اولین کنفرانس ملی
عمران، معماری و فناوری اطلاعات در زندگی شهری
۱۳۹۹ - مشهد مقدس

یک سیستم تشخیص حملات توزیع شده رد سرویس خدمات در شهرهای هوشمند مبتنی بر شبکه نرم افزار محور

ابوالفضل نظری خاکشور[۱] ، محمد تحقیقی شریان[۲]

۱-گروه کامپیوتر، دانشگاه رجا، قزوین، ایران

۲-گروه کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران

چکیده

شبکه اینترنت اشیاء هر وسیله یا شی هوشمند را می‌تواند در بربگیرد و شبکه‌های کامپیوتری نیز می‌توانند یک جزء این شبکه باشند و از این جهت می‌توان انتظار داشت که این شبکه بسیار بزرگ و ناهمگن باشد زیرا گره‌های مختلف عضو آن می‌باشد. یکی از چالش‌های مهم در حوزه اینترنت اشیاء و کاربردهای آن مانند شهرهای هوشمند، بحث امنیت شبکه است و متاسفانه مشاهده می‌شود که چالش‌های مهم امنیتی، شبکه اینترنت اشیاء وکاربردهای آن نظیر شهرهای هوشمند را تهدید می‌نمایند و یکی از این چالش‌ها همان حملات رد سرویس خدمات توزیع شده و حملات آتشبار به شبکه شهر هوشمند است.این پژوهش اهداف زیادی را دنبال می کند که مهمترین اهداف آن شناسایی و تشخیص نفوذ به شبکه اینترنت اشیاء و شهرهای هوشمند و ارتقای امنیت کاربران در شهرهای هوشمندمی باشد .نوع مطالعات انجام شده برای این پژوهش و روش انجام پژوهش از نوع کتابخانه‌ای است و منابع آن از کتابخانه های آنلاین دانشگاه ها، کتب مرجع و مقالات معتبر، پایان نامه های مرتبط و اینترنت گرفته شده است. ازآنجا که در این پژوهش از ترکیب الگوریتم غنی و فقیر با شبکه عصبی مصنوعی به همراه سوئیچ های شبکه مبتنی بر نرم افزار محور استفاده شده است در مقایسه با برخی روشهای دیگر همچون الگوریتم های بهینه سازی وال و کفتار و پروانه که در این پژوهش مورد مقایسه واقع شده اند نتایج بهتری بدست آمده است.

واژگان کلیدی: الگوریتم غنی و فقیر، شبکه عصبی مصنوعی، سوئیچ های شبکه نرم افزار محور،سیستم تشخیص نفوذ

۱-مقدمه

یکی از موضوعات مهم در شبکه‌های کامپیوتری و بخصوص شبکه اینترنت اشیاء، امنیت در این شبکه‌ها است که باید حفظ شود و چالش‌های مختلف امنیتی وجود دارد که یکی از آنها حملات رد سرویس خدمات توزیع[۱] است که نمونه آن را می‌توان در حملات آتشبار[۲] مشاهده نمود. امروزه حملات آتشبار که با نرخ ترافیک پایین و عمرکوتاه ساخته می‌شود یکی از چالش‌های مهم در شبکه‌های از نوع اینترنت اشیاء است. در این نوع حملات سرویس دهندگان مورد حمله قرار گرفته نمی‌شوند اما در مقابل لینکهای ارسال و دریافت بسته مورد حمله قرار گرفته می‌شود. در این نوع از حملات مشاهده می‌شود مسیر و لینکهای ارتباطی در شبکه به عمد مورد حمله قرار گرفته می‌شود تا ترافیک شبکه با کندی از مبدا به مقصد هدایت شود. در این نوع حملات سرویس دهندگان مورد حمل نبوده و لینکهایی که ارتباط بین مبدا و مقصد را فراهم می‌نمایند به عنوان مقصد حمله در نظر گرفته می‌شود. یکی از روش‌های که می‌توان از آن برای مقابله با این نوع حملات استفاده نمود، بکارگیری سوئیچ‌های شبکه نرم افزار محور[۳] است (Galeano-Brajones,2020) در این نوع فناوری می‌توان آدرسهای مبدأ مورد اعتماد را شناسایی نمود و بدون صرف هزینه‌های زیاد و لوازم اضافی ترافیک شبکه را فیلتر نمود یا اجازه داد که این ترافیک در شبکه جریان یابد. برای دفع این حملات نیاز است که ترافیک شبکه را مورد تجزیه و تحلیل قرار داد و حملات و ویژگی‌های مهم آن را شناسایی نمود و برای این مورد می‌توان از یادگیری ماشین[۴] استفاده نمود و با تحلیل ترافیک شبکه می‌توان ترافیکی که توسط توسط مهاجمان ایجاد می‌شود را شناسایی (Tuan, 2020) نمود. نفوذ و حملات برعلیه شبکه‌های کامپیوتری روز به روز در حال افزایش است که یکی از آنها حملات رد سرویس خدمات است. حملات رد سرویس خدمات به حملاتی گفته می‌شود که یک هکر یا یک تیم هکری با ارسال درخواستهای مختلف اما کاذب به یک سرویس دهنده در وب امکانات پردازشی آن را بیهوده تلف نموده تا این سروس دهنده نتواند خدمات خود را بخوبی انجام دهد. در این نوع از حملات مکان حمله یک مورد نبوده بلکه تعداد زیادی گره در شبکه به ویروس آلوده شده و هر کدام از این ویروسها باعث می‌شوند تا یک درخواست کاذب برای سرویس دهنده ارسال شود و توان پردازش آن را مختل نماید. بیشتر حملات رد سرویس خدمات بر علیه شبکه‌های تجاری و بانکی اعمال می‌شود و در بیشتر موارد یک حمله سایبری[۵] پشت این حملات قرار دارد. مطالعات نشان می‌دهد حملات رد سرویس خدمات توزیع شده از سال ۲۰۱۲ تا کنون رشد قابل توجه‌ای داشته است و مشکل بزرگ این حملات آن است که در آنها تلاش می‌شود سرویس‌های کاربردی اینترنت مانند شبکه بانکی و مالی مورد هدف قرار گرفته شود. مطالعات نشان می‌دهد که ۲۳٪ حملات رد سرویس خدمات به شبکه-

[1] Distributed denial-of-service (DDoS)
[2] Crossfire
[3] Software-defined networking (SDN)
[4] Machine learning
[5] Cyber attack

های تجارت الکترونیک و شبکه‌های بانکی انجام می‌شود و مسلماً زیان این حملات قابل توجه بوده و باعث می‌شود که شناسایی این نوع از حملات مهم باشد و از جنبه‌های مختلف اهمیت بالایی داشته باشد. یکی از روش‌های که می‌تواند با حملات رد سرویس خدمات یا نوع خاص آن که به حملات آتشبار معرف است استفاده از سیستم‌های تشخیص نفوذ به شبکه است. یکی از چالش‌های مهم حملات رد سرویس خدمات، زیان مالی آنها است که به شبکه‌های کامپیوتری وارد می‌نمایند. مطالعات نشان می‌دهد که حملات نوع DDoS دارای بیشترین زیان قابل توجه به شبکه‌های کامپیوتری بوده و سپس در مرتبه دوم و سوم بدافزارها و کدهای مخرب قرار دارد .در واقع یکی از ضرورتهای مهم برای مقابله با حملات آتشبار و DDoS استفاده از سیستم‌های تشخیص نفوذ به شبکه است که سهم مهمی در افزایش و ارتقاء امنیت شبکه کامپیوتری دارد. مطالعات نشان می‌دهد که در صدر ابزارهای مقابله با حملات به شبکه‌های کامپیوتری دیواره آتش قرار دارد سپس در مرتبه دوم روش‌های مقابله با حملات DDoS مهم و حیاتی بوده و در مرتبه سوم نیز سیستم‌های تشخیص نفوذ به شبکه قرار دارند (Tounsi and Rais, 2018).

۱-۱: ادبیات و پیشینه تحقیق:

سای و همکاران سال ۲۰۱۹(Cai et al, 2019)، با استفاده از پیکربندی سیستم‌های پیشگیری از نفوذ مبتنی بر یک کاربر قانونی یک رویکرد پیشگیری از نفوذ به جای سیستم های تشخیص نفوذ فعلی ارائه دادند. یک سیستم پیشگیری از نفوذ (IPS) به عنوان یک نوع جدید از فناوری امنیت اطلاعات عمل می‌کند و پیکربندی و مدیریت آن در حال حاضر چالش مهم به شمار می‌رود. در این مقاله ، با تجزیه و تحلیل شبکه سعی می‌شود به این پرسش پاسخ داده شود که آیا یک شرکت به ترتیب از یک IPS به جای سیستم تشخیص نفوذ (IDS) در یک تنظیمات پیش فرض و یک پیکربندی بهینه استفاده نماید آیا می‌تواند عملکرد بهتری را کسب نماید. نتایج آنها نشان می دهد که IPS هنگام پیکربندی بهینه نمی تواند به شرکت صدمه بزند و از طرفی تنظیمات بهینه IPS نه تنها به پارامترهای هزینه بلکه به محیط خارجی (کیفیت IDS) که در آن شرکت فعالیت می‌کند بستگی دارد.

کریست و همکاران سال ۲۰۱۹ (Khraisat et al, 2019) ، یک مقاله مروری در مورد سیستم‌های تشخیص نفوذ و روش‌های مقابله با حملات سایبری ارائه دادند. امروزه می‌توان به جرات گفت که حملات سایبری پیچیده‌تر شده و در نتیجه چالش های فزاینده‌ای در تشخیص دقیق هجومها ایجاد شده است و عدم پیشگیری از هجوم می‌تواند اعتبار خدمات امنیتی را در شبکه کاهش دهد، به عنوان مثال محرمانه بودن اطلاعات، درستی و در دسترس بودن شبکه با این حملات

زیر سوال می‌رود. برای مقابله با تهدیدات امنیتی رایانه، روشهای زیادی برای کشف نفوذ تاکنون ارائه و معرفی شده است که می تواند به طور گسترده در سیستمهای تشخیص نفوذ متقابل مبتنی بر امضاها (SIDS) و سیستمهای تشخیص نفوذ مبتنی بر ناهنجاری (AIDS) طبقه بندی شود. این مقاله تلاش می‌کند تا یک طبقه بندی موثر از سیستم‌های تشخیص نفور به شبکه را ارائه دهد و با انجام یک بررسی جامع از آثار قابل توجه اخیر و یک مرور کلی از مجموعه داده‌های استفاده شده آنها را با هم مورد ارزیابی قرار دهد. همچنین تکنیک های استفاده شده توسط مهاجمان برای جلوگیری از شناسایی نیز در این پژوهش مورد استفاده قرار گرفته شده است.

ایلهنگ و همکاران سال ۲۰۱۹(Elhag et al,2019)، یک سیستم فازی تکاملی چند هدفی برای به دست آوردن مجموعه ای گسترده و دقیق از راه حل ها در سیستم های تشخیص نفوذ ارائه و معرفی نمودند. سیستم‌های تشخیص نفوذ برای نظارت بر شبکه با هدف پیدا کردن و جلوگیری از وقایع غیرعادی ارائه و ایجاد شده است. به طور خاص، در این پژوهش بر روی سیستم‌های تشخیص نفوذ تمرکز شده است که برای شناسایی چندین نوع حمله شناخته شده آموزش دیده‌اند. این موارد می تواند دسترسی غیرمجاز یا انکار حملات خدماتی باشد. هر زمان که اثری از یک رویداد مشکوک تشخیص داده شود آنگاه برای ایجاد هشدار و یا مسدود کردن این دسترسی خطرناک به سیستم هشدارهای لازم صادر می‌گردد. بسته به سیاست‌های امنیتی شبکه، مدیر شبکه ممکن است به دنبال موارد مختلفی باشد که وابستگی شدیدی به رفتار سیستم تشخیص نفوذ داشته باشند. برای یک برنامه مشخص، هزینه جمع آوری هشدارهای کاذب می‌تواند بالاتر از انجام قفل دسترسی پیشگیرانه باشد. در سناریوهای دیگر، می توان یک نوع صحیح تشخیص دقیق نوع حمله سایبری را برای انجام یک روش خاص ضروری دانست. در این پژوهش، یک سیستم فازی تکاملی چند هدفی را برای توسعه سیستمی در جهت تشخیص نفوذ به شبکه ارائه شده است که می‌تواند با استفاده از معیارهای مختلف آموزش داده شود. با افزایش فضای جستجو در حین بهینه‌سازی مدل، راه حل‌های دقیق‌تری محاسبه می‌گردد و علاوه بر این ، این طرح به

کاربر نهایی اجازه می‌دهد از میان مجموعه گسترده‌ای از راه حل‌ها تصمیم بگیرد که کدام یک برای ویژگی‌های شبکه فعلی مناسب‌تر است. نتایج تجربی آنها نشان می‌دهد روش پیشنهادی دارای کارایی بالایی در تشخیص نفوذ است.

بن و همکاران در سال ۲۰۱۹(Benmessahel et al, 2019)، با استفاده از رفتار هوش گروهی ملخ‌ها و شبکه عصبی مصنوعی یک روش برای تشخیص نفوذ به شبکه ارائه دادند. بسیاری از محققان برای مقابله با تهدیدات مختلف امنیتی رویکردهای مختلفی مانند سیستم های تشخیص نفوذ (IDS) را اتخاذ کرده‌اند. تشخیص نفوذ به یک سیستم ضروری برای تشخیص نقض‌های امنیتی مختلف تبدیل شده است. در این پژوهش با استفاده از برنامه الگوریتم بهینه‌سازی فرااکتشافی ملخ برای تشخیص نفوذ به شبکه از ترکیب آن با شبکه عصبی مصنوعی استفاده شده است و برای ساختن یک سیستم تشخیص پیشرفته و بهبود استفاده شده است. روش پیشنهادی آنها برای بررسی توانایی و عملکرد رویکرد پیشنهادی، به یک سری آزمایشات را انجام داده و مطالعات تجربی با استفاده از داده‌های ارزیابی شناسایی نفوذ مانند KDD استفاده شده است. آزمایشات نشان می‌دهد رویکرد پیشنهادی آنها دقیق‌تر می شود از الگوریتم ذرات و الگوریتم ژنتیک عمل می‌نماید.

دیا و گوپتا در سال ۲۰۲۰ (Dahiya and Gupta, 2020)، یک روش مبتنی بر چند راه حل و تکنیک در مقابل حملات DDoS ارایه دادند تا امنیت شبکه را افزایش دهند. پیچیدگی و شدت حملات رد سرویس خدمات توزیع شده روز به روز در حال افزایش است. اینترنت از نظر توزیع منابع از ساختار بسیار متناقضی برخوردار است. راه حل های فنی بی شماری در این حوزه وجود دارد ، اما راه حل‌های موجود برای افزایش امنیت شبکه با توجه به جنبه‌های اقتصادی مورد توجه قرار نگرفته است. بنابراین ، در این پژوهش ، یک مکانیسم مبتنی بر چند ویژگی برای کاهش حملات رد سرویس خدمات توزیع شده ارائه شده است و تلاش شده مکانیزم شناسایی افراد معتبر در شبکه به شیوه حریصانه انجام شود تا از ارسال بسته‌های بیهوده و مبتنی بر حملات رد سرویس خدمات توزیع شده جلوگیری شود. نتایج به دست آمده از شبیه سازی‌ها به وضوح نشان داد که روش پیشنهادی عملکرد بهتری نسبت به تکنیک های کاهش حملات رد سرویس خدمات توزیع شده مرسوم دارد.

۲-۱: راه کار پیشنهادی

یکی ازچالش‌های موجود در حملات رد سرویس خدمات و حملات آتشبار آن است که برخی از تکنیک‌ها در مورد شناسایی مبداء غیرقابل اعتماد وجود دارد اما این روش‌ها ایستا بوده و توانایی یادگیری ندارند اما در روش پیشنهادی برای شناسایی مبداء حملات از یک روش یادگیری ماشین استفاده می‌نمایند و در واقع تلاش می کند با یادگیری ماشین‌های که در شبکه حملات ردسرویس خدمات و حملات آتشبار را انجام می‌دهند شناسایی نماید و سپس به کمک سوئیچ‌های SDN تلاش می‌شود تا جریان داده آنها فیلتر شود. در روش پیشنهادی تلاش می‌شود که با شناسایی مبداء حملات، همزمان حملات ردسرویس خدمات و حملات آتشبار به شبکه خنثی شود. در اینجا نقش شبکه عصبی مصنوعی یک روش طبقه‌بندی است که ترافیک آتشبار را از نرمال تشخیص می‌دهد و اگر یک ترافیک از نوع حمله و آتشبار تشخیص داده شود آنگاه مبداء ارسال ترافیک به عنوان عامل حمله در سویچ SDN فیلتر می‌شود. در روش پیشنهادی شبکه عصبی مصنوعی دارای تعدادی ورودی است که این ورودی‌ها از نوع ویژگی‌های ترافیک شبکه می‌توانند باشند و اگر ورودی-ها به شبکه عصبی مصنوعی(Wang and Qin, 2020) وصل شوند آنگاه خروجی دو حالت است یا ترافیک نرمال یا غیرنرمال را نشان می‌دهد. چالش مهم برای هر ابزار طبقه‌بندی و یادگیری ماشین مانند شبکه عصبی مصنوعی در تشخیص حملات آتشبار دو موضوع ذیل است:

۱.شبکه عصبی به عنوان یک عامل کشف حملات رد سرویس خدمات و حملات آتشبار نیاز است که فقط بر روی ویژگی‌های مهم متمرکز شود تا خطای تشخیص مبداء حملات کاهش داده شود.

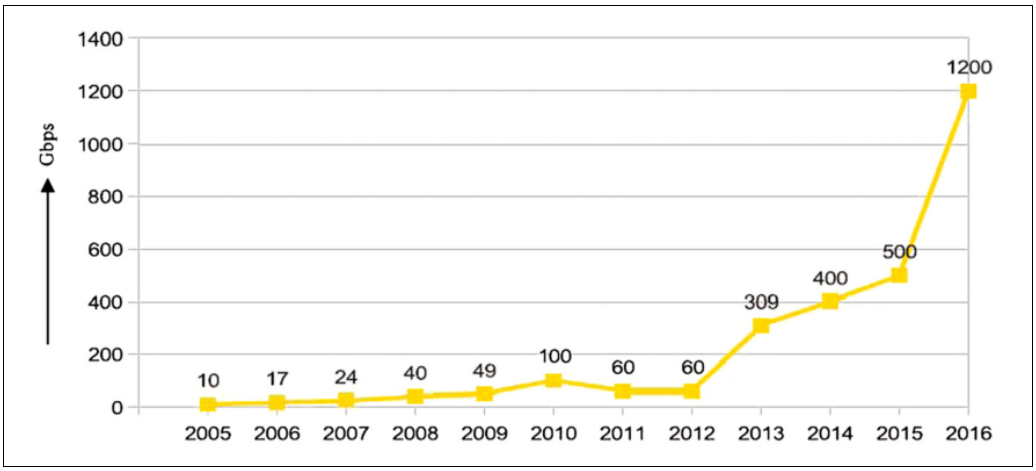
۲.در روش پیشنهادی با انتخاب ویژگی، ورودی شبکه عصبی به عنوان تکنیک یادگیری ماشین داده می‌شود و این موضوع باعث می‌شود ورودی دچار کاهش ابعاد[6] شده و تعداد کمتری ورودی برای یادگیری در نظر گرفته شود و از این جهت زمان پردازش نیز کاهش داده شود.

در روش پیشنهادی مجموعه‌ای از ویژگی‌ها که می‌تواند به نظر مهم یا غیر مهم باشد به عنوان ویژگی‌های ترافیک شبکه و حملات رد سرویس خدمات و حملات آتشبار در نظر گرفته می‌شود و این ویژگی‌ها به عنوان یک بردار در نظر گرفته می‌شود که می‌تواند صفر یا یک در نظر گرفته شود. در این صفر نشان می‌دهد که این ویژگی در تشخیص حملات نقش زیادی ندارد و یک نشاندهنده نقش و اهمیت آن است. در روش پیشنهادی یک بردار ویژگی بهینه نیاز است که به عنوان ورودی شبکه عصبی مصنوعی در نظر گرفته شود تا خطای تشخیص حملات شناسایی مبداء حملات کاهش داده شود و

[6] Dimension reduction

از این جهت فاز انتخاب ویژگی را برروی بردارهای ویژگی اعمال نموده تا بهینه‌ترین بردار ویژگی برای یادگیری شبکه عصبی مصنوعی درنظرگرفته شود. درروش پیشنهادی برای تشخیص نوع ترافیک مخرب تلاش می‌شود تا ترافیک شبکه مورد انتخاب ویژگی قرار گرفته شود و سپس این ترافیک دچار کاهش ابعاد شود و به عنوان ورودی یادگیری شبکه عصبی مصنوعی درنظرگرفته شود تا با دقت بیشتر و زمان کمترترافیک تحلیل و سوئیچ‌های SDN در مورد جریان داده مورد نظر تصمیم‌گیری نمایند. درروش پیشنهادی برای انتخاب ویژگی و فیلتر نمودن ورودی یادگیری شبکه عصبی مصنوعی جهت تشخیص مبداء حملات از الگوریتم بهینه‌سازی فقیرو غنی[۷] (Moosavi and Bardsiri 2019)که در سال ۲۰۱۹ ارایه شده است استفاده می‌شود زیرا این الگوریتم پیچیدگی اندک دارد و از طرفی دارای خطای محاسباتی اندکی است.

۳-۱: اهمیت موضوع:

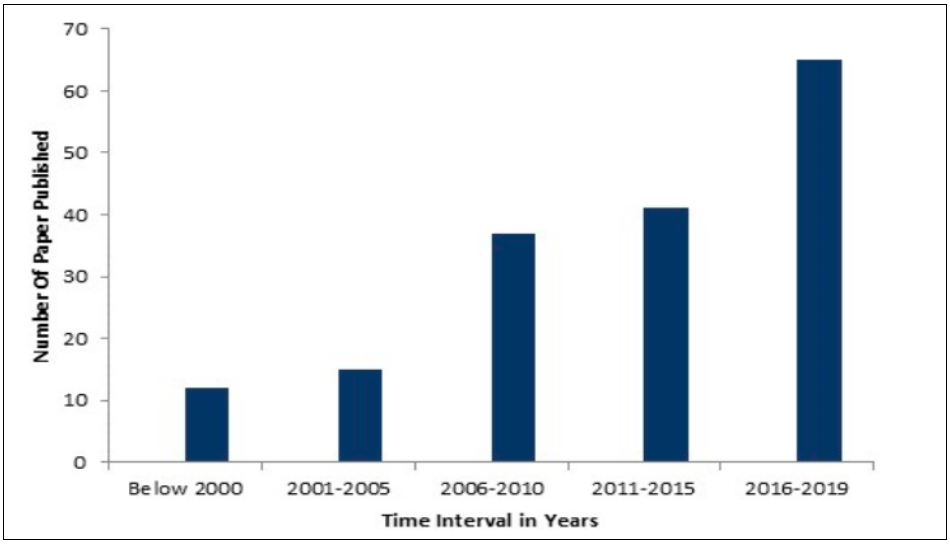


شکل .Error! No text of specified style in document: **افزایش حملاتDDOS بر علیه شبکه های کامپیوتری**

با توجه به نمودار فوق مشاهده می‌شود که تعداد زیادی از ترافیک شبکه‌های کامپیوتری مرتبط با بسته‌های است که بیهوده و برای حملات DDoS ارسال می‌شوند و باعث می‌شود ترافیک شبکه توسط این حملات به هدر برود. بیشتر حملات رد سرویس خدمات بر علیه شبکه‌های تجاری و بانکی اعمال می‌شود و در بیشتر موارد یک حمله سایبری پشت

[7] Poor and rich optimization algorithm

این حملات قرار دارد. مطالعات نشان می‌دهد حملات رد سرویس خدمات توزیع شده از سال ۲۰۱۲ تا کنون رشد قابل توجه‌ای داشته است و مشکل بزرگ این حملات آن است که در آنها تلاش می‌شود سرویس‌های کاربردی اینترنت مانند شبکه بانکی و مالی مورد هدف قرار گرفته شود. مطالعات نشان می‌دهد که ۲۳٪ حملات رد سرویس خدمات به شبکه-های تجارت الکترونیک و شبکه‌های بانکی انجام می‌شود و مسلماً زیان این حملات قابل توجه بوده و باعث می‌شود که شناسایی این نوع از حملات مهم باشد و از جنبه‌های مختلف اهمیت بالایی داشته باشد. یکی از روش‌های که می‌تواند با حملات رد سرویس خدمات یا نوع خاص آن که به حملات آتشبار معرف است استفاده از سیستم‌های تشخیص نفوذ به شبکه است. یکی از چالش‌های مهم حملات رد سرویس خدمات زیان مالی آنها است که به شبکه‌های کامپیوتری وارد می‌نمایند. مطالعات نشان می‌دهد که حملات نوع DDoS دارای بیشترین زیان قابل توجه به شبکه‌های کامپیوتری بوده و سپس در مرتبه دوم و سوم بدافزارها و کدهای مخرب قرار دارد. در واقع یکی از ضرورتهای مهم برای مقابله با حملات آتشبار و DDoS استفاده از سیستم‌های تشخیص نفوذ به شبکه است که سهم مهمی در افزایش و ارتقاء امنیت شبکه کامپیوتری دارد.در نمودار شکل(۷-۱)، تعداد مقالات معتبر در چند سال اخیر برای مقابله با حملات نمایش داده شده و می‌توان مشاهده نمود که تعداد پژوهش در این زمینه در حال افزایش است و این افزایش می‌تواند به دلیل آن باعث که حملات بر علیه شبکه و تکنیک‌های آن در حال افزایش و تنوع است:



شکل۲: افزایش تعداد مقالات در مورد مقابله به حملات به شبکه های کامپیوتری

با توجه به مطالب فوق، می‌توان اهمیت روش پیشنهادی برای تشخیص حملات آتش‌بار وDDoS را در موارد ذیل خلاصه نمود:

- نفوذ به شبکه‌های کامپیوتری در حال افزایش بوده و حملات رد سرویس خدمات و آتش‌بار نیز در حال توسعه و گسترش است.
- حملات رد سرویس خدمات و آتش‌بار زیان قابل توجه‌ای به شبکه دارد.
- حملات رد سرویس خدمات و آتش‌بار زیان باعث شده تا خدمات شبکه‌های کامپیوتری برای کاربران از بین رفته و این خدمات متوقف شود.

٤-١: فرضیات تحقیق

فرضیات این تحقیق به شرح ذیل ارایه و معرفی می‌شود:

۱.روش پیشنهادی با انتخاب ویژگی در زمان کمتر و با دقت بیشتر می‌تواند مبداء حملات رد سرویس خدمات و آتشبار را شناسایی نماید.

۲.استفاده از یادگیری ماشین در کنار تفکیک جریان داده مخرب و مبتنی بر حملات در سوئیچ‌های SDN نفوذ به شبکه را تا حدود زیادی غیر ممکن می‌نماید.

۳. کاهش دادن همزمان متوسط خطای تشخیص ترافیک نرمال از غیر نرمال و همچنین کاهش دادن تعداد ویژگی انتخاب شده عامل مهم در افزایش کارایی روش پیشنهادی است.

۴.خطای تشخیص نفوذ به شبکه و شناسایی حملات به اندازه جمعیت و تکرار الگوریتم غنی و فقیر و همچنین به پارامترهای یادگیری نظیر تعداد لایه‌های پنهان و تعداد نورونهای عصبی هر لایه پنهان بستگی دارد.

٥-١:اهداف پژوهش:

۱. شناسایی و تشخیص نفوذ به شبکه اینترنت اشیاء و شهرهای هوشمند
۲. شناسایی حملات مخرب رد سرویس خدمات توزیع شده و حملات آتشبار با شناسایی مبداء حملات
۳. افزایش دقت در شناسایی حملات به شهرهای هوشمند با روش‌های یادگیری و فناوری SDN

۴. ارتقای امنیت کاربران در شهرهای هوشمند

۵. بهبود امنیت شبکه با هوش گروهی انسان نظیر الگوریتم بهینه‌سازی غنی و فقیر و روش‌های یادگیری

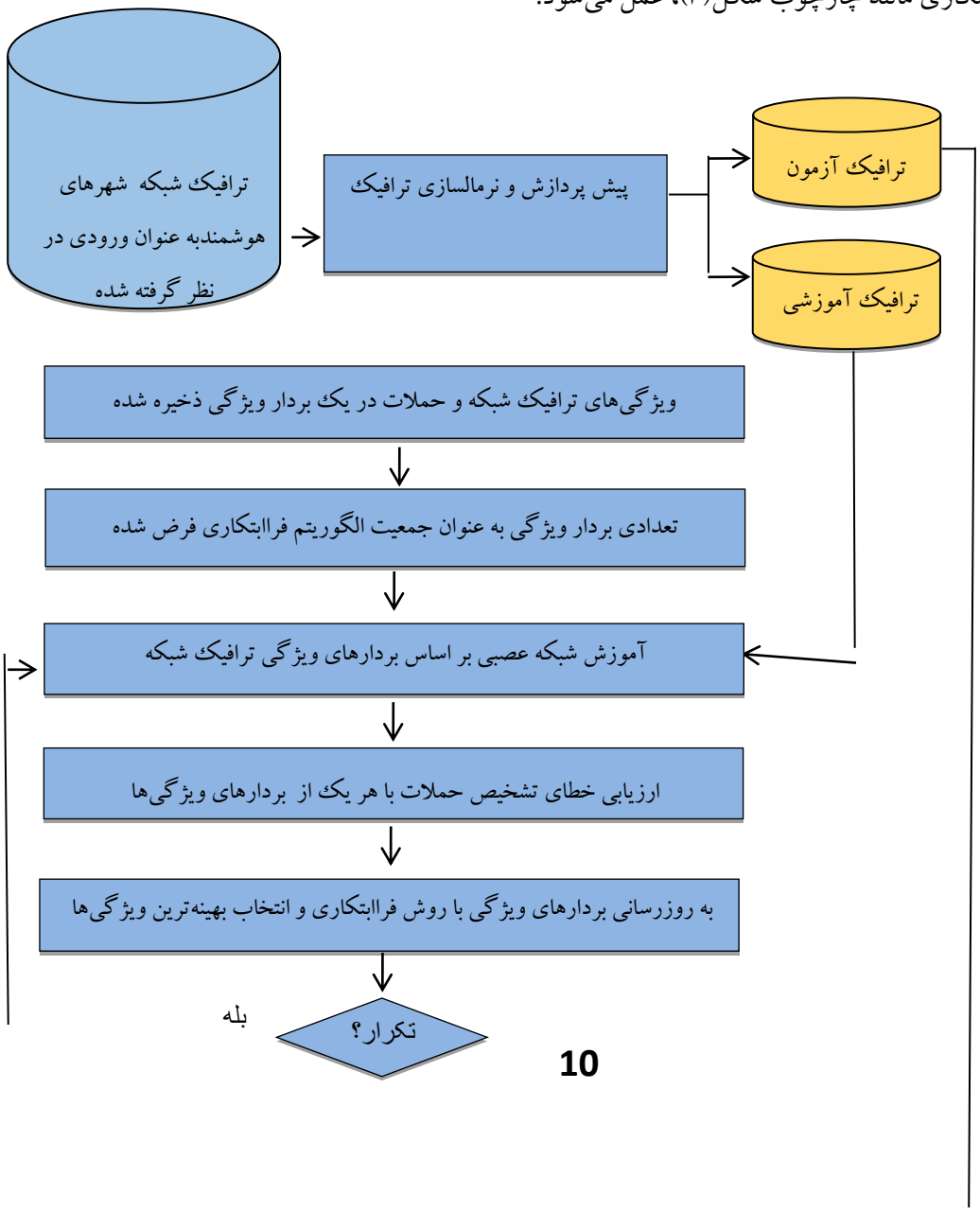
ارایه یک روش و چارچوب برای تشخیص حملات به شهرهای هوشمند با تلفیق روش‌های مختلف

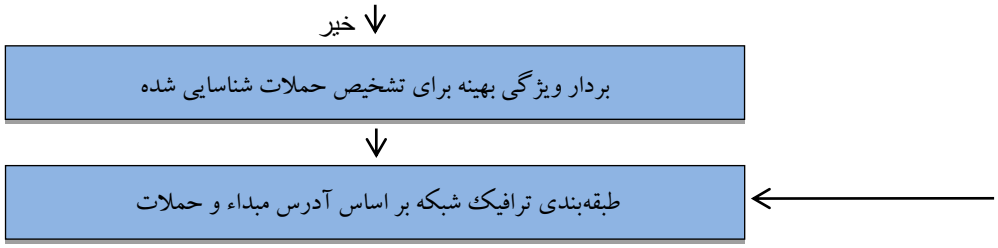
اهداف دیگر نیز می باشد که از برشمردن آنها صرفنظرمی گردد.

در ادامه روش پیشنهادی در این پژوهش شرح داده خواهدشد.

۲- روش پیشنهادی:

برای شناسایی حملات رد سرویس خدمات و حملات آتشبار در روش پیشنهادی با استفاده از توانایی یادگیری ماشین و الگوریتم‌های فراابتکاری مانند چارچوب شکل(۳)، عمل می‌شود:





شکل۳: چارچوب پیشنهادی در تشخیص حملات رد سرویس خدمات و حملات آتشبار

در این چارچوب ترافیک شبکه به عنوان ورودی در نظر گرفته می‌شود و این ترافیک پیش پردازش شده و بخشی از این ترافیک که برچسب آن از نظر حملات رد سرویس خدمات و حملات آتشبار بودن و نرمال بودن مشخص است در نظر گرفته شده و این ترافیک برچسب‌دار برای آموزش و یادگیری شبکه عصبی مصنوعی استفاده می‌شود. در اینجا نقش شبکه عصبی مصنوعی یک روش طبقه‌بندی است که ترافیک حملات رد سرویس خدمات و حملات آتشبار را از نرمال تشخیص می‌دهد و اگر یک ترافیک از نوع حمله و آتشبار تشخیص داده شود آنگاه مبداء ارسال ترافیک به عنوان عامل حمله در سویچ SDN فیلتر می‌شود.

در روش پیشنهادی شبکه عصبی مصنوعی دارای تعدادی ورودی است که این ورودی‌ها از نوع ویژگی‌های ترافیک شبکه می‌توانند باشند و اگر ورودی‌ها به شبکه عصبی مصنوعی وصل شوند آنگاه خروجی دو حالت است یا ترافیک نرمال یا غیرنرمال را نشان می‌دهد. چالش مهم برای هر ابزار طبقه‌بندی و یادگیری ماشین مانند شبکه عصبی مصنوعی در تشخیص حملات رد سرویس خدمات و حملات آتشبار دو موضوع ذیل است:

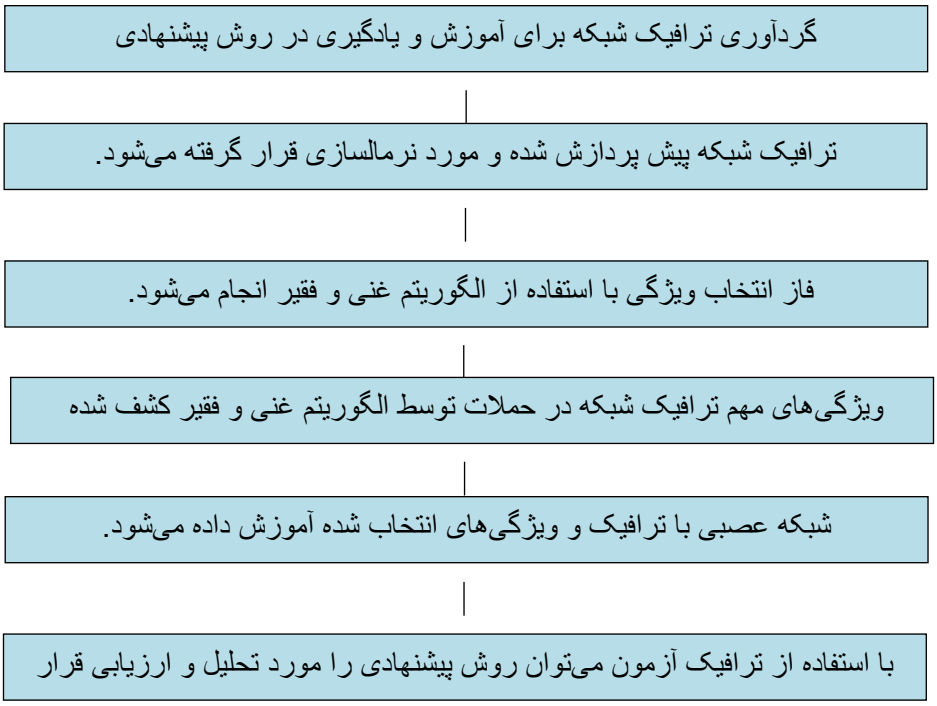
الف:شبکه عصبی به عنوان یک عامل کشف حملات رد سرویس خدمات و حملات آتشبار نیاز است که فقط بر روی ویژگی‌های مهم متمرکز شود تا خطای تشخیص مبداء حملات کاهش داده شود.

ب: در روش پیشنهادی با انتخاب ویژگی ورودی شبکه عصبی یا هر روش یادگیری ماشین هم کاهش داده می‌شود و این موضوع باعث می‌شود ورودی دچار کاهش ابعاد[8] شده و زمان پردازش نیز کاهش داده شود.

[8] Dimension reduction

2-1: مراحل روش پیشنهادی

تشخیص حملات رد سرویس خدمات و حملات آتشبار به شبکه یک مسئله بهینه‌سازی و از نوع طبقه‌بندی است زیرا نیاز است که ترافیک نرمال از غیرنرمال شبکه طبقه‌بندی شود از طرفی خطای طبقه‌بندی کمینه‌یابی و بهینه‌سازی شود از این جهت در فاز طبقه‌بندی از الگوریتم‌های یادگیری ماشین و داده‌کاوی استفاده می‌شود و در فاز کمینه نمودن خطای طبقه‌بندی ترافیک نرمال از غیرنرمال از الگوریتم‌های بهینه‌سازی استفاده می‌شود. مراحل اساسی در روش پیشنهادی برای تشخیص ترافیک نرمال و غیرنرمال در روش پیشنهادی به مانند شکل4، است:



شکل Error! No text of specified style in document.**: مراحل روش پیشنهادی برای تشخیص نفوذ به شبکه**

در روش پیشنهادی در ابتدا داده‌ها و ترافیک شبکه گردآوری شده و از این ترافیک برای آموزش شبکه عصبی مصنوعی چند لایه به عنوان یک روش طبقه‌بندی استفاده می‌شود تا بتوان نوع ترافیک نرمال از ترافیک آتشبار و حمله را تشخیص دهد. برای بهبود عملکرد روش پیشنهادی در ابتدا ترافیک پیش پردازش شده و می‌توان مهمترین فاز پیش پردازش را نرمالسازی ترافیک شبکه در نظر گرفت سپس می‌توان ترافیک نرمال شده را برای آموزش شبکه عصبی مصنوعی استفاده نمود. در روش پیشنهادی از همه ویژگی‌های ترافیک شبکه استفاده نمی‌شود بلکه فقط ترافیک و ویژگی‌های مهم آن برای یادگیری شبکه عصبی مصنوعی استفاده می‌شود و می‌توان انتخاب ویژگی را برای این مرحله در نظر گرفت.

برای انتخاب ویژگی از الگوریتم بهینه‌سازی فقیر و غنی[9] که در سال ۲۰۱۹ (Moosavi and Bardsiri,2019)ارایه شده است استفاده می‌شود. علت استفاده از این الگوریتم در روش پیشنهادی برای انتخاب ویژگی را می‌توان در دلایل ذیل خلاصه نمود:

- الگوریتم ساده است و پیچیدگی ندارد و از طرفی این الگوریتم دقت بالایی دارد.
- الگوریتم بر اساس هوش انسانی است و می‌تواند در ترکیب با یادگیری ماشین توانایی تحلیل ترافیک شبکه را افزایش دهد.

۳- تجزیه و تحلیل روش پیشنهادی:

روش پیشنهادی در حوزه طبقه‌بندی قرار دارد و هدف آن است که ترافیک شبکه به دسته نرمال و آتشبار طبقه‌بندی شود و از این جهت برای تجزیه و تحلیل روش پیشنهادی در تشخیص حملات آتشبار می‌توان از شاخص‌های مانند خطای تشخیص نفوذ به شبکه به مانند رابطه(۱)، استفاده نمود:

رابطه ۱
$$mse = \frac{1}{m}\sum_{i=1}^{m}(\bar{Y}_i - Y_i)^2$$

در این روابط، نوع ترافیک واقعی از نظر حمله بوده DDOS یا آتشبار بودن یا نرمال بودن با Y_i و مقدار تخمینی آن نیز با $\bar{Y}_i$ نمایش داده شده است و از طرفی m برابر تعداد ترافیک موجود برای ارزیابی است. متغییری مانند خطای تشخیص

[9] Poor and rich optimization algorithm

حملات وابسته است و این وابسته بوده می‌تواند به متغیرهای مستقل مانند اندازه جمعیت و تعداد تکرار الگوریتم فراابتکاری و همچنین تعداد لایه‌های شبکه عصبی بستگی داشته باشد. در جدول(۱)، تعدادی از پارامترها و متغیرهای مهم وابسته که برای ارزیابی روش پیشنهادی می‌توان استفاده نمود در جدول(۱)، نمایش داده شده است:

جدول ۱: تعدادی از متغیرهای وابسته در ارزیابی روش پیشنهادی

روش	مفهوم
TP	ترافیک از نوع حمله رد سرویس خدمات و حمله آتشبار است و روش پیشنهادی به درستی نوع ترافیک را حمله و از نوع آتشبار تشخیص داده است.
TN	ترافیک از نوع حمله رد سرویس خدمات و حمله آتشبار نبوده و روش پیشنهادی به درستی نوع ترافیک را نرمال و عادی تشخیص داده است.
FP	ترافیک از نوع حمله رد سرویس خدمات و حمله آتشبار نبوده است و روش پیشنهادی به غلط نوع ترافیک را حمله و از نوع آتشبار تشخیص داده است.
FN	ترافیک از نوع حمله رد سرویس خدمات و حمله آتشبار بوده است و روش پیشنهادی به غلط نوع ترافیک را نرمال و عادی تشخیص داده است.

۴-یافته ها

یک سوال مهم که برای آن باید پاسخ قانع کننده ارایه نمود آن است که چرا برای انتخاب ویژگی و کاهش دادن ابعاد ترافیک شبکه در سیستم‌ها و شبکه نرم‌افزار محور از الگوریتم بهینه غنی و فقیر استفاده شده است. برای پاسخ دادن به این سوال می‌توان این الگوریتم را روی توابع ارزیابی که برای سنجش دقت الگوریتم‌های فراابتکاری بکار می‌روند مورد آزمایش قرار داد. توابع ارزیابی در واقع مجموعه‌ای از توابع بهینه‌سازی بوده که به عنوان یک مسئله بهینه‌سازی بکار گرفته می‌شود و هدف آن است که مشخص شد که الگوریتم بهینه غنی و فقیر یا هر الگوریتم فراابتکاری تا چه اندازه می‌تواند خطای الگوریتم را کاهش دهد. دو تابع ارزیابی مهم Sphere و Ackley وجود دارد که در بیشتر پژوهش‌ها

برای ارزیابی و سنجش دقت الگوریتم‌های فراابتکاری استفاده می‌شود. تابع ارزیابی Sphere یکی از توابع ارزیابی پرکاربرد برای سنجش دقت الگوریتم‌های فراابتکاری است. این تابع ارزیابی فقط یک کمینه سراسری ۱۰ دارد و فاقد هرگونه بهینه محلی می‌باشد. تابع ارزیابی مورد نظر دارای یک بهینه یا کمینه سراسری در $x = ۰, y = ۰$ بوده که مقدار تابع ارزیابی به ازای آن کمینه ممکن و برابر $f^*(۰,۰) = ۰$ است. تابع Ackley نیز به مانند Sphere دارای بهینه در مختصات $x = ۰, y = ۰$ است و مقدار بهینه آن نیز برابر صفر است اما این تابع دارای پیچیدگی بالایی بوده و دارای بی نهایت بهینه محلی است که هر الگوریتم را با چالش مواجه می‌سازد. معادله تابع ارزیابی Sphere و Ackley به ترتیب مطابق رابطه(۱-۴) و (۲-۴) بیان و ارایه شده است:

$$f(x,y) = x^۲ + y^۲$$

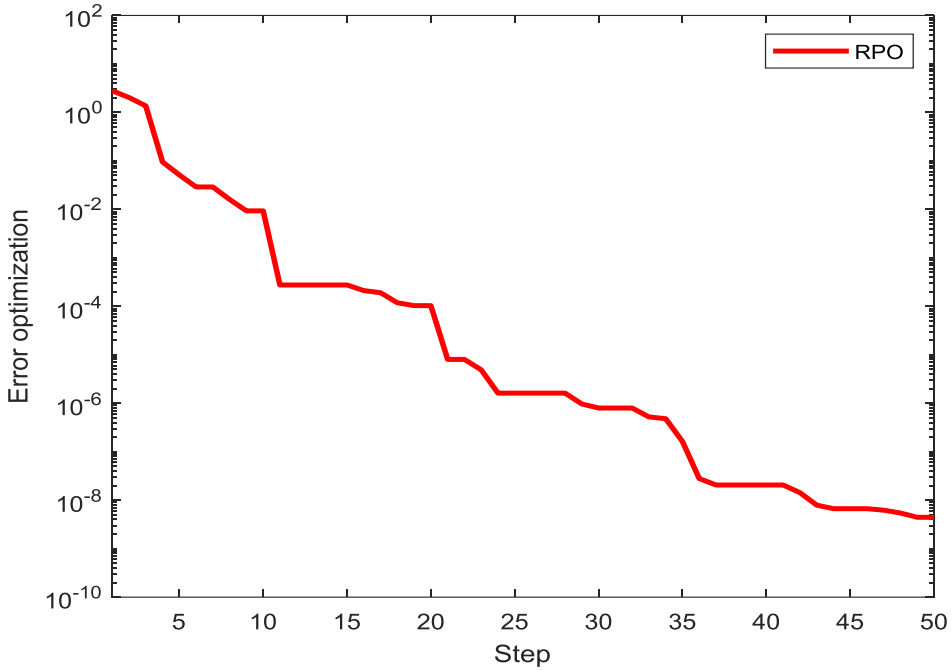
Error! No text of specified style in document.-۱

$$f(x,y) = ۲۰ exp\left(-۰.۲\sqrt{\frac{x^۲+y^۲}{۲}}\right) - exp\left(\frac{۱}{۲}(cos2(\pi x) + cos2(\pi y))\right) + ۲۰ + e$$

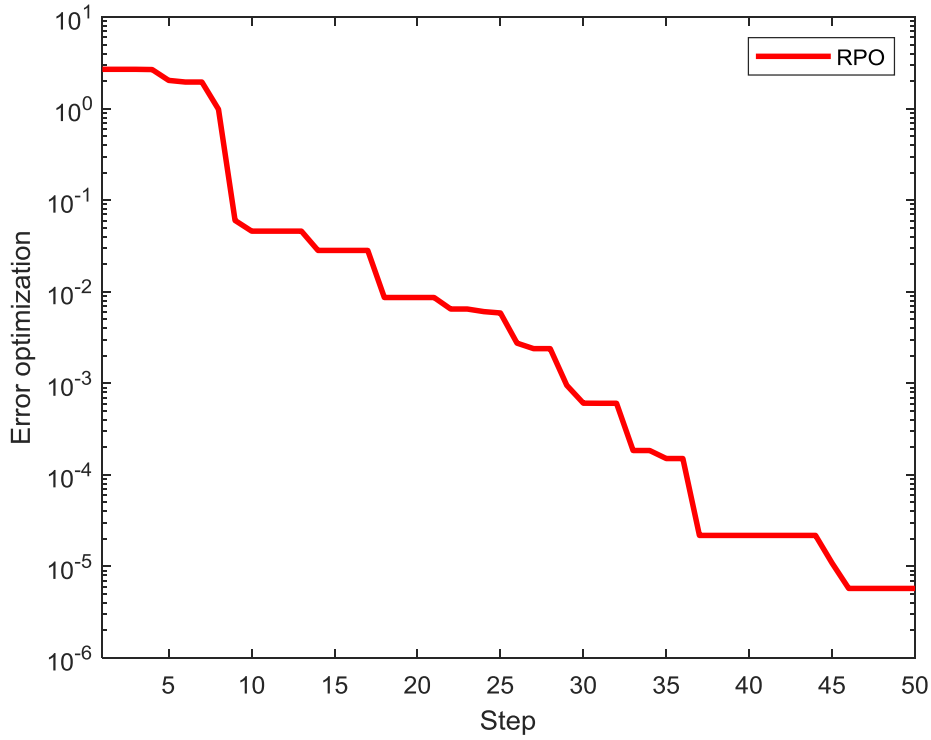
Error! No text of specified style in document.-۲

می‌توان الگوریتم بهینه‌سازی غنی و فقیر را روی این دو تابع ارزیابی پیاده‌سازی نمود و سپس متوسط خطای محاسبه بهینه سراسری الگوریتم فراابتکاری روی این توابع بر حسب تکرار به ترتیب در نمودار شکل۴ و۵ نمایش داده شده است:

[10] Global minimum



شکلError! No text of specified style in document. : کاهش یافتن خطای محاسبه بهینه روی تابع ارزیابی اول



شکل٦: کاهش یافتن خطای محاسبه بهینه روی تابع ارزیابی دوم

در شکل 5 و 6، دو نمونه از روند کاهش یافتن خطای الگوریتم بهینه‌سازی غنی و فقیر روی دو تابع ارزیابی Sphere و Ackley که برای سنجش خطای الگوریتم‌های فراابتکاری بکار گرفته می‌شود نمایش داده شده است و هدف از این دو خروجی آن است که نشان داده شود خطای الگوریتم مورد نظر برای محاسبه بهینه تا چه اندازه اندک است و می‌تواند برای توسعه روش پیشنهادی بکار گرفته شود:

تجزیه و تحلیل الگوریتم پیشنهادی یا الگوریتم بهینه‌سازی فقیر و غنی نشان می‌دهد این الگوریتم اگر با جمعیت ۱۰ و تعداد تکرار ۵۰ انجام شود در تابع ارزیابی اول خطای در حدود ۹ رقم اعشار و در تابع ارزیابی دوم نیز خطای آن در حدود ۴ رقم اعشار است. به عبارت بهتر الگوریتم بهینه‌سازی فقیر و غنی در توابع ارزیابی مختلف دارای خطای ناچیزی است و می‌توان از آن برای انتخاب ویژگی در تحلیل ترافیک شبکه استفاده نمود و خطای تشخیص حملات را به کمک این الگوریتم تا حد امکان کاهش داد. در اینجا برای سنجش سطح خطای الگوریتم بهینه‌سازی فقیر و غنی در یافتن جواب بهینه از دو تابع ارزیابی معرف که مختص ارزیابی الگوریتم‌های فراابتکاری است استفاده شده است و مطالعات و آزمایشات دیگر ما نیز بخوبی نشان می‌دهد روش الگوریتم بهینه‌سازی فقیر و غنی روی سایر توابع ارزیابی نیز خطای اندکی را برای یافتن جواب بهینه ارایه می‌دهد و می‌توان از آن برای مسئله پیچیده و چند بعدی انتخاب ویژگی در تشخیص حملات به شبکه از آن استفاده نمود و از این جهت در بخش بعدی یک نسخه باینری از آن برای انتخاب ویژگی ترافیک شبکه و تشخیص حملات استفاده می‌شود.

۵-نتیجه گیری:

نتایج آزمایشات و تحلیل الگوریتم پیشنهادی با مجموعه داده‌های مرتبط با حملات نشان می‌دهد:

۱. تابع هدف انتخاب ویژگی که دارای دو بخش متوسط خطا و متوسط تعداد ویژگی انتخاب شده است بر حسب آموزش روش پیشنهادی کاهش یافته و این کاهش نشان می‌دهد خطا و تعداد ویژگی در تشخیص حملات در روش پیشنهادی مرتباً در حال کاهش است.

۲.خطای الگوریتم پیشنهادی بر حسب تکرار در حال کاهش بوده و دقت آن نیز بر حسب تکرار در حال افزایش است و این بدان دلیل است که الگوریتم پیشنهادی بر حسب آموزش در حال یافتن بردارهای ویژگی بهینه برای تحلیل ترافیک شبکه است.

۳.خطای تشخیص حملات در روش پیشنهادی، الگوریتم بهینه‌سازی وال، الگوریتم بهینه‌سازی کفتار و الگوریتم بهینه-سازی پروانه به ترتیب برابر ۰.۱۰۷، ۰.۱۲۹، ۰.۱۳۶ و ۰.۱۴۷ است.

۴.دقت روش پیشنهادی، الگوریتم بهینه‌سازی وال، الگوریتم بهینه‌سازی کفتار و الگوریتم بهینه‌سازی پروانه برای تشخیص حملات نیز برابر ۹۸.۸۵٪، ۹۸.۳۲٪، ۹۸.۱۴٪ و ۹۷.۸۴٪ است.

۵.روش پیشنهادی خطای کمتری در تشخیص حملات نسبت به الگوریتم بهینه‌سازی وال، الگوریتم بهینه‌سازی کفتار و الگوریتم بهینه‌سازی پروانه دارد و از طرفی دقت آن نیز نسبت به این روش‌های انتخاب کننده ویژگی در تشخیص حملات بیشتر است.

۶.روش پیشنهادی در شاخص دقت برای تشخیص حملات نسبت به الگوریتم بهینه‌سازی وال، الگوریتم بهینه‌سازی کفتار، الگوریتم بهینه‌سازی پروانه، الگوریتم کبوتر، الگوریتم ماهی، الگوریتم ژنتیک و ماشین بردار پشتیبان دارای عملکرد بهتری است.

۱.Galeano-Brajones, J., et al., Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. Sensors, ۲۰۲۰. ۲۰(۳): p. .۸۱٦

۲.Tuan, N.N., et al., A DDoS Attack Mitigation Scheme in ISP Networks Using Machine Learning Based on SDN. Electronics, ۲۰۲۰. ۹(۳): p. .٤۱۳

3. Tounsi, W. and H. Rais, A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security, ۲۰۱۸. ۷۲: p. .۲۳۳-۲۱۲

4.Cai, C., S. Mei, and W. Zhong, Configuration of intrusion prevention systems based on a legal user: the case for using intrusion prevention systems instead of intrusion detection systems. Information Technology and Management, ۲۰۱۹. ۲۰(۲): p. .۷۱-۵۵

5.Khraisat, A., et al., Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, ۲۰۱۹. ۲(:(۱p. .۲۰

6. Elhag, S., et al., A multi-objective evolutionary fuzzy system to obtain a broad and accurate set of solutions in intrusion detection systems. Soft Computing, ۲۰۱۹. ۲۳(٤): p. ۱۳۳٦-۱۳۲۱

7.Benmessahel, I., et al., A new evolutionary neural networks based on intrusion detection systems using locust swarm optimization. Evolutionary Intelligence, ۲۰۱۹. ۱۲(۲): p. ۱٤٦-۱۳۱

8.Dahiya, A. and B. Gupta, Multi Attribute Auction Based Incentivized Solution Against DDoS Attacks. Computers & Security, :۲۰۲۰p. ۱۰۱۷٦۳

9. Wang, M., Lu, Y., & Qin, J. (2020). A dynamic MLP-based DDoS attack detection method using feature selection and feedback. *Computers & Security*, *88*, 101645.

10.Moosavi, S. H. S., & Bardsiri, V. K. (2019). Poor and rich optimization algorithm: A new human-based and multi populations algorithm. *Engineering Applications of Artificial Intelligence*, *86*, 165-181.