



تاریخ:
شماره:
پیوست:

فرم تعریف پروژه کارشناسی ارشد

شماره دانشجویی: ۴۰۰۲۱۰۷۵۵
تعداد واحدهای گذرانده: ۳
معدل: ۱۳.۱۰
نام استاد راهنمای همکار پروژه: (در صورت وجود):
نام استاد ممتحن پروژه:

نام و نام خانوادگی دانشجو: روح‌الله جهان‌افروز
گرایش دانشجو: رایانش امن
نام استاد راهنمای پروژه: دکتر رسول جلیلی
تعداد واحد پروژه: ۶

عنوان کامل پروژه:

فارسی: ارائه رویکرد تطبیق‌پذیر با تنوع ترافیکی شبکه‌های پهن‌بند برای شناسایی حملات منع‌خدمت توزیع‌شده
انگلیسی: An Adaptive Approach with the Variety Characteristic of the High-Bandwidth Networks for Distributed Denial of Service Attacks Detection

☐ نظری

☒ کاربردی

شرح مختصر پروژه: (با تاکید بر اهمیت موضوع، مشکلات موجود، تعریف مسئله، کاربردها، دادگان مورد استفاده (در صورت نیاز) و نحوه ارزیابی در حدود ۲۵۰ کلمه)

با توجه به گسترش روزافزون شبکه‌های کامپیوتری و متداول‌شدن استفاده از آنها، حجم تبادل و انتقال اطلاعات نیز بالاتر رفته و امروزه نرخ‌گذر اطلاعات در بسیاری از تجهیزات شبکه به بیش از ۱۰۰ گیگابایت در ثانیه رسیده است. از طرفی با متنوع‌شدن کاربردهای شبکه، شاهد رفتارهای متفاوت در ترافیک هستیم. با افزایش نرخ ترافیک، چالش‌های امنیتی نظیر تشخیص حملات منع‌خدمت، که به دلیل سادگی در پیاده‌سازی و تاثیر بسیار مخرب [۱] یک تهدید جدی به حساب می‌آیند، افزایش پیدا کرده است. سیستم‌های تشخیص نفوذ علیرغم اینکه نقش مهمی در شناسایی آسیب‌ها دارند، اما در ترافیک‌هایی با نرخ‌گذردهی بالا به درستی نمی‌توانند ترافیک را پایش^۱ و حملات را تشخیص دهند [۲ و ۳].

در دهه‌های گذشته، محققان روش‌های شناسایی بسیاری را برای حملات منع‌خدمت توزیع‌شده پیشنهاد کرده‌اند. بیشتر روش‌های موجود مبتنی بر یادگیری ماشین یا یادگیری عمیق هستند. در این روش‌ها با تغییر در رفتار ترافیک باید مدل را با تعداد زیادی از داده‌های ترافیک شبکه برچسب‌گذاری شده از قبل، آموزش داد که این عملیات در شبکه‌های با نرخ‌گذر بالا و ترافیک متغیر می‌تواند بسیار زمانبر باشد [۴]. راهکار ارائه شده توسط شی و چنگ [۴] با استفاده از ویژگی نامتقارن، ترافیک‌های غیرعادی را تشخیص می‌دهد. ضعف این راهکار این است که با تغییر رفتار ترافیک شبکه باید به صورت دستی سائز جداول استفاده‌شده را تعیین کرد. همچنین با استفاده از ویژگی نامتقارن می‌توان تنها حملات منع‌خدمت کمی را تشخیص داد. روش ارائه شده توسط مونیال و وارگری [۲] نیز مبتنی بر شبکه‌های نرم‌افزارمحور هست که امکان ارتقای آن و استفاده در شبکه‌های با نرخ‌گذردهی بالا وجود ندارد. همچنین عدم سازگارپذیری مقدار حد‌آستانه الگوریتم استفاده‌شده، شناسایی تنها انواع خاص حملات منع‌خدمت، و استفاده از تنها یک معیار آماری از دیگر مشکلات موجود در این روش هستند. راهکار دیگری به نام پوسایدن [۵] مبتنی بر سویچ‌های برنامه‌پذیر توسط ژانگ و همکاران ارائه شده است. این روش علیرغم سازگارپذیری با تنوع ترافیکی، به دلیل استفاده از روش نمونه‌برداری تصادفی بسته‌ها^۲ برای تشخیص حملات، از دقت کافی برخوردار نیست. راهکار جاکن [۶] نیز علیرغم برطرف نمودن ضعف‌های موجود در پوسایدن [۵]، به علت عدم واریسی کامل بسته‌ها توسط سویچ‌ها، قادر به پیاده‌سازی برخی مکانیزم‌های تشخیص مبتنی بر محتوای داده‌ای بسته‌ها^۳ نیست. لذا برای شناسایی صحیح حملات منع‌خدمت در شبکه‌های پهن‌بند نیاز به یک رویکرد و روشی است که شامل دو ویژگی پردازش جامع به معنای پردازش تمامی بسته‌ها و سازگارپذیری به معنای قابلیت تطبیق‌پذیری با ترافیک متغیر باشد [۷].

در این پایان‌نامه قصد داریم رویکردی بهینه و تطبیق‌پذیر با تنوع ترافیکی موجود در شبکه‌های پهن‌بند برای شناسایی حملات منع‌خدمت توزیع‌شده معرفی نماییم که از دو ویژگی پردازش جامع و سازگارپذیری برخوردار باشد. در روش پیشنهادی از DPDK استفاده می‌کنیم که سرعت ضبط و پردازش بسته‌ها را به طرز چشمگیری بهبود می‌بخشد. کارایی روش ارائه شده را نیز در مقایسه با دیگر راهکارها و با در نظر گرفتن معیارهایی نظیر میزان استفاده از پردازشگر و حافظه، نرخ دورانداختن بسته‌ها، و میزان تاخیر در شناسایی حملات بررسی می‌کنیم.

¹ Monitor

² Packet Sampling

³ Payload Information



فرم تعریف پروژه کارشناسی ارشد

تاریخ:

شماره:

پیوست:

کلمات کلیدی: ۱- حملات منع خدمت توزیع شده ۲- شبکه‌های پهن‌بند ۳- تطبیق‌پذیری با تنوع ترافیکی ۴-DPDK
۵- سامانه‌های تشخیص نفوذ

مراحل انجام پروژه و زمان‌بندی آن:

۱	مطالعه مقالات پیشین در این زمینه	۱ (ماه)
۲	ارائه روش پیشنهادی	۳ (ماه)
۳	جمع‌آوری داده	۱ (ماه)
۴	پیاده‌سازی و ارزیابی روش	۵ (ماه)
۵	نگارش پایان‌نامه	۲ (ماه)

الف) مراجع:

- [۱] Salopek, D., Zec, M., Mikuc, M., & Vasić, V. (2022). Surgical DDoS Filtering With Fast LPM. *IEEE Access*, 10, 4200-4208.
- [۲] Varghese, J. E., & Muniyal, B. (2021). An Efficient IDS framework for DDoS attacks in SDN environment. *IEEE Access*, 9, 69680-69699.
- [۳] Hu, Q., Yu, S. Y., & Asghar, M. R. (2020). Analysing performance issues of open-source intrusion detection systems in high-speed networks. *Journal of Information Security and Applications*, 51, 102426.
- [۴] Shi, H., Cheng, G., Hu, Y., Wang, F., & Ding, H. (2021). RT-SAD: Real-Time Sketch-Based Adaptive DDoS Detection for ISP Network. *Security and Communication Networks*, 2021.
- [۵] Zhang, M., Li, G., Wang, S., Liu, C., Chen, A., Hu, H., ... & Wu, J. (2020, February). Poseidon: Mitigating volumetric ddos attacks with programmable switches. In *the 27th Network and Distributed System Security Symposium (NDSS 2020)*.
- [۶] Liu, Z., Namkung, H., Nikolaidis, G., Lee, J., Kim, C., Jin, X., ... & Sekar, V. (2021). Jaqen: A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 3829-3846).
- [۷] Noferesti, M., & Jalili, R. (2020). ACoPE: An adaptive semi-supervised learning approach for complex-policy enforcement in high-bandwidth networks. *Computer Networks*, 166, 106943.

ب) دروس مورد نیاز:

تخصصی (ارتباط موضوع پروژه با دروسی که دانشجو گذرانده یا باید بگذراند)			جبرانی		
باید بگذراند	نمره	گذرانده	باید بگذراند	نمره	گذرانده

استاد راهنما:	نظر گروه:	نظر کمیته تحصیلات تکمیلی دانشکده:
تاریخ تحویل فرم به مدیر گروه:	تاریخ جلسه گروه:	تاریخ جلسه کمیته:
امضای استاد راهنما:		

بسمه تعالی

دانشکده مهندسی کامپیوتر



دانشگاه صنعتی شریف

فرم تعریف پروژه کارشناسی ارشد

تاریخ:

شماره:

پیوست:

امضای معاون تحصیلات تکمیلی:	امضای مدیر گروه:	
-----------------------------	------------------	--

توجه: فرم تعریف پروژه بایستی یک روز قبل از جلسه گروه توسط استاد راهنما تحویل مدیر گروه شود.