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: تعداد واحدهای گذرانده: معدل:

نام استاد راهنمای پروژه: نام استاد راهنمای همکار پروژه: (در صورت وجود):

تعداد واحد پروژه: ۶ نام استاد ممتحن پروژه:

عنوان کامل پروژه:

فارسی: ارائه راهکار تطبیق پذیر برای شناسایی حملات منع‌خدمت توزیع‌شده در شبکه‌های پهن‌باند

انگلیسی: An Adaptive Approach for Detecting Distributed Denial of Service Attacks in High-Bandwidth Networks

نوع پروژه: کاربردی ✓ نظری ☐

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 ۱۰۰گیگابیت‌درثانیه رسیده است. از طرفی با متنوع شدن 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 یک تهدید جدی به حساب می‌آیند، افزایش پیدا کرده‌است. سیستم‌های تشخیص نفوذ علیرغم اینکه نقش مهمی در شناسایی آسیب‌ها دارند، اما در ترافیک‌ها و با جریان‌هایی نرخ گذردهی بالا به درستی نمی‌توانند ترافیک را پایش[1] و حملات را تشخیص دهند[۱].

در دهه‌های گذشته، محققان روش‌های شناسایی بسیاری را برای حملات منع‌خدمت توزیع‌شده پیشنهاد کرده‌اند. بیشتر روش‌های موجود مبتنی بر یادگیری ماشینی یا یادگیری عمیق هستند ولی 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[۲]. راهکار ارائه شده توسط شی و چنگ[۲] با استفاده از ویژگی نامتقارن ترافیک‌های غیر عادی را تشخیص می‌دهد. ضعف این راهکار این است که با تغییر رفتار ترافیک شبکه باید به صورت دستی سایز جداول استفاده شده را تعیین کرد. همچنین با استفاده از ویژگی نامتقارن میتوان تنها حملات منع خدمت کمی را تشخیص داد. روش ارائه شده توسط مونیال و وارگزی[۱] نیز مبتنی بر شبکه‌های نرم‌افزارمحور هست که امکان ارتقای آن و استفاده در شبکه‌های با نرخ گذردهی بالا وجود ندارد. همچنین عدم سازگارپذیری مقدار آستانه 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[۳] مبتنی بر سوییچ‌های برنامه‌پذیر توسط ژانگ 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. لذا برای شناسایی صحیح حملات منع خدمت در شبکه های پهن باند نیاز به یک رویکرد و روشی است که شامل دو ویژگی پردازش جامع به معنای پردازش تمامی بسته‌ها و سازگارپذیری به معنای قابلیت تطبیق پذیری با ترافیک متغیر باشد[۴].

در این پایان نامه قصد داریم روشی بهینه و تطبیق‌پذیر برای شناسایی حملات منع خدمت توزیع شده 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 معیارهای 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-تطبیق پذیری ۴-DPDK ۵-سامانه‌های تشخیص نفوذ

[1] monitor

[2] Packet sampling

بسمه تعالی

دانشکده مهندسی کامپیوتر

فرم تعریف پروژه کارشناسی ارشد

تاریخ: .....

شماره:.....

پیوست: .....

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 دیتا	۱ (ماه)
۴.	پیاده سازی و ارزیابی روش	۵ (ماه)
۵.	نگارش پایان نامه	۲ (ماه)
۶.		
۷.		
۸.		
۹.		
۱۰.		

الف) مراجع:

[۱] Varghese, J. E., & Muniyal, B. (2021). An Efficient IDS framework for DDoS attacks in SDN environment. *IEEE Access*, *9*, 69680-69699.

[۲] 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*.

[۳] 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)*.

[٤] Noferesti, M., & Jalili, R. (2020). ACoPE: An adaptive semi-supervised learning approach for complex-policy enforcement in high-bandwidth networks. Computer Networks, 166, 106943.

[۵] 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.

[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).

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:	نظر کمیته تحصیلات تکمیلی دانشکده: تاریخ جلسه کمیته:

بسمه تعالی

دانشکده مهندسی کامپیوتر

تاریخ: .....

شماره:.....

پیوست: .....

فرم تعریف پروژه کارشناسی ارشد

دانشگاه صنعتی شریف

	امضای مدیر گروه:	امضای معاون تحصیلات تکمیلی:

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