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: 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 به بیش از ۱۰۰گیگابیت‌درثانیه رسیده است. همچنین شاهد رفتارهای متفاوت در ترافیک شبکه‌ها هستیم. با افزایش نرخ ترافیک، چالشهای امنیتی نیز افزایش پیداکرده‌است. علاوه‌براین حملات منع‌خدمت به دلیل سادگی در پیاده‌سازی و تاثیر بسیارمخرب یک تهدید جدی به حساب می‌آیند. سیستم‌های تشخیص نفوذ با اینکه نقش مهمی در شناسایی آسیب‌ها دارند، اما در ترافیک‌ها و جریان‌های بالا به درستی نمی‌توانند ترافیک را مانیتور و حملات را تشخیص دهند. به صورت کلی روشهای سنتی به دودسته تقسیم میشوند.دسته اول روش‌های سخت‌افزاری هستند که از میدل‌باکس‌ها بهره می‌گیرند. برای تعریف مکانیزم‌های دفاعی جدید نیاز به ارتقاء دستگاه هست که بایستی هزینه بسیار زیادی متحمل شویم. دسته دیگر روشهای مبتنی بر نرم‌افزار هستند. بااینکه انعطاف‌پذیری بالایی دارند اما تاخیر و سربار زیادی دارند. راهکارهای دیگری که بر مبنای یادگیری ماشین بودند نیز با وقوع حملات جدید، نیاز به اجرای عملیات یاددهی مجدد داشتند که این عملیات نیز مشکلاتی ازقبیل طولانی بودن به همراه داشت. روشهای نوینی در سالیان اخیر ارائه شده‌است. راهکار ارائه شده توسط شی و چنگ[۲] مبتنی بر انگاره‌ها هست. ولی مشکل اینست که با تغییر رفتار ترافیک شبکه باید به صورت دستی سایز جداول انگاره را تعیین کرد. نقطه ضعف دیگر استفاده از ویژگی نامتقارن برای تشخیص ترافیک غیرعادی و حملات هست ونمیتوان با این روش همه انواع حملات منع خدمت را تشخیص داد. روش ارائه شده توسط مونیال و وارگزی[۳] نیز مبتنی بر شبکه‌های نرم‌افزارمحور هست. ولی امکان ارتقای آن و استفاده در محیط‌های بزرگتر هنوز بررسی نشده است. همچنین عدم سازگارپذیری مقدار آستانه الگوریتم استفاده‌شده، عدم شناسایی همه انواع حملات منع‌خدمت و استفاده از تنها یک معیار آماری از دیگر مشکلات آن هستند. راهکار دیگری به نام پوسایدن[۴] مبتنی بر سوییچ‌های برنامه‌پذیر توسط ژانگ ارائه شد. با وجود اینکه به صورت پویا می‌تواند حملات را تشخیص دهد اما مشکلش این است که در هنگام تغییر حملات تمامی راهکارهای دفاعی را به سرورها منتقل می‌کند که درشبکه‌های بزرگ این موضوع می‌تواند باعث بروز تاخیر برای کاربران مجاز شود. لذا نیاز به یک رویکرد و روشی داریم که تغییرات ترافیک شبکه را تشخیص دهد، بتواند خود را با آن تطبیق دهد و مهاجمین را به درستی شناسایی کند. در این مقاله قصد داریم روشی بهینه و تطبیق‌پذیر معرفی نماییم که امکان شناسایی حملات جدید و پویای شبکه را دارد. 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 پهن باند ۳-DPDK ۴- یادگیری تطبیقی ۵- سامانه‌های تشخیص نفوذ

بسمه تعالی

دانشکده مهندسی کامپیوتر

تاریخ: .....

شماره:.....

پیوست: .....

فرم تعریف پروژه کارشناسی ارشد

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

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

[٤] 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)*.

[٥] 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: امضای مدیر گروه:	نظر کمیته تحصیلات تکمیلی دانشکده: تاریخ جلسه کمیته: امضای معاون تحصیلات تکمیلی:

بسمه تعالی

دانشکده مهندسی کامپیوتر

تاریخ: .....

شماره:.....

پیوست: .....

فرم تعریف پروژه کارشناسی ارشد

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