بسمه تعالی

دانشکده مهندسی کامپیوتر

تاریخ: .....
شماره:.....
پیوست: .....

فرم تعریف پروژه کارشناسی ارشد

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 Variety Characteristic of High-Bandwidth Networks for Distributed Denial of Service Attacks Detection

نوع پروژه: کاربردی ✓ نظری ✓

باتوجه 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 ۱۰۰ گیگابیت در ثانیه رسیده است. بسیاری از برنامه‌های کاربردی امروزی از پروتکل‌های یکسان و مشترکی برای تبادل اطلاعات استفاده می‌کنند. برنامه‌های پیام‌رسان و مرورگرهای وب از بسته‌های مبتنی بر پروتکل HTTP برای تبادل اطلاعات استفاده می‌کنند، با این تفاوت که در برنامه‌های پیام‌رسان با ارسال تعداد معینی از بسته‌های HTTP در مقایسه با مرورگرهای اینترنتی، نرخ متفاوتی از بسته‌ها را در پاسخ دریافت خواهیم کرد. لذا با ظهور برنامه‌های کاربردی مختلف شاهد بروز تنوع ترافیکی بر روی پروتکل‌های مختلف و رفتارهای متفاوت در ترافیک شبکه هستیم. با افزایش نرخ ترافیک، چالش‌های امنیتی نظیر تشخیص حملات منع خدمت، که به دلیل سادگی در پیاده‌سازی و تاثیر بسیارمخرب یک تهدید جدی به حساب می‌آیند، افزایش پیداکرده‌است. سیستم‌های تشخیص نفوذ در ترافیک‌هایی با نرخ‌گذردهی بالا به‌درستی نمی‌توانند ترافیک را پایش[1] و حملات را تشخیص دهند. در دهه‌های گذشته محققان روش‌های شناسایی بسیاری را برای حملات منع خدمت توزیع‌شده پیشنهاد کرده‌اند. عدم تطبیق پذیری و مقیاس‌پذیری برای استفاده در شبکه‌های پهن‌باند، از متداول‌ترین مشکلات این روش‌ها هستند. به عنوان مثال، روش ارائه شده توسط مونیال و وارگزی مبتنی‌بر شبکه‌های نرم‌افزارمحور می‌باشد که امکان استفاده در شبکه‌های با نرخ گذردهی بالا را ندارد. بررسی تنها نمونه‌هایی از بسته‌ها و درنتیجه پوشش کم شناسایی انواع حملات، از مشکلات روش‌های پیشنهادشده دیگری مانند پوسایدن، که مبتنی بر سوییچ‌های برنامه‌پذیر می‌باشد، هستند. لذا برای شناسایی صحیح حملات منع خدمت در شبکه‌های پهن‌باند نیاز به یک رویکردی است که شامل دو ویژگی پردازش جامع به معنای پردازش تمامی بسته‌ها و تطبیق‌پذیری به معنای قابلیت تطبیق‌پذیری با تنوع ترافیکی باشد.

در این پایان‌نامه قصد داریم رویکردی تطبیق‌پذیر با تنوع ترافیکی موجود در شبکه‌های پهن‌باند برای شناسایی حملات منع خدمت 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 درنظرگرفتن 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

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)

[1] monitor

بسمه تعالی

دانشکده مهندسی کامپیوتر

تاریخ: .....

شماره:.....

پیوست: .....

فرم تعریف پروژه کارشناسی ارشد

۴.	پیاده سازی و ارزیابی روش	۵ (ماه)
۵.	نگارش پایان نامه	۲ (ماه)

الف) مراجع:

[۱] D. Salopek, M. Zec, M. Mikuc, and V. Vasi, "Surgical DDoS Filtering with Fast LPM," *IEEE Access*, vol. 10, pp. 4200–4208, 2022.

[۲] Z. Liu *et al.*, "Jaqen: A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches," *30th USENIX Security Symposium (USENIX Security 21)*,pp. 3829–3846,2021.

[۳] M. Zhang *et al.*, "Poseidon: Mitigating Volumetric DDoS Attacks with Programmable Switches," 27th Network and Distributed System Security Symposium (NDSS 2020), 2020.

[۴] H. Shi, G. Cheng, Y. Hu, F. Wang, and H. Ding, "RT-SAD: Real-Time Sketch-Based Adaptive DDoS Detection for ISP Network," *Security and Communication Networks*, vol. 2021, p. 9409473, 2021.

[۵] Q. Hu, S.-Y. Yu, and M. R. Asghar, "Analyzing Performance Issues of Open-Source Intrusion Detection Systems in High-Speed Networks," *Journal of Information Security and Applications*, vol. 51, p. 102426, 2020.

[۶] J. E. Varghese and B. Muniyal, "An Efficient IDS Framework for DDoS Attacks in SDN Environment," *IEEE Access*,vol. 9, pp. 69680–69699, 2021.

[۷] M. Noferesti and R. Jalili, "ACoPE: An Adaptive Semi-Supervised Learning Approach for Complex-Policy Enforcement in High-Bandwidth Networks," *Computer Networks*, vol. 166, p. 106943, 2020.

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.