بسمه تعالی

دانشکده مهندسی کامپیوتر

تاریخ: .....

شماره:.....

پیوست: .....

فرم تعریف پروژه کارشناسی ارشد

دانشگاه صنعتی شریف

نام و نام خانوادگی دانشجو: روح‌الله جهان‌افروز — شماره دانشجویی: ۴۰۰۲۱۰۷۵۵

گرایش دانشجو: رایانش امن — تعداد واحدهای گذرانده: ۳ — معدل: ۱۳.۱۰

نام استاد راهنمای پروژه: دکتر رسول جلیلی — نام استاد راهنمای همکار پروژه: (در صورت وجود):

تعداد واحد پروژه: ۶ — نام استاد ممتحن پروژه:

عنوان کامل پروژه:

فارسی: ارائه رویکرد تطبیق‌پذیر با تنوع ترافیکی شبکه‌های پهن‌باند 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

نوع پروژه: کاربردی ✓ — نظری ✓

با توجه به گسترش روزافزون شبکه‌های کامپیوتری و متداول‌شدن استفاده از آنها، حجم تبادل اطلاعات نیز بالاتر رفته و امروزه نرخ‌گذر اطلاعات در بسیاری از تجهیزات شبکه به بیش از ۱۰۰گیگابیت‌درثانیه 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 بسیارمخرب [۱] یک تهدید جدی به حساب می‌آیند، افزایش پیدا کرده‌است. سیستم‌های تشخیص نفوذ در ترافیک‌هایی با نرخ گذردهی بالا به درستی نمی‌توانند ترافیک را پایش[1] و حملات را تشخیص دهند[۲و۳].

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 سایز 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 وارگزی[۲] نیز مبتنی بر شبکه‌های نرم‌افزارمحور هست که امکان استفاده در شبکه‌های با نرخ گذردهی بالا را ندارد. 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 سوییچ‌های برنامه‌پذیر توسط ژانگ و همکاران ارائه شده است. این روش علیرغم سازگارپذیربودن با تنوع ترافیکی، به‌دلیل استفاده از روش نمونه‌برداری تصادفی بسته‌ها[2] برای تشخیص حملات، از دقت کافی برخوردار نیست. راهکار جاکن[۶] نیز علیرغم برطرف نمودن ضعف‌های موجود در پوسایدن[۵]، به علت عدم وارسی کامل بسته‌ها توسط سوییچ‌ها، قادر به پیاده‌سازی برخی مکانیزم‌های تشخیص مبتنی بر محتوای داده‌ای بسته‌ها[3] نیست. لذا برای شناسایی صحیح حملات منع‌خدمت در شبکه‌های پهن‌باند نیاز به یک رویکردی 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 تطبیق‌پذیر با تنوع ترافیکی موجود در شبکه‌های پهن‌باند 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 پردازش بسته‌ها را به طرز چشمگیری بهبود می‌بخشد. کارایی روش ارائه شده را نیز در مقایسه با دیگر راهکارها و با در نظرگرفتن معیارهایی نظیر میزان استفاده از پردازشگر و حافظه، نرخ دورانداختن بسته‌ها، و میزان تاخیر در شناسایی حملات بررسی می‌کنیم.

کلمات کلیدی: ۱- حملات منع‌خدمت توزیع‌شده ۲- شبکه‌های پهن‌باند ۳-تطبیق‌پذیری با تنوع ترافیکی ۴-DPDK ۵-سامانه‌های تشخیص نفوذ

[1] Monitor
[2] Packet Sampling
[3] Payload Information

بسمه تعالی

دانشکده مهندسی کامپیوتر

تاریخ: .....

شماره:.....

پیوست: .....

فرم تعریف پروژه کارشناسی ارشد

دانشگاه صنعتی شریف

مراحل انجام پروژه و زمان‌بندی آن:

۱.	مطالعه مقالات پیشین در این زمینه	۱ (ماه)
۲.	ارائه روش پیشنهادی	۳ (ماه)
۳.	جمع آوری 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.

[٤] 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*.

[٥] 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)*.

[٦] 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:

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

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

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