یازدهمین کنفرانس بین المللی نوآوری و تحقیق در علوم مهندسی
گرجستان – تفلیس(۱۹ اسفند ماه ۱۴۰۰) -آکادمی بین المللی علوم و مطالعات گرجستان
ICIRES 2022
www.icires.ir
info@icires.ir

ارائه سیستم ترکیبی تشخیص حملات DDoS در شبکه‌های نرم‌افزار محور با رای‌گیری از عملکرد الگوریتم‌های طبقه‌بندی

بختیار جانانی[۱]، علی غفاری[۲]
[۱]گروه مهندسی کامپیوتر، واحد علوم و تحقیقات آذربایجان شرقی، دانشگاه آزاد اسلامی، تبریز، ایران
[۲] گروه مهندسی کامپیوتر، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران

چکیده - امروزه با گسترش روزافزون شبکه های کامپیوتری و اینترنت، مدیریت این شبکه ها با مشکلات زیادی روبرو شده است. معماری شبکه‌های مبتنی بر نرم افزار با جداسازی لایه کنترلی و داده توانسته قابلیت برنامه‌ریزی، انعطاف‌پذیری و پویایی را برای پشتیبانی از نیاز شبکه-های جدید ایجاد نماید. این معماری پیشنهادی، به عنوان راهکاری برای شبکه‌های آینده مورد توجه محققان دانشگاهی و صنعتی قرار گرفته است. با این حال، باید توجه داشت که معماری شبکه نرم افزار محور نیز از همان مسائل امنیتی که در مورد شبکه های رایج مطرح است، رنج می‌برد. به عنوان مثال، یکی از ضعف‌های معماری نرم افزار محور مربوط به آسیب‌پذیری بالای آن در برابر حملات منع سرویس توزیع شده و سایر موارد مشابه به آن می‌باشد. در این تحقیق، به منظور مقابله با حملات منع سرویس توزیع شده، یک روش ترکیبی جدید مبتنی بر یادگیری ماشین و با رای گیری از عملکرد الگوریتم های طبقه بندی شده ارائه شده است. الگوریتم های یادگیری ماشین بردار پشتیبان، k نزدیکترین همسایه و درخت تصمیم می باشد. در نهایت از خروجی سه روش مذکور رای گیری به عمل می آید. نتایج حاصل از شبیه سازی روش پیشنهادی نشان می دهد که این روش در مقایسه با روش های دیگر در برابر حملات منع سرویی توزیع شده مقاوم بوده و کارایی آن مناسب می باشد.

کلید واژه- الگوریتم های دسته بندی، تشخیص حملات، حملات انکار سرویس، شبکه های نرم افزار محور.

۱- مقدمه

در سال های اخیر، با توجه به توسعه اینترنت و تجهیزات مخابراتی و الکترونیکی هوشمند مانند گوشی‌های هوشمند، تبلت‌ها و رایانه‌های همراه و همچنین ظهور مفاهیمی چون رایانش ابری ، شبکه‌های اجتماعی، اینترنت اشیاء و شبکه‌های مخابراتی نسل ۴ و ۵ نیازمندی‌های شبکه تغییر کرده است. بنابراین مواردی چون دسترسی به گذردهی بالا، توسعه‌پذیری، مدیریت خودکار و ارائه کیفیت مناسب در شبکه از چالش‌هایی هستند که معماری سنتی شبکه نمی‌تواند پاسخ‌گوی آن‌ها باشد. معماری شبکه‌های مبتنی بر نرم‌افزار برای افزایش قابلیت پویایی، قابلیت کنترل، قابلیت انعطاف و نوآوری ارائه گردیده است که اصلی‌ترین شناسه آن جداسازی فضای کنترلی از فضای ارسال بسته‌ها است. شبکه‌های کامپیوتری با کاربردهای متفاوت به سرعت در حال توسعه هستند و نیازمندی های مختلفی مانند رایانش ابر، تحلیل دادگان عظیم، امنیت و پشتیبانی از حرکت گره‌ها را به شبکه‌های گسترده تحمیل می‌کنند. معماری شبکه‌های سنتی به تدریج و در اثر افزایش کاربران و نرخ تنوع نرم‌افزارهای کاربردی ارائه‌شده در معرض مشکلاتی قرار گرفته‌اند که حل این مشکلات از موضوعات مورد توجه محققان دانشگاهی و صنعتی قرار گرفته است؛ بنابراین پروژه‌های تحقیقاتی بسیاری در سراسر جهان تعریف شدند که معماری‌های مختلفی برای شبکه‌های نسل آینده پیشنهاد داده و طراحی کرده‌اند. نتایج اولیه تحقیقات انجام شده نشان می‌دهد که محدود بودن شبکه های سنتی دلیل اصلی عدم توسعه شبکه های سنتی است. معماری شبکه های سنتی با مشکلات زیادی رو به رو هستند.

با این حال در سال های اخیر شبکه‌های مبتنی بر نرم‌افزار به عنوان معماری اصلی شبکه‌های آینده پیشنهاد شده است[۳-۱]. معماری شبکه‌های مبتنی بر نرم‌افزار بخش کنترلی و انتقال داده را از یکدیگر جدا کرده و ترافیک شبکه را به صورت متمرکز در کنترل‌کننده مدیریت می کند. کنترل‌کننده با استفاده از