kasim, O.: An efficient and robust deep learning based network anomaly detection against distributed denial of service attacks. Comput. Netw. ۱۸۰, ۱۰۷۳۹۰ (۲۰۲۰)

C¸akmakc¸ı, S.D., Kemmerich, T., Ahmed, T., Baykal, N.: Online DDoS attack detection using Mahalanobis distance and Kernel based learning algorithm. J. Netw. Comput. Appl. ۱٦۸, ۱۰۲۷٥٦ (۲۰۲۰)

Kshirsagar, D., Kumar, S.: An efficient feature reduction method for the detection of DoS attack. ICT Express (۲۰۲۱)

Mazini, M., Shirazi, B., Mahdavi, I.: Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. J. King Saud Univ. Comput. Inf. Sci. ۳۱(٤), ٥٤١–٥٥۳ (۲۰۱۹)

Guo, C., Ping, Y., Liu, N., Luo, S.S.: A two level hybrid approach for intrusion detection. Neurocomputing ۲۱٤, ۳۹۱–٤۰۰ (۲۰۱٦)

Hezavehi, S.M., Rahmani, R.: An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments. Cluster Comput. ۲۳, ۲٦۰۹–۲٦۲۷ (۲۰۲۰)

Ahmed, M., Mahmood, A.N., Hu, J.: A survey of network anomaly detection techniques. J. Netw. Comput. Appl. ٦٠, ١٩–٣١ (٢٠١٦)

Siddiqui, A.J., Boukerche, A.: TempoCode-IoT: temporal code book-based encoding of flow features for intrusion detection in Internet of Things. Cluster Comput. ٢٤, ١٧–٣٥ (٢٠٢١)

Umamaheswari, N., Renuga Devi, R.: TPF-IEHO: tuning phan tom features on traffic flow network behavioral conditions to detected DDos based on improved elephant herding optimizationneural classification. Mater. Today (٢٠٢١)

David, J., Thomas, C.: Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic. Comput. Secur. ٨٢, ٢٨٤–٢٩٥ (٢٠١٩)

Muraleedharan, N., Janet B.: A deep learning based HTTP slow DoS classification approach using flow data. ICT Express (٢٠٢٠)

Bhuvaneswari Amma, N.G., Selvakumar, S.: A statistical class center based triangle area vector method for detection of denial of service attacks. Cluster Comput. ٢٤, ٣٩٣–٤١٥ (٢٠٢١).

Jain, M., Kaur, G.: Distributed anomaly detection using concept drift detection based hybrid ensemble techniques in streamed network data. Cluster Comput. (٢٠٢١)