دانشگاه یزد تحصیلات تکمیلی	بسمه تعالی کاربرگ تصویب پیشنهادیه پایان‌نامه دانشجوی دوره کارشناسی ارشد در شورای گروه و دانشکده (ویرایش پاییز ۱۳۹۴)	شناسه: ک/۱ شماره: تاریخ: پیوست:

مشخصات دانشجو :

نام و نام خانوادگي: زهرا همتی شماره دانشجويي: ۹۳۱۸۰۶۴

دوره: نوبت اول ■ نوبت دوم □ پردیس □

رشته/ گرايش تحصيلي: مهندسی فناوری اطلاعات- شبکه‌های کامپیوتری گروه: مهندسی کامپیوتر دانشکده: مهندسی برق و کامپیوتر

- مشخصات پایان نامه:

۱- عنوان :

فارسی : بررسی حملات انکار سرویس توزیع شده در شبکه‌های نرم‌افزار محور و بهبود روشهای کشف آن

انگلیسی: **Distributed Denial of Service Attacks in Software defined networks and improving its detection methods**

نوع پایان نامه: کاربردی■ بنیادی□ توسعه ای■ اولین نیمسال اخذ احد

پایان نامه نیمسال دوم ۹۴-۹۵ تعداد واحد ۶

- مشخصات استادان راهنما و مشاور:[1]

مسئولیت	نام و نام خانوادگی	آخرین مدرک تحصیلی /مرتبه علمی	گروه/دانشکده/ دانشگاه یا موسسه	امضاء
استاد راهنمای اول	کیارش میزانیان	دکتری / استادیار	کامپیوتر/برق و کامپیوتر/یزد	
استاد راهنمای دوم				
استاد مشاور اول	قاسم میرجلیلی	دکتری/استاد	مخابرات/ برق و کامپیوتر/یزد	
استاد مشاور دوم				

این پیشنهادیه در شورای تحصیلات تکمیلی/ شورای گروه ..... به تاریخ ..... مورد بررسی و تصویب قرار گرفت.

در ضمن، ماهیت پایان‌نامه[2]: نظری□ تجربی□ اعلام می‌گردد.

نام و امضای مدیر گروه

این پیشنهادیه در شورای تحصیلات تکمیلی دانشکده ..... به تاریخ ..... مورد بررسی و تصویب قرار گرفت و اطلاعات مربوط به آن در سامانه پژوهشگاه علوم و فنآوری اطلاعات ایران ثبت و تایید شده است.

نام و امضای رئیس / معاون آموزشی دانشکده

اصل پیشنهادیه تایید شده باید به اداره تحصیلات تکمیلی دانشگاه ارسال و تصویر آن توسط دانشجو به استادان راهنما و مشاور تحویل داده شود.

---

[1] امضای استادان راهنما و مشاور الزامی است و امضای "از طرف" پذیرفته نمی‌شود. درصورتی که هریک ازاستادان یاد شده عضو هیات علمی دانشگاه یزد نباشند، ضمن درج نشانی و شماره تلفن آنان، آخرین حکم کارگزینی آن‌ها ضمیمه گردد.

[2] پایان‌نامه‌هایی که انجام آنها مستلزم تامین لوازم و مواد مصرفي و هزینه خدمات آزمایشگاهی و میدانی (مانند نمونه‌برداری و انجام آزمایشات) است، تجربي محسوب مي‌شوند. هزینه انجام کلیه اموري که جزء وظایف دانشجو محسوب مي‌شود و لوازم مصرفي که تأمین آنها معمولاً براي تمام دانشجویان تحصیلات تکمیلي ضرورت پیدا مي‌کند (نظیر تهیه مقاله یا کتاب، نرم افزار، داده یا تکمیل پرسشنامه و ...) ملاک تجربي بودن پایان‌نامه نیست.

۲- شرح پایان‌نامه:

الف) تعریف موضوع (تعریف مسئله، هدف از اجرا و کاربرد نتایج تحقیق):

شبکه نرم‌افزار محور (SDN) یک معماری جدید برای شبکه است که با جداکردن بخش انتقال داده از بخش کنترلی، یک سیستم کنترل مرکزی را برای شبکه فراهم می‌کند. ایده اصلی شبکه‌های نرم‌افزار محور، ارائه یک روش جدید برای مدیریت شبکه است. در شبکه‌های نرم‌افزار محور، سوییچ‌ها پردازش بسته‌های رسیده را انجام نمی‌دهند. هر سوییچ، یک جدول پیشرانی دارد که با توجه به آن بسته‌های رسیده را به جلو می‌فرستد و اگر هیچ تطبیقی برای بسته در جدول خود نیافت آن بسته را به کنترلر می‌فرستد. کنترلر، سیستم عامل این معماری است و بسته را پردازش می‌کند و تصمیم می‌گیرد که جریان داده مربوطه بایستی به کجا ارسال شود، سپس این تصمیم را در قالب جدول پیشرانی به سوییچ می‌فرستد. به‌وسیله این رویه، در شبکه‌های نرم‌افزار محور، عملیات پیشرانی بسته و پردازش بسته تفکیک می‌شود..[۱]

معماری شبکه‌های نرم‌افزار محور می‌تواند شامل چندین کنترلر باشد که هرکدام به سوییچ‌ها و روترها متصل هستند. اگر ارتباط بین کنترلر و سوییچ‌ها از دست برود و یا کنترلر دچار مشکل نرم‌افزاری یا سخت‌افزاری شود، بدان معناست که محل کنترل شبکه و پردازش بسته‌ها غیرقابل دسترسی می‌شود. در این صورت، پردازش بسته‌ها انجام نمی‌شود و عملاً با از بین رفتن کنترلر، معماری شبکه‌های نرم‌افزار محور از بین می‌رود.[۱][۲]

یکی از مواردی که کنترلر را غیرقابل دسترس می‌کند، حملات انکار سرویس توزیع شده (DDoS) است. در حمله انکار سرویس توزیع شده، تعداد زیادی بسته به میزبان یا میزبان‌ها فرستاده می‌شود. از آنجایی که آدرس این بسته‌ها جعلی هست سوییچ نمی‌تواند هیچ تطبیقی در جدول پیشرانی بیابد و آن بسته‌ها را به کنترلر می‌فرستد. جمع‌آوری بسته‌های واقعی و بسته‌های جعلی ناشی از حملات انکار سرویس توزیع شده و پردازش آن‌ها کنترلر را دچار ازدحام شدید کرده و برای دیگر بسته‌هایی که در صف منتظرند غیرقابل دسترس می‌کند.[۳]

در این تحقیق به مطالعه و بررسی شبکه‌های نرم‌افزار محور و تأثیر حملات انکار سرویس بر آن می‌پردازیم تا نقطه‌ضعف اصلی این شبکه را در برابر حملات انکار سرویس توزیع شده بیابیم. تمرکز اصلی روی کنترلر است. برای محافظت از کنترلر، اولین و مهم‌ترین راهکار، کشف حملات احتمالی است. بر این اساس، در این پایان‌نامه، روش‌های مختلف کشف حملات انکار سرویس توزیع شده را بررسی نموده و سعی خواهیم کرد تا به ارائه روشی جدید جهت کشف حملات انکار سرویس توزیع شده و یا بهبود روش‌های موجود بپردازیم.

ب) سابقه تحقیق:

پژوهش‌های انجام شده در زمینه حملات انکار سرویس توزیع شده در شبکه‌های نرم‌افزار محور اکثراً در سال‌های اخیر بوده است. در ادامه تعدادی از این پژوهش‌ها به اختصار شرح داده شده می‌شود.

در [۴]، به بررسی شبکه‌هایSDN و به‌طور خاص استفاده از پروتکل OpenFlow به‌عنوان وسیله‌ای برای کاهش خطرات حمله در حملات انکار سرویس توزیع شده پرداخته شده است. در این مقاله به‌وسیله OpenFlow و کنترل ترافیک شبکه سعی شده است تا عنصری که مورد حمله قرار گرفته است بتواند رفتار طبیعی برای بقیه بسته‌ها داشته باشد.

با طبقه‌بندی حملات انکار سرویس توزیع شده می‌توان آن‌ها را بهتر مدیریت و کشف کرد. در .[۵]، نویسندگان با استفاده از SVM به طبقه‌بندی و تجزیه‌وتحلیل این‌گونه حملات در شبکه‌های نرم‌افزار محور پرداخته‌اند. SVM به‌طور گسترده طبقه‌بندی را با دقت بالا و نرخ خطای مثبت کمتر انجام می‌دهد. آزمایش‌ها نشان می‌دهد که SVM در انجام طبقه‌بندی از ابزارهای دیگر دقیق‌تر است. با طبقه‌بندی این حملات می‌توان نحوه مقابله و کشف آن را بهتر درک کرد.

در[٦] ، راهکارهای ایمن نگه‌داشتن شبکه‌های نرم‌افزار محور در برابر حملات انکار سرویس توزیع شده به‌وسیله اجرای چندین نرم‌افزار ارائه شده است. به‌طور خاص، یک برنامه کاربردی شرح داده می‌شود که می‌تواند در شبکه‌های نرم‌افزار محور با رابط کنترلی openflow ، حملات انکار سرویس توزیع شده را بلاک کند.
در [۷]، یک مکانیسم برای شبکه‌های SDN بر اساس CDNi با یک استراتژی چند دفاع در برابر حملات انکار سرویس توزیع شده پیشنهاد شده است. همچنین مرجع [۸] در این رابطه، به بیان تجزیه‌وتحلیل SDN با پروتکل OpenFlow از منظر حملات انکار سرویس توزیع شده می‌پردازد. در این مرجع، نحوه استفاده از امکانات فعلی و جدید برای تحقق، تشخیص و کاهش حملات انکار سرویس توزیع شده شرح داده شده است و نشان می‌دهد تکنیک‌های مبتنی بر یادگیری ماشین برای کاهش چنین حملاتی تأثیرگذار هستند.
محاسبات ابری یک روند مقرون به صرفه و مقیاس‌پذیر را برای ارائه خدمات فناوری اطلاعات فراهم ساخته است. از آن‌سو SDN نیز به دلیل انعطاف‌پذیری که در خدمات مدیریت شبکه دارد مورد توجه قرار گرفته است و به نظر می‌رسد ادغام این دو تکنولوژی گرچه خدمات بسیاری را برای سازمان‌ها فراهم می‌آورد، اما با چالش‌هایی به‌خصوص در حوزه امنیت رو برو می‌شود. مرجع [۹] به بررسی این مشکل مهم پرداخته است. ابتدا به تأثیر مسائل امنیتی، به‌ویژه تأثیر حملات انکار سرویس توزیع شده و مکانیسم‌های دفاعی، در شبکه‌هایی که در آن هر دو تکنولوژی استفاده شده است، می‌پردازد. سپس یک معماری برای کاهش حمله انکار سرویس توزیع شده پیشنهاد شده است که این معماری منجر به حبس مؤثر حمله و حفاظت از شبکه در طول حملات انکار سرویس توزیع شده می‌شود.
مرجع[۹] نیز به بحث درباره روند و ویژگی‌های حملات انکار سرویس توزیع شده در محاسبات ابری، و ارائه یک بررسی جامع از مکانیسم‌های دفاعی در برابر حملات انکار سرویس توزیع شده با استفاده از مزایای SDN در محیط‌های محاسبات ابری پرداخته است. در اینجا از قابلیت‌های SDN، از جمله تجزیه‌وتحلیل ترافیک مبتنی بر نرم‌افزار ، کنترل متمرکز، دیدگاه کلی از شبکه، به‌روزرسانی پویای قوانین پیشرانی، برای تشخیص و واکنش به حملات انکار سرویس توزیع شده استفاده شده است.

ج) کلمات کلیدی:
فارسی:

حملات انکار سرویس توزیع‌شده ، شبکه‌های نرم‌افزار محور، بهبود روش های کشف،

انگلیسی:

Distributed Denial of Services (DDoS), Software-defined networking, Improving its Detection Methods,

د) فرضیات (یا سئوالات پژوهشی):
۱- تاثیر حملات انکار سرویس توزیع شده در شبکه‌های نرم‌افزار محور چگونه است؟
۲- چگونه می توان بطور موثر، حملات انکار سرویس توزیع شده را در شبکه‌های نرم‌افزار محور کشف کرد؟
۳-چه راهکاری برای بهبود عملکرد کنترلرها در شبکه های نرم افزار محور در هنگام وقوع حملات انکار سرویس توزیع شده وجود دارد؟

هـ) روش تحقیق (مخصوص دانشکده‌های علوم انسانی، منابع طبیعی و هنر و معماری):

و) مراحل اجرای پروژه و زمان بندی:

زمانبندی / مراحل اجرا	دی ۹۴	بهمن ۹۴	اسفند ۹۴	فروردین ۹۵	اردیبهشت ۹۵	خرداد ۹۵	تیر ۹۵	مرداد ۹۵	شهریور ۹۵
جستجوی منابع و مطالعات اولیه									
بررسی پژوهش‌های مشابه									
طراحی، اجرا، شبیه سازی و بررسی نتایج									
جمع‌بندی و نگارش پایان‌نامه									

ز) فهرست منابع ومآخذ:

[1]Mousavi, S. M., “Early Detection of DDoS Attacks in Software Defined Networks Controller”, M.S. thesis, Carleton. Univ, Ottawa, Ontario, Canada, 2014

[2]Ashraf, J.; Latif, S., "Handling intrusion and DDoS attacks in Software Defined Networks using machine learning techniques," *in Software Engineering Conference (NSEC), 2014* National ,pp.55-60, 11-12 Nov. 2014

[3]Mousavi, S.M.; St-Hilaire, M., "Early detection of DDoS attacks against SDN controllers," in *Computing, Networking and Communications (ICNC), 2015 International Conference on* ,pp.77-81, 16-19 Feb. 2015

[4]Giotis, K.; Androulidakis, G.; Maglaris, V., "Leveraging SDN for Efficient Anomaly Detection and Mitigation on Legacy Networks," in *Software Defined Networks (EWSDN), 2014 Third European Workshop on* ,pp.85-90, 1-3 Sept. 2014

[5]Kokila, R.T.; Thamarai Selvi, S.; Govindarajan, K., "DDoS detection and analysis in SDN-based environment using support vector machine classifier," *in Advanced Computing (ICoAC), 2014 Sixth International Conference on* , pp.205-210, 17-19 Dec. 2014

[6] Lim, S.; Ha, J.; Kim, H.; Kim, Y.; Yang, S., "A SDN-oriented DDoS blocking scheme for botnet-based attacks," *in Ubiquitous and Future Networks (ICUFN), 2014 Sixth International Conf on* ,pp.63-68, 8-11 July 2014

[7]Mowla, N.I.; Inshil Doh; Kijoon Chae, "Multi-defense Mechanism against DDoS in SDN Based CDNi," *in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS),* 2014 Eighth International Conference on , pp.447-451, 2-4 July 2014

[8]Vizváry, M.; Vykopal, J.,” Monitoring and Securing Virtualized Networks and Services,” Vol. 8508, 2014, PP.123-127

[9]Wang, B.; Zheng, Y.; Lou, W.; Hou, Y.TH, “DDoS attack protection in the era of cloud computing and Software-Defined Networking,” *Computer Networks*, Vol. 81, 22 April 2015, PP. 308-319

[10]Yan, Q.; Yu, R.; Gong, Q.; Li, J., "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges," in *Communications Surveys & Tutorials, IEEE* , no.99 ,2015

۳- مواد، وسایل و دستگاه‌های مورد نیاز و منبع تأمین:

نام ماده یا دستگاه
محل تامین

٤- تعهد نامه دانشجو:*
اینجانب زهرا همتی متعهد می‌شوم که با توجه به مفاد این پیشنهادیه به طور تمام وقت، زیر نظر استادان راهنما و مشاور انجام وظیفه نمایم. در ضمن «**تعهد رعایت حقوق معنوی دانشگاه یزد**» را مطالعه نموده و با اطلاع از اینکه شرط فارغ‌التحصیلی اینجانب پایبندی شرعی و قانونی به رعایت حقوق معنوی مذکور است و باید تعهدنامه امضاء شده را همراه پایان نامه صحافی نمایم، اقدام به انجام پیشنهادیه تصویب شده خواهم کرد.
.

تاریخ و امضای دانشجو