JCWR2020

کنفرانس بین المللی وب پژوهی
ایران، تهران، ۲۲ و ۲۳ شهریور ۱۳۹۹

An Intrusion Detection System in Computer Networks using the Firefly Algorithm and the Fast Learning Network

Samira Rajabi, Shahram Jamali, Javad Javidan

Department of Computer Engineering University of Mohaghegh Ardabili, Ardabil, Iran

Samira_61R@yahoo.com, jamali@uma.ac.ir, javidan@uma.ac.ir

Abstract

Due to extensive use of communication networks and the ease of communicating via wireless networks, these types of networks are increasingly considered. Usability in any environment without the need for monitoring and environmental engineering of these networks, have been caused increasing use of it in various fields. It also caused the emergence security problems in the sending and receiving of information that the intrusion detection has been raised as the most important issue. Hence, Network intrusion detection system (NIDS) is the process of identifying malicious activity in a network by analyzing the network traffic behavior. Wireless sensor network is a special type of wireless network is composed of sensors that are responsible for the task of collecting information from the environment. This wireless networks because of the limitation of resources, mobility and critical tasks are relatively high vulnerabilities in comparison to other network. There are several ways to secure a wireless network but those ways are not able to detect the majority of attacks. In addition, due to the limited power wireless sensor nodes, the use of observer nodes to permanent monitoring in wireless sensor networks in order to prevention and detection intrusion and attacks has practically impossible. Therefore, forecasting and intrusion detection systems play an important role in providing security in wireless sensor networks that can involve a wide range of attacks. Traffic behavior in the network has many features and dimensions, so dimensionality reduction plays a vital role in IDS, since detecting anomalies from high dimensional network traffic feature is time-consuming process. Feature selection influences the speed of the analysis and detection. For this purpose, in this project, a new approach is proposed to predict the intrusion of wireless networks using firefly based feature selection and fast learning network. Selected features in the feature selection phase are used as inputs to the fast learning network to analyze the intrusion of the network in real-time. According to the simulation results in this thesis it can be said that the fast neural network method continues training so as to avoid overfitting error. While neural networks further learns training set features until the training process is completed. Thus, the occurrence of overfitting phenomenon in neural networks is common. Therefore, the proposed method overall shows better performance than the neural network method in predicting new attacks on the network.

Keywords: Network Intrusion Detection System, Feature Subset Selection, Firefly Optimization Algorithm, Fast Learning neural network.

JCWR2020
کنفرانس بین المللی وب پژوهی
ایران، تهران، ۲۲ و ۲۳ شهریور ۱۳۹۹

یک سیستم تشخیص نفوذ شبکه های کامپیوتری با استفاده از الگوریتم کرم شب‌تاب و شبکه یادگیری سریع

سمیرا رجبی[۱]، شهرام جمالی[۲]، جواد جاویدان[۳]

[۱] دانشجوی کارشناسی ارشد، گروه آموزشی مهندسی برق و کامپیوتر، دانشگاه محقق اردبیلی، اردبیل،
samira_61R@yahoo.com

[۲] دانشیار ، گروه آموزشی مهندسی برق و کامپیوتر، دانشگاه محقق اردبیلی، اردبیل
jamali@uma.ac.ir

[۳] دانشیار ، گروه آموزشی مهندسی برق و کامپیوتر، دانشگاه محقق اردبیلی، اردبیل
javidan@uma.ac.ir

چکیده

با توجه به گستردگی استفاده از شبکه‌های ارتباطی و سهولت برقراری ارتباط از طریق شبکه‌های کامپیوتری، این نوع از شبکه‌ها بیش‌ازپیش مورد توجه قرارگرفته‌اندکه باعث مطرح شدن مسئله‌های امنیتی در زمینه ارسال و دریافت اطلاعات شده که تشخیص نفوذ به‌عنوان مهم‌ترین مسئله مطرح شده است. تشخیص نفوذ شبکه فرایند شناسایی فعالیت‌های مخرب در یک شبکه با تحلیل رفتار ترافیک شبکه است. این شبکه‌ها به دلیل بی‌سیم بودن، محدودیت منابع، تحرک و پویایی و وظایف مهم و بحرانی که دارند، نسبت به شبکه‌های دیگر دارای آسیب‌پذیری نسبتاً بالایی هستند. علاوه بر این با توجه به انرژی محدود گره‌های بی‌سیم، استفاده از گره‌های ناظر برای نظارت دائمی در شبکه‌های بی‌سیم به‌منظور جلوگیری و کشف نفوذ و حملات را در این نوع از شبکه‌ها عملاً غیرممکن کرده است. ازاین‌رو سیستم‌های پیش‌بینی و تشخیص نفوذ در شبکه (NIDS) نقش مهمی در ایجاد امنیت در شبکه‌های بی‌سیم بر عهده دارند و می‌توانند محدوده وسیعی از حملات را در برگیرند. رفتار ترافیکی در شبکه دارای ویژگی‌ها و ابعاد زیادی است، بنابراین کاهش ابعاد نقش حیاتی در NIDS بازی می‌کند، زیرا شناسایی ناهنجاری‌ها از ویژگی ترافیک شبکه با ابعاد بزرگ، فرایند زمان‌گیر است. انتخاب ویژگی بر سرعت تجزیه‌وتحلیل و تشخیص تأثیر می‌گذارد. به همین منظور در این پژوهش برای پیش‌بینی نفوذ در شبکه‌های بی‌سیم رویکرد جدیدی با استفاده از انتخاب زیرمجموعه ویژگی مبتنی بر الگوریتم کرم شب‌تاب و شبکه یادگیری عصبی سریع ارائه می‌شود. ویژگی‌های منتخب در مرحله انتخاب زیرمجموعه ویژگی‌ها، به‌عنوان ورودی به شبکه یادگیری عصبی سریع مورد استفاده قرار می‌گیرد تا در زمان بلادرنگ تحلیلی از نفوذها در شبکه صورت گیرد. با توجه به نتایج شبیه‌سازی در این پایان‌نامه می‌توان گفت روش شبکه‌های عصبی سریع آموزش را تا جایی ادامه می‌دهد که از بروز خطای overfitting جلوگیری به عمل آید درصورتی‌که شبکه‌های عصبی تا کامل شدن روند آموزش، ویژگی‌های نمونه‌های آموزشی را بیشتر یاد می‌گیرد. بنابراین بروز پدیده Overfitting در شبکه‌های عصبی طبیعی است. ازاین‌رو روش پیشنهادی درمجموع عملکرد بهتری نسبت به روش شبکه‌های عصبی در تشخیص گره‌های سالم و حملات جدید در شبکه را نشان می‌دهد.

کلمات کلیدی

سیستم تشخیص نفوذ در شبکه، انتخاب زیرمجموعه ویژگی، الگوریتم بهینه‌سازی کرم شب‌تاب، یادگیری سریع

۱- مقدمه

شبکه‌های کامپیوتری به‌وسیله مجموعه‌ای از میزبان‌های سیار تشکیل یافته‌اند و از طریق لینک‌های بی‌سیم به یکدیگر متصل شده‌اند. هر گره می‌تواند به‌عنوان یک سیستم نهایی عمل کند علاوه بر آن می‌تواند در نقش یک روتر بسته‌ها را ارسال کند[۱]. هنگامی که یک گره مبدأ قصد انتقال اطلاعات به یک گره مقصد را دارد بسته‌ها بین گره‌های میانی انتقال می‌یابند و بنابراین

جستجو و ایجاد سریع یک مسیر از مبدأ به گره مقصد برای شبکه‌های کامپیوتری سیار امری حیاتی است[۲]. توپولوژی شبکه‌های کامپیوتری سیار ممکن است به‌طور متناوب و درنتیجه جابجایی گره‌ها تغییر یابد، بنابراین با این تکنولوژی گره‌ها می‌توانند به‌راحتی خود را با همسایگان محلی تغییر دهند [۳–۵]. هنگامی که بحث شبکه‌های بی‌سیم مطرح می‌شود بحث امنیت و جلوگیری از حملات بسیار مشکل‌تر می‌شود و این مشکل در شبکه‌های کامپیوتری سیار نیز چندین برابر است[۶, ۷].

نفوذ گره‌های مخرب در میان گره‌های این شبکه می‌تواند موجب تضعیف و یا تخریب بسته‌های اطلاعاتی انتقال یافته شود و تمام یا قسمتی از اطلاعات موردنیاز از بین برود. درنتیجه کارایی کل سیستم تهدید شده و ممکن است نتایج به گونه دیگری مورد تفسیر قرار گیرند[۸–۱۰]. بنابراین جلوگیری و کشف نفوذها و حملات در شبکه‌های کامپیوتری به یک امر حیاتی و چالشی جدی تبدیل شده است. ازاین‌رو سیستم‌های تشخیص نفوذ نقش مهمی در ایجاد امنیت در شبکه‌های بی‌سیم بر عهده دارند و می‌توانند محدوده وسیعی از حملات را در برگیرند[۱۱].

سیستم‌های تشخیص نفوذ به‌منظور تعیین این که فعالیت کاربر تحت نظارت یا فعالیت ترافیک شبکه، مخرب است یا خیر، تلاش می‌کنند[۱۲, ۱۳]. اگر در طی دوره نظارت یک حمله مخرب شناسایی شود، هشدار ایجاد می‌شود. تکنیک‌های مختلفی برای IDSها برای تشخیص حمله مانند تشخیص آنومالی یا امضاء حمله وجود دارد که نکته قابل‌ذکر این است که موفقیت IDS بستگی به تکنیک‌های مورد استفاده دارد[۱۴]. یکی از عوامل اصلی که اثربخشی IDS را بر عهده دارد، کیفیت ساخت ویژگی و الگوریتم انتخاب ویژگی است. به‌منظور بهبود کارایی کلیIDS، کاهش تعداد ویژگی‌های قابل‌استفاده ترافیکی شبکه، بدون تأثیر بر روی دقت طبقه‌بندی، موردنیاز است[۱۵].

ازاین‌رو در این تحقیق روشی برای سیستم تشخیص نفوذ در شبکه بر اساس ترکیب انتخاب زیرمجموعه ویژگی مبتنی بر الگوریتم کرم شب‌تاب و شبکه یادگیری عصبی سریع[۱] ارائه شده است. روش پیشنهادی از مجموعه‌داده‌های آموزشی به دست آمده از مجموعه‌داده‌ها KDD Cup [۱۶] برای تعیین الگوهای شناسایی نفوذ در شبکه و از مجموعه‌داده‌های تست تهیه شده از هم این مجموعه‌داده‌ها، به‌منظور ارزیابی مدل استفاده خواهد نمود. در روش پیشنهادی با توجه به تنوع و تعداد ویژگی‌های رفتار کاربران و ترافیک شبکه، انتخاب زیرمجموعه ویژگی‌ها در راستای افزایش دقت طبقه‌بندی مدل ضروری به نظر می‌رسد. هدف انتخاب زیرمجموعه ویژگی‌ها، حذف ویژگی‌ها و صفت‌های نامرتبط و افزونه است تا به این طریق علاوه بر کاهش بعد داده‌ها و کاهش پیچیدگی اجرایی و فضایی سیستم، بتوان دقت طبقه‌بندی را افزایش داده و با سرعت بالا و هزینه کمتری داده‌ها را طبقه‌بندی نمایم. علاوه بر این انتخاب زیرمجموعه‌ای از ویژگی‌ها می‌تواند وابستگی ضمنی میان داده‌ها و برچسب کلاس این داده‌ها را تشخیص دهد تا طبقه‌بندی نمونه‌های تست که در آینده به مدل اضافه خواهند شد به‌راحتی صورت گیرد.

بدین منظور در روش پیشنهادی از رویکرد انتخاب زیرمجموعه ویژگی مبتنی بر الگوریتم کرم شب‌تاب به‌منظور تعیین ویژگی‌های با اهمیت و مرتبط با برچسب کلاس استفاده شده است[۱۷]. ویژگی‌های باقیمانده از این مرحله که به‌عنوان خروجی الگوریتم شب‌تاب نتیجه شده است، به‌عنوان ورودی شبکه یادگیری سریع مورد استفاده در روش پیشنهادی، به‌منظور افزایش دقت طبقه‌بندی نمونه‌های آموزشی و تعیین برچسب نمونه‌های تست در نظر گرفته می‌شود.

در ادامه مقاله، در بخش ۲ برخی از سیستم‌های تشخیص نفوذ در شبکه های کامپیوتری بررسی خواهند شد. در بخش ۳ جزئیات روش پیشنهادی ارائه خواهد شد.در بخش۴ به مدل‌سازی و ارزیابی عملکرد روش پیشنهادی خواهیم پرداخت.د نهایت در بخش ۵ نتیجه‌گیری مقاله و کارهای آینده بیان خواهد شد.

۲- کارهای مرتبط

نیاز به خدمات همیشه با سرعت بالا برای خدمات شبکه‌ای برای کسب‌وکار و سایر سرویس‌های شبکه، از ملزومات شبکه بوده و نیازی به تأکید بیش‌ازحد ندارد. سیستم‌های تشخیص نفوذ (IDS) یک ابزار مهم برای حفاظت از شبکه هستند[۱۸]. سیستم‌های تشخیص نفوذ (IDS) تجزیه‌وتحلیل مسیرهای ورود گره‌ها به سیستم را در ارتباط با سیستم‌های حفاظت‌شده، بررسی می‌کنند و تصمیم می‌گیرند که آیا این مسیرهای ورود به سیستم حاوی گره‌هایی از یک حمله است یا نه. اگر سیستم تشخیص نفوذ یک حمله را تشخیص دهد، هشدار را افزایش می‌دهد. به‌طور سنتی، سیستم‌های تشخیص نفوذ از بازرسی عمیق بسته‌ها یا تجزیه‌وتحلیل پروتکل‌های وضعیتی برای شناسایی حملات در ترافیک شبکه استفاده می‌کنند. بازرسی عمیق بسته زمانی که ترافیک شبکه رمزگذاری می‌شود امکان‌پذیر نیست. همچنین بازرسی کامل اجزای کامپیوتری پرهزینه است و می‌تواند در شبکه‌های با سرعت بالا به یک مشکل بزرگ تبدیل شود. تجزیه‌وتحلیل کامل پروتکل‌ها برای تعیین ویژگی‌ها و محدوده هر یک از نفوذها در نظر گرفته می‌شود. تکنیک‌های تجزیه‌وتحلیل پروتکل نیز می‌توانند به‌صورت محاسباتی پرهزینه باشند[۱۱].

در [۷] یک مدل یادگیری توسعه‌یافته برای شبکه یادگیری عصبی سریع (FLN) مبتنی بر بهینه‌سازی ازدحام ذرات[۲] (PSO) پیشنهاد شده است و به نام PSO-FLN نام‌گذاری شده است. این مدل بر روی مسئله تشخیص نفوذ و اعتبار سنجی بر اساس مجموعه‌داده معروف KDD99 اعمال شده است. در [۱۷]روشی را با به‌کارگیری الگوریتم کرم شب‌تاب مبتنی بر روش‌های فیلتر و Wrapper توسعه یافته است که بر سرعت تجزیه‌وتحلیل مدل طبقه‌بندی تأثیر می‌گذارد. ویژگی‌های حاصل از این گام انتخاب ویژگی، به طبقه‌بندی C4.5 و شبکه‌های بیزین[۳] (BN) با مجموعه‌داده KDD CUP 99 منتهی می‌شود.در [۱۵]، یک سیستم تشخیص نفوذ جدید مبتنی

بر ترکیبی از یک شبکه عصبی چندلایه و یک کلونی زنبورعسل مصنوعی و الگوریتم‌های خوشه‌بندی فازی ارائه شده است. بسته‌های ترافیکی شبکه عادی و غیرعادی توسط شبکه عصبی شناسایی می‌شوند، درعین‌حال آموزش آن با استفاده از الگوریتم کلونی زنبور عسل توسط بهینه‌سازی مقادیر وزن و پیوند بایاس انجام می‌شود. در [۱۹]یک رویکرد بهینه برای ساخت سیستم تشخیص نفوذ در شبکه بر اساس شبکه عصبی پسرو با استفاده از الگوریتم یادگیری پیشرفته ارائه کرده‌اند و یک معماری جدید برای شبکه استفاده کرده‌اند. این رویکرد برای اولین بار بر تولید تمام ترکیبات ممکن از مقادیر مناسب پارامترهای موجود در ساخت چنین طبقه‌بندی، یا تأثیر عملکرد آن در تشخیص ناهنجاری، نظیر انتخاب ویژگی، نرمال‌سازی داده‌ها، معماری شبکه عصبی و تابع فعال‌سازی، متکی است. در [۲۰] استفاده از روش‌های یادگیری تنبل برای بهبود عملکرد کلی IDS را پیشنهاد شده است. یک روش اندیس گذاری مبتنی بر وزن مکاشفه‌ای برای غلبه بر نقص پیچیدگی جستجوی که ذاتاً در یادگیری تنبل وجود دارد، استفاده شده است. IBk و LWL، دو الگوریتم معروف یادگیری تنبل هستند که بر روی مجموعه‌داده NSL-KDD برای شبیه‌سازی یک سناریو در دنیای واقعی و مقایسه عملکرد نسبی آن با hw-IBk اعمال شده‌اند. در [۲۱] برای شناسایی و یا جلوگیری از حملات شبکه، یک سیستم تشخیص نفوذ شبکه با الگوریتم یادگیری ماشین برای رسیدن به دقت بهتر و سرعت تشخیص سریع‌تر ارائه نموده‌اند. استفاده از یادگیری ماشین یکی دیگر از مزیت‌های عمده‌ای است که در آن دانش پیشرفته به اندازه مدل لیست سیاه‌وسفید موردنیاز نیست. ماشین‌های یادگیری شدید[۴] (ELMs) شبکه‌های عصبی مصنوعی تک لایه هستند که نیازی به تکرار آموزش ندارند. بنابراین، سرعت یادگیری آن‌ها سریع است و سرعت در موفقیت سیستم‌های تشخیص نفوذ شبکه بسیار مهم است و برای آن‌ها واکنش سریع و مؤثر دفاع می‌کنند. در [۲۲] یک روش یادگیری نیمه نظارتی مبتنی بر فازی را با استفاده از نمونه‌های بدون برچسب با کمک الگوریتم یادگیری نظارت‌شده برای بهبود عملکرد طبقه‌بندی برای سیستم تشخیص نفوذ ارائه شده است. یک شبکه عصبی پیش رو یکپارچه برای به دست آوردن بردار عضویت فازی آموزش داده شده است و طبقه‌بندی نمونه (دسته‌های کم، متوسط و زیاد فازی) در نمونه‌های بدون برچسب با استفاده از مقدار فازی انجام می‌شود. طبقه بند پس از ترکیب هر دسته به‌طور جداگانه در مجموعه آموزش اصلی، آموزش مجدد روی داده‌ها انجام می‌دهد. [۲۲].

۳- روش پیشنهادی

شبکه‌های بی‌سیم با توپولوژی متغیر و بدون وجود زیرساخت مشخص، دائماً در معرض حملات توسط گره‌های مخرب قرار دارند. دسترسی آسان به شبکه‌ها و امکان اتصال سریع به سایر گره‌ها باعث شده این نوع از شبکه‌ها مستعد حملات باشند. این شبکه‌ها اغلب بدون برنامه‌ریزی قبلی ایجاد می‌شوند و برای مدت کوتاهی نیاز به برقراری امنیت دارند. ازآنجایی‌که شبکه‌های موردی سیار بدون زیرساخت هستند و از هیچ تجهیزاتی مثل روتر و یا سوئیچ برای مسیریابی استفاده نمی‌کنند، خود گره‌ها در عمل مسیریابی شرکت می‌کنند. هر گره می‌تواند در نقش یک روتر، بسته‌ها را در مسیر بین مبدأ و مقصد ارسال نماید، حضور یک گره مخرب در بین گره‌های موجود در شبکه می‌تواند موجب اختلال در روند ارسال و دریافت بسته‌های اطلاعاتی شود، وجود یک حمله در این نوع شبکه‌ها می‌تواند به نابودی شبکه بیانجامد[۲۳, ۲۴]. ازاین‌رو در این تحقیق روشی برای سیستم تشخیص نفوذ در شبکه بر اساس ترکیب انتخاب زیرمجموعه ویژگی مبتنی بر الگوریتم کرم شب‌تاب و شبکه یادگیری عصبی سریع ارائه شده است. در ادامه این فصل به بررسی اجمالی انتخاب زیرمجموعه ویژگی‌ها، الگوریتم کرم شب‌تاب، شبکه‌های عصبی، شبکه عصبی با یادگیری سریع و توصیف روش پیشنهادی خواهیم پرداخت.

۳-۱- پیش‌پردازش داده‌ها

در سال‌های اخیر انواع مدل‌های طبقه‌بندی توسعه یافته‌اند که با انجام فرآیند آموزشی روی داده‌ها، قادر به طبقه‌بندی و پیش‌بینی داده‌های تست و موارد ناشناخته برای سیستم می‌باشند. نکته قابل‌توجه در این میان، نوع داده مورد استفاده برای هریک از انواع مدل‌هاست. درواقع هر مدل با نوع داده خاصی سروکار دارد و به طبقه‌بندی نوع خاصی از داده‌ها می‌پردازد. برای استفاده از مدل‌ها و بهره‌گیری از نتایج خروجی از مدل نیاز به آماده‌سازی داده‌ها در قالب خاص مدل است. فرآیند آماده‌سازی داده‌ها برای هر مدل پیش‌پردازش داده‌ها نام دارد. پیش‌پردازش داده‌ها دارای گام‌های متعددی است که در این تحقیق دو نمونه از این گام‌های پیش‌پردازشی موردنیاز است که در ادامه توضیح داده می‌شود[۲۵].

۳-۲- انتخاب زیرمجموعه ویژگی‌ها

گام پیش‌پردازشی که در این تحقیق مورد استفاده قرار گرفته است انتخاب زیرمجموعه‌ای از صفت‌هاست که با برچسب کلاس ارتباط مستقیم دارند[۲۵]. با توجه به اینکه مجموعه‌داده‌های مربوط به تشخیص نفوذ KDD دارای ۴۱ ویژگی در سه دسته ویژگی‌های پایه اتصالات تکی tcp، ویژگی‌های محتوایی با اتصالات پیشنهادی توسط دامنه دانش و ویژگی‌های ترافیک محاسبه‌شده با استفاده از پنجره زمانی دوثانیه‌ای توزیع شده‌اند. این تعداد زیاد صفت‌ها می‌تواند موجب پیچیدگی مدل طبقه‌بندی مورد استفاده شود. ازاین‌رو باید تعدادی از این صفت‌ها که توزیع نامتوازن داشته و در تعیین برچسب کلاس نمونه‌ها تأثیر چندانی ندارند، طی گام پیش‌پردازشی انتخاب زیرمجموعه ویژگی‌ها حذف شوند.

هدف گام پیش‌پردازشی انتخاب زیرمجموعه ویژگی‌ها حذف ویژگی‌ها و صفت‌های نامرتبط و افزونه است تا به این طریق علاوه بر کاهش بعد داده‌ها و کاهش پیچیدگی اجرایی و فضایی سیستم، بتوان دقت طبقه‌بندی را افزایش داده و با سرعت بالا و هزینه کمتری داده‌ها را طبقه‌بندی نمایم. علاوه بر این انتخاب زیرمجموعه‌ای از داده‌ها می‌تواند وابستگی ضمنی میان داده‌ها و

برچسب کلاس این داده‌ها را تشخیص داد تا طبقه‌بندی نمونه‌های تست که در آینده به مدل اضافه خواهند شد به‌راحتی صورت گیرد. ازاین‌رو در این تحقیق ویژگی‌های غیر مرتبط و صفت‌های که تغییرات زیادی در نمونه‌ها ندارند و طبیعتاً تأثیر چندانی در برچسب کلاس نمی‌توانند داشته باشند، حذف می‌شوند تا از تحمیل پیچیدگی اضافی بر مدل طبقه‌بندی پیشنهادی جلوگیری شود[۲۶].

۳-۳- نرمال‌سازی داده‌ها

با توجه به مجموعه ویژگی‌های انتخاب‌شده به‌عنوان معیار شباهت در بخش قبلی، می‌توان دید که بازه توزیع داده‌ها در این مجموعه ویژگی‌ها متفاوت از هم است. طبیعی است که اگر بُرد مقادیر صفت‌های داده در معیارهای شباهت متفاوت باشد، در این صورت صفتی که حوزه مقادیر بزرگ‌تری دارد، سایر صفت‌ها را تحت تأثیر قرار داده و بر روی عملکرد مدل طبقه‌بندی مورد استفاده مؤثرتر خواهد بود. این تأثیر می‌تواند دقت طبقه‌بندی را کاهش داده و موجب پیش‌بینی نادرست نمونه‌های تست شود. برای حل این مشکل از نرمال‌سازی داده‌ها در مجموعه‌داده آموزش و تست استفاده می‌شود[۲۷]. نرمال‌سازی داده‌ها موجب نگاشت مقادیر در بازه صفر و یک می‌شود که تأثیر منفی ویژگی‌ها با مقادیر بیشتر روی دقت طبقه‌بندی را از بین می‌برد. از روابط نرمال‌سازی معروف موجود در نشریات می‌توان به نرمال‌سازی گاوسی و نرمال‌سازی min-max اشاره کرد که در این تحقیق از نرمال‌سازی min-max استفاده شده است. در رابطه (۱) نرمال‌سازی min-max به شرح زیر نشان داده شده است[۲۸]:

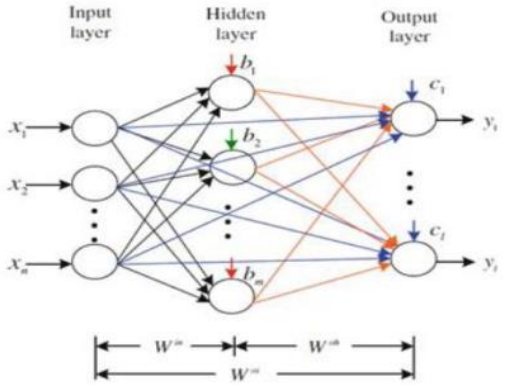
$$min-\max normalization=\frac{(x_{i,j}-x_{min})}{(x_{max}-x_{min})} \qquad (۱)$$

که در آن $x_{i,j}$ مقادیر هر ویژگی به ازای هریک از نمونه‌ها و x_{min} کوچک‌ترین مقدار برای یک ویژگی و x_{max} بزرگ‌ترین مقدار برای یک ویژگی است.

۳-٤- شبکه یادگیری عصبی سریع

شبکه یادگیری عصبی سریع (FLN) یک اتصال موازی از یک شبکه تک لایه پیشرو و یک شبکه عصبی ۳ لایه شامل لایه‌های ورودی، پنهان و خروجی است. FLN، یک شبکه عصبی مصنوعی است که یک شبکه عصبی دوطرفه موازی (DPFNN) می‌باشد، که با استفاده از یک رویکرد تحلیلی به نام روش کمترین مربع در شکل(۱) نشان داده شده است.

FLN اساساً یک شبکه پیش رو موازی است. این یک اتصال موازی FNN چندلایه و FNN تک لایه را توصیف می‌کند. همان‌طور که قبلاً بحث شد، اطلاعات خارجی دوباره کدگذاری شده از گره‌های پنهان، همراه با اطلاعات خارجی خود، به‌طور مستقیم از گره‌های ورودی به گره خروجی از DFNNs ارسال می‌شود.



شکل (۱) : ساختار شبکه یادگیری عصبی سریع[۲۹]

همان‌طور که اشاره شده است، FLN ازنظر عدم وجود وزن، توزیع یا انتساب مطلوب شبیه به یادگیری ماشین خبره (ELM) است. درنتیجه، دقت کلی ANN کاهش خواهد یافت مگر اینکه یک روش مناسب برای انتخاب وزن‌ها، اعمال شود. FLN بهینه‌شده توسط PSO در این روش بر اساس انتخاب وزن با استفاده از بهینه‌سازی ازدحام ذرات آموزش دیده است. بهینه‌سازی مبتنی بر PSO از FLN بر اساس طراحی ذره‌ای است که یک راه‌حل کاندیدا از وزن FLN را نشان می‌دهد. یک مشکل خاص در انجام بهینه‌سازی، نیاز به انتخاب هر دو مقدار وزن و تعداد نورون‌هایی است که در لایه پنهان برای افزایش دقت موردنیاز است. این بدان معنی است که تعداد نورون‌های پنهان راه‌حل در FLN متغیر است و برای غلبه بر این مشکل، حداکثر تعداد نورون‌ها برای طول ذره در نظر گرفته شده است. برای تابع فعال‌سازی، خروجی نورون‌های لایه پنهان استفاده شده است[۲۹].

۳-۵- الگوریتم کرم شب‌تاب

الگوریتم کرم شب‌تاب (FA) به‌عنوان یکی از روش‌های جدید هوش مصنوعی در این تحقیق مورد استفاده قرار گرفته است. این الگوریتم از رفتار اجتماعی کرم‌های شب‌تاب الهام گرفته شده است. این روش نیز مانند بقیه روش‌های بهینه‌سازی هوشمند، با جمعیت اولیه‌ای از حشرات آغاز می‌شود. در این روش حشرات دوبه‌دو با هم مقایسه شده و حشره‌ای که جذابیت کمتری دارد به سمت حشره جذاب‌تر حرکت می‌کند. نهایتاً یک حشره به‌عنوان جذاب‌ترین حشره انتخاب می‌شود که همان پاسخ بهینه‌ی مسئله موردنظر می‌باشد.

بررسی مکان و اندازه بهینه واحدهای تولید پراکنده ، با ملاحظات فنی و اقتصادی به‌صورت هم‌زمان در کنار یکدیگر توسط یک الگوریتم بهینه‌سازی مناسب می‌تواند نقش بسزایی را در افزایش سود اقتصادی واحدهای تولید پراکنده داشته از طرفی باعث افزایش کیفیت توان ارائه شده به مشتری گردد.

الگوریتم کرم شب‌تاب یک الگوریتم بر مبنای هوش مصنوعی می‌باشد که اولین بار در سال ۲۰۰۸ توسط Xin-She Yang مطرح شد این الگوریتم

که شباهت بسیار زیادی به الگوریتم pso دارد از رفتار جمعی کرم‌های شب‌تاب در فرایند جفت‌یابی استفاده می‌کند.

انتشار نور کرم‌های شب‌تاب منظره‌ی شگفت‌انگیزی در آسمان برخی از نواحی معتدل مثل تایلند و برخی قسمت‌های آفریقا ایجاد می‌کند. بیش از دو هزار شب‌پره با یک ریتم خاصی به گسیل نور می‌پردازند. توابع زیادی را می‌توان از این سیستم اطلاع‌رسانی موردبررسی قرار داد اما تابع جذب حشرات دیگر برای جفت‌یابی مدنظر ما در این الگوریتم می‌باشد. آهنگ گسیل نور مدت‌زمان گسیل نور و شدت نوردهی از عوامل متفاوت در جذب حشره نر یا ماده خواهد بود. برای توسعه الگوریتم کرم شب‌تاب معمولاً از سه قانون ایده‌آل ساز استفاده می‌کنند :

۱ – همه شب‌پره‌ها تک‌جنسی هستند: به‌طوری‌که یک شب‌پره قادر به جذب سایر شب‌پره‌ها صرف‌نظر از جنسیت آن خواهد بود.

۲ – جذابیت هر شب‌پره نسبت به میزان نوردهی آن مشخص خواهد شد به نحوی که شب‌پره با نور کمتر به سمت شب‌پره با نور بیشتر حرکت خواهد کرد و اگر جذابیت یکسان باشد حرکت تصادفی خواهد بود.

۳ – نورانیت هر شب‌پره با تابع هدف تعریف شده خواهد بود[۳۰].

۳-۵-۱- جذابیت و حرکت حشرات

دو موضوع مهم در این الگوریتم، عبارت‌اند از:۱- تغییرات شدت روشنایی ۲- فرموله کردن جذابیت.به‌منظور سادگی معمولاً فرض می‌شود که جذابیت حشرات با شدت روشنایی آن‌ها بیان می‌شود. شدت روشنایی نیز متناسب با برازندگی حشره می‌باشد.

در حالت کلی جذابیت پارامتری نسبی بوده و از دید حشرات دیگر سنجیده می‌شود.همچنین به فاصله حشرات از یکدیگر نیز بستگی دارد. در رابطه (۲) جذابیت با تغییرات فاصله حشرات به‌صورت زیر نشان داده شده است:

$$\beta = \beta_0 . e^{-\gamma . r} \qquad (۲)$$

که در آن β_0 بیانگر ماکزیمم جذابیت بوده و مقداری در بازه $[0,1]$دارد. γنیز بیانگر ضریب جذب می‌باشد و مقداری در بازه $[0,\infty)$ دارد. r بیانگر فاصله حشرات بوده و به‌عنوان‌مثال در مقیاس دوبعدی فاصله حشره i ام از حشره j ام به‌صورت رابطه (۳) محاسبه می‌شود:

$$r_{ij} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \qquad (۳)$$

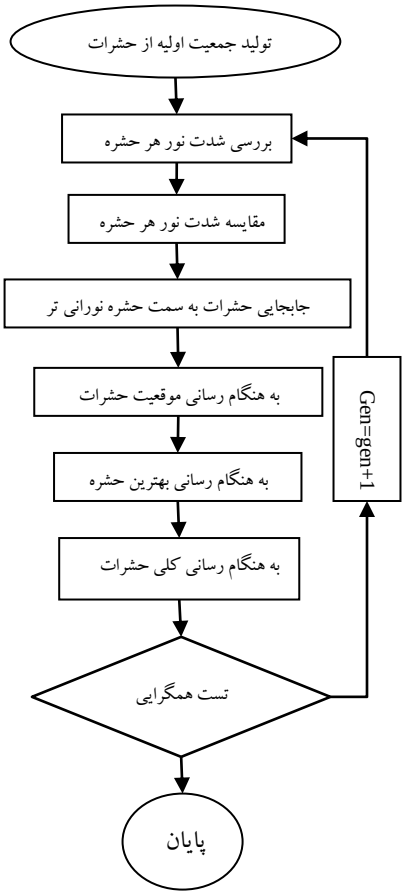
حرکت حشره i ام به سمت حشره j ام نیز از رابطه (۴) به دست می‌آید:

$$X_i = X_i + \beta . e^{-\gamma . r} (X_j - X_i) + \alpha . (rand - ۰.۵) \qquad (۴)$$

در الگوریتم کرم شب‌تاب مقادیر α، β_0 و γ ثابت در نظر گرفته می‌شوند.α و β_0 در بازه $[0,1]$ و γ در بازه $[0,\infty)$ انتخاب می‌شود. فلوچارت این الگوریتم در شکل (۲) نشان داده شده است.

٤- پیاده سازی

به‌منظور پیاده‌سازی روش پیشنهادی از نرم افزار MATLAB نسخه ۲۰۱۵ استفاده شده است. در این تحقیق داده‌های استاندارد kddcup.data موجود در مخزن داده استاندارد UCI به کار گرفته شده است. در روش کاهش بعد کرم شب‌تاب، ابتدا ویژگی‌های پیوسته مربوط به مجموعه‌داده جدا شده است. سپس به ازای مقادیر درون هر یک از ویژگی‌ها، کمترین و بیشترین مقدار ویژگی به‌منظور نرمال‌سازی بر طبق (۱) مقادیر درون ویژگی محاسبه شده است. پس از نرمال‌سازی داده‌های در ویژگی‌های پیوسته، این داده‌های به‌عنوان ورودی به الگوریتم کرم شب‌تاب ارائه می‌شود. وظیفه الگوریتم کرم شب‌تاب در این مقاله یافتن ارتباط بین ویژگی‌ها با برچسب کلاس مربوط به داده‌ها درمجموعه‌داده آموزشی است. درواقع کرم‌های شب‌تاب با توجه به تابع ارزیابی بر طبق (۴)، همبستگی بین ویژگی‌ها و کلاس داده‌ها را از طریق



شکل (۲) : فلوچارت عملکرد الگوریتم کرم شب‌تاب[۳۰]

محاسبه حرکت حشرات بر طبق (۲) فاصله حشرات بر طبق (۳) بررسی می‌کنند. کرم‌های شب‌تاب بر اساس مقادیر ویژگی و همبستگی هر یک از ویژگی‌ها با برچسب کلاس، به سمت ویژگی‌های مؤثر جمع شده‌اند. بنابراین ویژگی‌های مهم برای طبقه‌بندی نفوذ در شبکه را می‌توان بر اساس خروجی الگوریتم بهینه‌سازی کرم شب‌تاب پیشنهادی تعیین کرد.

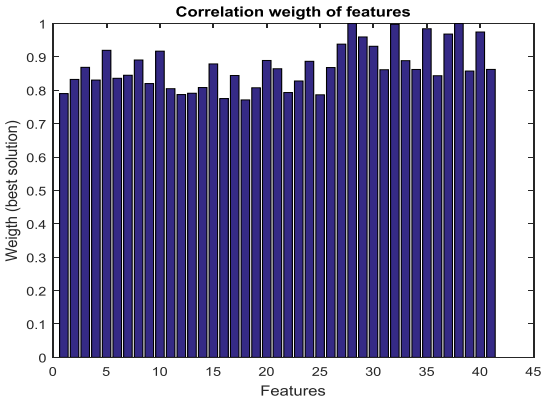
همان‌طور که در جدول (۱) نشان داده شده است، مقادیر وزن همبستگی برای هر یک از ویژگی‌ها محاسبه شده است. بیشترین مقدار مربوط به ویژگی‌هایی است که بیشترین همبستگی را به برچسب کلاس دارند. همچنین شکل (۳) نمودار میله‌ای مربوط به وزن همبستگی ویژگی‌ها به برچسب کلاس را نشان می‌دهد.

همان‌طور که در شکل (۳) نشان داده شده است، با تعیین آستانه‌ای می‌توان ویژگی‌های مربوط مهم را در مجموعه‌داده‌های مربوط به تشخیص نفوذ در شبکه، تعیین کرد. مقدار این آستانه باید طوری انتخاب شود که داده‌های کاهش‌یافته به‌عنوان نمایندگی داده‌های اصلی در نظر گرفته شده و دقت تشخیص نفوذ در شبکه را تحت تأثیر خود قرار ندهد. ازاین‌رو در مقاله مقدار آستانه $\alpha=0.9$ برای انتخاب ویژگی‌ها استفاده شده است. درواقع ویژگی‌هایی که وزن همبستگی بیشتر از ۰.۹ دارند در مجموعه‌داده‌ها باقی‌مانده و مابقی ویژگی‌های از مجموعه‌داده حذف می‌شوند. این مقدار آستانه بر اساس شبیه‌سازی و تعیین بیشترین دقت ویژگی‌های باقیمانده صورت گرفته است. بر این اساس تعداد ۱۱ ویژگی با اهمیت به‌منظور کشف نفوذ در شبکه‌های بی‌سیم باقی‌مانده و مابقی حذف می‌شوند. ویژگی‌های باقیمانده به‌عنوان ورودی شبکه‌های عصبی و شبکه یادگیری عصبی سریع پیشنهادی مورد استفاده قرار می‌گیرد.

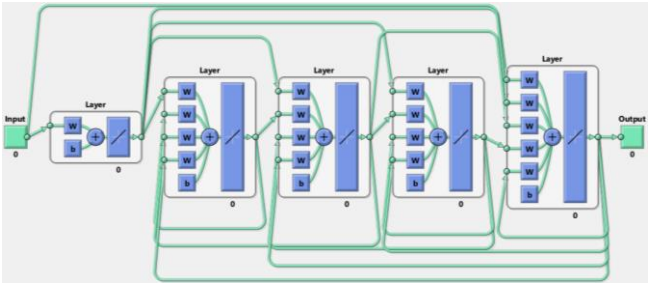
در شبکه‌های عصبی مصنوعی مجموعه‌داده‌ها به سه قسمت آموزشی، اعتبار سنجی و تست تقسیم می‌شود. بخش اعتبار سنجی برای سنجش عملکرد مدل در ازای داده‌های آموزشی است. شبکه‌های عصبی مصنوعی در لایه میانی بر اساس صفات داده‌های آموزشی، مدلی را آموزش می‌دهد. اعتبار این مدل در مرحله اول از طریق قسمتی از داده‌ها که اعتبارسنجی نامیده می‌شود، انجام می‌گیرد. زمانی که دقت عملکرد مدل آموزشی برای داده‌های آموزشی در حد قابل‌قبولی باشد، دقت عملکرد مدل برای داده‌های تست و داده‌های ناشناخته، از طریق دیگر قسمت داده‌ها که تست نامیده می‌شود، مورد سنجش قرار می‌گیرد. شکل(۴) شبکه‌های عصبی توسعه‌یافته در این تحقیق را نشان می‌دهد.

همان‌طور که در شکل (۴) نشان داده شده است، شبکه‌های عصبی مورد استفاده برای این تحقیق شامل سه لایه ورودی، میانی و خروجی است که تعداد گره‌ها در لایه ورودی برابر با تعداد ویژگی‌های مورد استفاده بعد از اعمال گام پیش‌پردازشی و کاهش ابعاد با استفاده از الگوریتم بهینه‌سازی کرم شب‌تاب است.

مقادیر وزن کلاس‌ها در لایه‌های میانی بر اساس تابع آموزشی یادشده بررسی می‌شود و برای هر یک از ویژگی‌ها وزنی به لایه بعدی انتقال می‌یابد.



شکل (۳) : نمودار وزن همبستگی ویژگی‌ها به برچسب کلاس



شکل (٤): شبکه‌های عصبی پیشنهادی

جدول (۱) : خروجی الگوریتم کرم شب‌تاب

Feature number	Firefly weight	Feature number	Firefly weight	Feature number	Firefly weight
۱	۰/۴۸	۱۴	۰/۵۹	۲۷	۰/۰۵۷
۲	۰/۵۴	۱۵	۰/۵۷	۲۸	۰/۳۵
۳	۰/۴۴	۱۶	۰/۵۷	۲۹	۰/۰۰۹۸
۴	۰/۴۹	۱۷	۰/۵۷	۳۰	۰/۱۳
۵	۰/۵۳	۱۸	۰/۶۰	۳۱	۰/۲۰
۶	۰/۵۸	۱۹	۰/۸۹	۳۲	۰/۱۹
۷	۰/۴۹	۲۰	۰/۴۵	۳۳	۰/۶۰
۸	۰/۵۱	۲۱	۰/۰۱۸	۳۴	۰/۷۴
۹	۰/۴۶	۲۲	۰/۸۲	۳۵	۰/۴۴
۱۰	۰/۵۴	۲۳	۰/۷۳	۳۶	۰/۴۶
۱۱	۰/۵۶	۲۴	۰/۴۰	۳۷	۰/۴۱
۱۲	۰/۴۸	۲۵	۰/۹۱	۳۸	۰/۵۲
۱۳	۰/۵۹	۲۶	۰/۸۹	–	–

درنهایت مقدار وزن برای هر یک از کلاس‌ها از لایه میانی به لایه خارجی ارسال می‌شود. با اعمال این وزن‌ها در مقادیر صفت‌ها، درصورتی‌که نتایج در آستانه مشخص شده صدق کنند، به کلاس مربوط به وزن‌ها اختصاص می‌یابند. درواقع می‌توان گفت نتایج حاصل از ضرب وزن‌ها در مقادیر صفت یک نمونه برای هریک از کلاس‌ها بیشتر باشد، نمونه موردنظر به آن کلاس اختصاص خواهد یافت.

٤-۱- ارزیابی روش پیشنهادی

برای سنجش دقت مدل پیشنهادی در این تحقیق، نرخ پیش‌بینی صحیح نمونه‌ها در مراحل آموزش مدل روی داده‌های آموزشی، اعتبار سنجی و

آزمایشی در مراحل تکرار مدل، مورد بررسی قرار می‌گیرد. بدین منظور ماتریسی با عنوان ماتریس آشفتگی[۵] رسم می‌شود که در آن تعداد داده‌های درست طبقه‌بندی شده در مقابل داده‌های غلط طبقه‌بندی شده در مراحل آموزش ، اعتبار سنجی و آزمایش داده‌ها مشخص می‌شود[۳۱, ۳۲]. این ماتریس شامل چهر عنصر مثبت صحیح[۶] (TP)، مثبت کاذب[۷] (FP)، منفی صحیح[۸] (TN) و منفی کاذب[۹] (FN) به شرح زیر است:

- TP: گره‌های سالم که کلاس واقعی آن‌ها نیز سالم است.
- TN: گره‌های نفوذ که کلاس واقعی آن‌ها سالم است.
- FP: گره‌های نفوذ که کلاس واقعی آن‌ها نفوذ است.
- FN: گره‌های سالم که کلاس واقعی آن‌ها نفوذ است.

حال پس از استخراج پارامترهای ماتریس آشفتگی، می‌توان معیارهای ارزیابی را بر اساس ماتریس آشفتگی به دست آورد. این معیارها شامل دقت، حساسیت، صحت، نرخ طبقه‌بندی، نرخ تشخیص، نرخ خطای مثبت و معیار F را به دست آورد. شکل (۵) مقایسه ماتریس آشفتگی مربوط به روش پیشنهادی و شبکه عصبی را نشان می‌دهد.

همان‌طور که در شکل (۵) نشان داده شده است، در روش پیشنهادی ۹۶.۷ درصد از کل داده‌ها درمجموعه‌داده که شامل داده‌های آموزشی، اعتبار سنجی و آزمایشی است، به‌درستی طبقه‌بندی شده‌اند. این در حالی است که شبکه عصبی درمجموع ۹۴.۹ درصد داده‌ها به‌درستی طبقه‌بندی کرده است. در جدول (۲) مقایسه مقادیر مربوط به روش پیشنهادی و شبکه عصبی نشان داده شده است.

همان‌طور که در جدول (۲) نشان داده شده است، روش پیشنهادی ازلحاظ معیارهای ارزیابی نسبت به شبکه عصبی عملکرد بهتری دارد. در شکل (۶) نمودار مربوط به مقایسه معیار نرخ طبقه‌بندی (دقت) بین روش پیشنهادی و شبکه عصبی در ده مرحله از Cross-validation 10-fold نشان داده شده است. نرخ طبقه‌بندی در روش پیشنهادی به‌صورت نرخ تشخیص گره‌های سالم و گره‌های مخرب در میان تمام گره‌های موجود درمجموعه‌داده است.

همان‌طور که در شکل (۶) نشان داده شده است، روش پیشنهادی ازلحاظ نرخ طبقه‌بندی (دقت) نسبت به روش شبکه عصبی بهبود داشته است. در روش شبکه‌های عصبی با توجه به این‌که روند آموزش به‌صورت کامل صورت می‌گیرد، ممکن است مدل دچار Overfitting شود. در این پدیده مدل تمرکز خود را بر روی نمونه‌های آموزشی منعطف می‌کند و تمامی ویژگی‌ها و روابط بین نمونه‌های آموزشی را فرامی‌گیرد و دقت آن در طبقه‌بندی نمونه‌های آموزشی به حداکثر مقدار خود می‌رسد. حال‌آنکه زمانی که نمونه‌های تستی جدید که قبلاً مدل آن‌ها را مشاهده نکرده است، وارد سیستم می‌شود، ممکن است مدل در تشخیص روابط بین ویژگی‌های نمونه‌های جدید که متفاوت از نمونه‌های آموزشی است، دقت کافی را نداشته و عملکرد سیستم کاهش یابد. بنابراین روش پیشنهادی به‌منظور جلوگیری از Oveefitting و افزایش عملکرد سیستم تشخیص نفوذ در شبکه، مراحل آموزشی را تا حدی که دقت موردنظر به دست آید ادامه می‌دهد. ازاین‌رو نمودار دقت روش پیشنهادی نسبت به روش شبکه‌های عصبی مصنوعی مقدار بهتری دارد. درواقع روش پیشنهادی توانسته است، درصد بیشتری از گره‌های حمله و گره‌های سالم را به‌درستی تشخیص دهد.

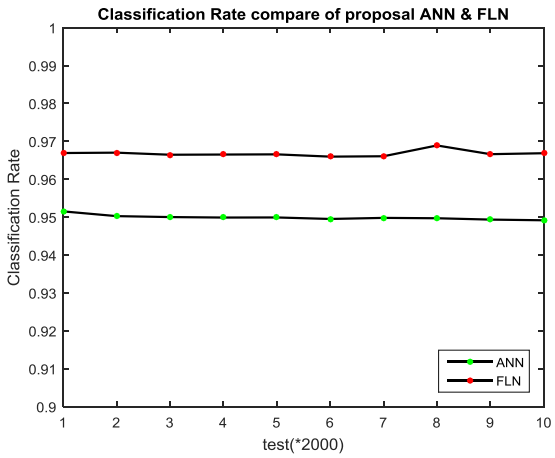
٤-۲- مقایسه روش پیشنهادی با روش‌های پیشین

پس از ارزیابی روش پیشنهادی با استفاده از معیارهای مرسوم در زمینه سیستم‌های تشخیص نفوذ در شبکه، حال نوبت به مقایسه روش پیشنهادی با سایر روش‌های پیشین به‌منظور بررسی میزان بهبود روش پیشنهادی نسبت و سایر روش‌هاست. با توجه به اهمیت سیستم‌های تشخیص نفوذ در شبکه که در فصل‌های قبلی نیز اشاره شد، محققان زیادی در این زمینه تلاش کرده‌اند که در ادامه روش پیشنهادی را به‌منظور بررسی نقاط ضعف و قوت آن با برخی ازاین‌روش‌ها مقایسه خواهیم کرد. ازآنجایی‌که تلاش بیشتر سیستم‌های تشخیص نفوذ در شبکه در راستای افزایش دقت پیش‌بینی گره‌های مخرب در شبکه است، پس مقایسه‌ها بر پایه معیارهای ماتریس آشفتگی که شامل نرخ طبقه‌بندی، نرخ تشخیص، دقت، صحت، حساسیت، نرخ تشخیص خطا و معیار F می‌باشد، استوار است. ازاین‌رو در جدول (۳) مقایسه روش پیشنهادی با روش‌های پیشین[۲۹, ۳۳, ۳۴] نشان داده شده است.

همان‌طور که در جدول (۳) نشان داده شده است، روش پیشنهادی از روش‌های پیشین ازلحاظ زمان و نرخ خطای منفی و معیار حساسیت عملکرد بهتری دارد و در کل با سایر سیستم‌های تشخیص نفوذ قابل‌مقایسه است.

۵- نتیجه

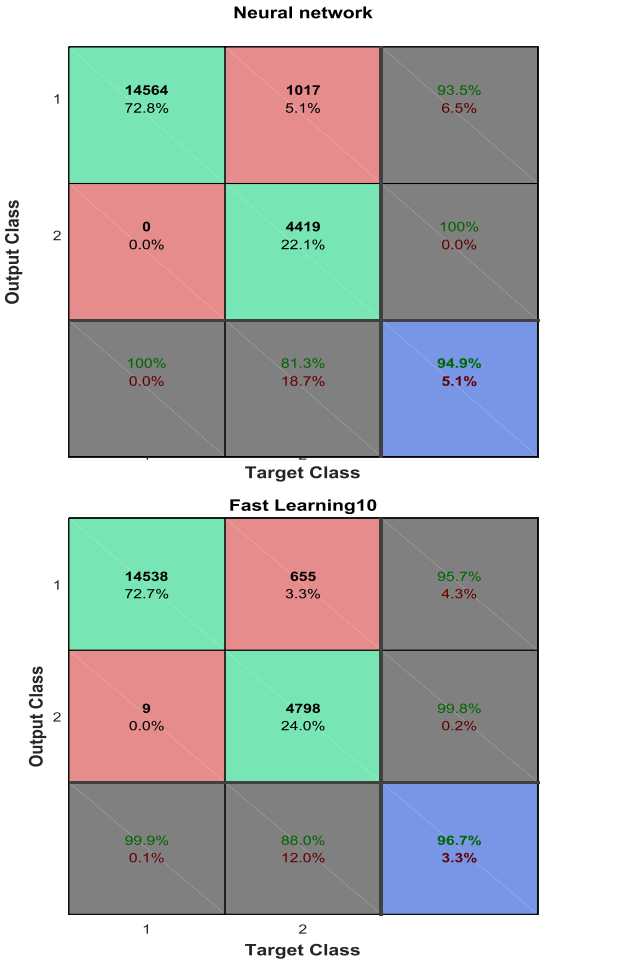
جلوگیری و کشف نفوذها و حملات در شبکه‌های حسگر بی‌سیم به یک امر حیاتی و چالشی جدی تبدیل شده است. از سوی دیگر با توجه به انرژی محدود گره‌های حسگر بی‌سیم، استفاده از گره‌های ناظر برای نظارت دائمی در شبکه‌های حسگر بی‌سیم به‌منظور جلوگیری و کشف نفوذ و حملات را در این نوع از شبکه‌ها عملاً غیرممکن کرده است. ازاین‌رو راه‌حلی برای غلبه بر این مشکل، امروزه بحث سیستم‌های کنترلی و نظارت از راه دور به یکی از مباحث موردعلاقه در زمینه‌های مختلف تبدیل شده است. نظارت از راه دور بر عملکرد و رفتار گره‌های موجود در شبکه‌های حسگر بی‌سیم علاوه بر تشخیص گره‌های مخرب و بدرفتار درون شبکه، می‌تواند به پیش‌بینی رفتار گره‌های بدرفتار در آینده نیز بیانجامد. ازاین‌رو در این پژوهش برای غلبه بر این مشکل از یک روش ترکیبی بر اساس انتخاب زیرمجموعه ویژگی مبتنی بر الگوریتم کرم شب‌تاب و شبکه یادگیری عصبی سریع استفاده شد. نتایج آزمایش‌ها نشان می‌دهد که دقت عملکرد روش پیشنهادی ۹۹.۹ ٪ بوده است که این مقدار در حد بالایی بوده و با سایر روش‌های پیشین قابل‌مقایسه است.



شکل (٦): مقایسه نرخ طبقه‌بندی (دقت) روش پیشنهادی و شبکه عصبی

جدول (۲) : مقادیر مربوط به معیارهای ارزیابی

معیار	روش پیشنهادی	شبکه عصبی
CR (Accuracy)	٪۹۹/۶۸	٪۹۴/۹۲
FPR	٪۰/۰۴۳۱	٪۰/۰۶۵۳
TPR	٪۹۹/۹۵	٪۹۸/۳۲
Precision	٪۹۵/۶۹	٪۸۱/۲۹
DR (Recall)	٪۹۹/۸۲	٪۱۰۰
F-measure	٪۹۷/۷۱	٪۸۹/۶۸



شکل (٥): مقایسه ماتریس آشفتگی روش پیشنهادی و شبکه عصبی

جدول (۳) : مقادیر مربوط به معیارهای ارزیابی

معیار	CR (Accuracy)	FPR	TNR	Precision	DR (Recall)	F-measure	Time (s)
روش پیشنهادی	٪۹۶/۶۸	٪۰/۰۴۳۱	٪۹۹/۹۵	٪۹۵/۳۳	٪۹۹/۸۲	٪۹۷/۷۱	۷۴/۴۸۱۴
شبکه عصبی	٪۹۴/۹۲	٪۰/۰۶۵۳	٪۹۸/۳۲	٪۸۱/۲۹	٪۱۰۰	٪۸۹/۶۸	۸۷/۳۰۶۴
روش ساخت افزایش تطبیقی (CAI)	٪۹۸/۹۲	٪۰/۹۲	٪۹۹/۰۸	٪۹۸/۳۳	٪۹۹/۱۳	٪۹۸/۴۸	۲۳۹/۹۶
ماشین پشتیبان بردار (SVM)	٪۹۹/۰۴	٪۱/۱۴	٪۹۸/۸۶	٪۹۹/۷۸	٪۹۹/۲۴	٪۹۹	۲۹۳۹/۸۸
شبکه پرسپترون چندلایه (MLP)	٪۹۹/۱۴	٪۰/۸۵	٪۹۹/۱۵	٪۹۹/۰۸	٪۹۸/۶۳	٪۹۹/۱۱	۷۶۲۲/۱۵
HSO based FLN	٪۹۵/۴	٪۰/۰۷۶۶	٪۹۹/۹۲	٪۹۸/۶۱	٪۹۵/۸۲	٪۹۷/۱۹	–
ATLBO based FLN	٪۹۱/۴۸	٪۰/۱۰۰۱	٪۸۹/۹۹	٪۹۱/۶۱	٪۹۲/۷۴	٪۹۲/۱۷	–
GA based FLN	٪۹۵/۳۵	٪۰/۱۶۶	٪۹۹/۸۳	٪۹۸/۶۱	٪۹۴/۷۴	٪۹۶/۶۴	–
PSO based FLN	٪۹۵/۷۱	٪۰/۱۷۸	٪۹۹/۸۲	٪۹۸/۴۵	٪۹۳/۶۴	٪۹۵/۹۹	–
DBN	٪۹۷/۹۰	٪۰/۲۱	٪۹۹/۷۹	٪۹۷/۸۱	٪۹۷/۹۱	٪۹۷/۴۷	۲۰۴۶۰۰
S-NDAE	٪۹۷/۸۵	٪۰/۲۱۵	٪۹۹/۷۸	٪۹۹/۹۹	٪۹۷/۸۵	٪۹۸/۱۵	۲۴۴۶

مراجع

[1] Liu, X., et al., *Information-centric mobile ad hoc networks and content routing: a survey.* Ad Hoc Networks, 2017. **58**: p. 255-268.
[2] Rosas, E., et al., *Survey on simulation for mobile ad-hoc communication for disaster scenarios.* Journal of Computer Science and Technology, 2016. **31**(2): p. 326-349.
[3] Rastegari, S., P. Hingston, and C.-P. Lam, *Evolving statistical rulesets for network intrusion detection.* Applied soft computing, 2015. **33**: p. 348-359.
[4] Young, C., et al., *Survey of Automotive Controller Area Network Intrusion Detection Systems.* IEEE Design & Test, 2019.
[5] Fotohi, R. and S. Jamali, *A comprehensive study on defence against wormhole attack methods in mobile Ad hoc networks.* International journal of Computer Science & Network Solutions, 2014. **2**: p. 37-56.
[6] Liu, G., Z. Yan, and W. Pedrycz, *Data collection for attack detection and security measurement in mobile ad hoc networks: A survey.* Journal of Network and Computer Applications, 2018. **105**: p. 105-122.
[7] Gupta, A.M.V., *Comprehensive survey on Blackhole attack with various Detection/Prevention techniques in Ad-hoc network.* International Journal of Applied Engineering Research, 2019. **14**(8): p. 2009-2017.
[8] Yeruru, S.V. and T.R. Rangaswamy, *An Anomaly-Based Intrusion Detection System with Multi-Dimensional Trust Parameters for Mobile Ad Hoc Network.* International Journal of Intelligence Engineering and Syatems, 2017. **10**(4): p. 81-90.
[9] Rajalakshmi, D. and K. Meena, *A Survey of intrusion detection with higher malicious misbehavior detection in Manet.* International journal of civil engineering and technology, 2017. **8**.
[10] Jamali, S. and V. Shaker, *Defense against SYN flooding attacks: a particle swarm optimization approach.* Computers & Electrical Engineering, 2014. **40**(6): p. 2013-2025.
[11] Babasaheb, D.R. and I. Raman. *Survey on Fault Tolerance and Security in Mobile Ad Hoc Networks (MANETs).* in *2018 3rd International Conference for Convergence in Technology (I2CT)*. 2018. IEEE.
[12] Soms, N. and P. Malathi, *Evolution of Intrusion Detection System in MANETs–A Survey.* International Journal of Innovations & Advancement in Computer Science (IJIACS), 2017. **6**(5).
[13] Jamali, S. and R. Fotohi, *DAWA: Defending against wormhole attack in MANETs by using fuzzy logic and artificial immune system.* the Journal of Supercomputing, 2017. **73**(12): p. 5173-5196.
[14] Scholar, M.T., S. GORAKHPUR, and I.C. Choubey, *A survey on malicious nodes in mobile ad hoc network.* Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org, 2016. **6**(3).
[15] Hajimirzaei, B. and N.J. Navimipour, *Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm.* ICT Express, 2019. **5**(1): p. 56-59.
[16] Dhanalakshmi, K. and B. Kannapiran, *Analysis of KDD CUP Dataset Using Multi-Agent Methodology with Effective Fuzzy Based Intrusion Detection System.* Journal of Applied Security Research, 2017. **12**(3): p. 424-439.
[17] Selvakumar, B. and K. Muneeswaran, *Firefly algorithm based feature selection for network intrusion detection.* Computers & Security, 2019. **81**: p. 148-155.
[18] Abedin, M., et al. *Performance Analysis of Anomaly Based Network Intrusion Detection Systems*. in *The 43nd IEEE Conference on Local Computer Networks (LCN)*. 2018. IEEE Computer Society.
[19] Chiba, Z., et al., *A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection.* Computers & Security, 2018. **75**: p. 36-58.
[20] Gupta, A. and A. Dubey, *A Survey on Various Applications and Blackhole Attack in Mobile Ad Hoc Network.* Recent Trends in Parallel Computing, 2018. **5**(1): p. 1-6.
[21] Chellam, A., L. Ramanathan, and S. Ramani, *Intrusion Detection in Computer Networks using Lazy Learning Algorithm.* Procedia computer science, 2018. **132**: p. 928-936.
[22] Ashfaq, R.A.R., et al., *Fuzziness based semi-supervised learning approach for intrusion detection system.* Information Sciences, 2017. **378**: p. 484-497.
[23] Karatas, G. and O.K. Sahingoz. *Neural network based intrusion detection systems with different training functions*. in *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. 2018. IEEE.
[24] Giokas, I., *Systems and methods for self-tuning network intrusion detection and prevention*. 2016, Google Patents.
[25] Al-Utaibi, K.A. and E.-S.M. El-Alfy, *Intrusion detection taxonomy and data preprocessing mechanisms.* Journal of Intelligent & Fuzzy Systems, 2018. **34**(3): p. 1369-1383.
[26] Madbouly, A.I. and T.M. Barakat, *Enhanced relevant feature selection model for intrusion detection systems.* International Journal of Intelligent Engineering Informatics, 2016. **4**(1): p. 21-45.
[27] Protić, D. and M. Stanković, *Anomaly-Based Intrusion Detection: Feature Selection and Normalization Influence to the Machine Learning Models Accuracy.* European Journal of Engineering and Formal Sciences, 2018. **2**(3): p. 101-106.
[28] Jain, Y.K. and S.K. Bhandare, *Min max normalization based data perturbation method for privacy protection.* International Journal of Computer & Communication Technology, 2011. **2**(8): p. 45-50.
[29] Ali, M.H., et al., *A new intrusion detection system based on fast learning network and particle swarm optimization.* IEEE Access, 2018. **6**: p. 20255-20261.
[30] Tilahun, S.L., J.M.T. Ngnotchouye, and N.N. Hamadneh, *Continuous versions of firefly algorithm: A review.* Artificial Intelligence Review, 2019. **51**(3): p. 445-492.
[31] Jamali, S. and Y.D. Navaei, *A two-level Product*

Recommender for E-commerce Sites by Using Sequential Pattern Analysis. International Journal of Integrated Engineering, 2016. **8**(1).

[32] Jamali, S. and G. Shaker, *PSO-SFDD: Defense against SYN flooding DoS attacks by employing PSO algorithm.* Computers & Mathematics with Applications, 2012. **63**(1): p. 214-221.

[33] Gurung, S., M.K. Ghose, and A. Subedi, *Deep Learning Approach on Network Intrusion Detection System using NSL-KDD Dataset.* International Journal of Computer Network and Information Security (IJCNIS), 2019. **11**(3): p. 8-14.

[34] Wang, C.-R., et al., *Network intrusion detection using equality constrained-optimization-based extreme learning machines.* Knowledge-Based Systems, 2018. **147**: p. 68-80.

زیرنویس‌ها

[1] Fast Learning Neural Network
[2] Particle swarm optimization
[3] Bayesian Networks
[4] Extreme learning machines
[5] Confusion Matrix
[6] True Positive
[7] False Positive
[8] True Negative
[9] False Negative