AN ELAPSED-TIME BASED SCHEME FOR DETECTING AND MITIGATING DDOS ATTACKS IN THE SDN ENVIRONMENT

WISAM H A. MURAGAA

UNIVERSITI SAINS ISLAM MALAYSIA

AN ELAPSED-TIME BASED SCHEME FOR DETECTING AND MITIGATING DDOS ATTACKS IN THE SDN ENVIRONMENT

Wisam H A. Muragaa

Thesis submitted in fulfillment for the degree of
DOCTOR OF PHILOSOPHY IN
ENGINEERING AND BUILT ENVIRONMENT

UNIVERSITI SAINS ISLAM MALAYSIA

July 2019

AUTHOR DECLARATION

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيمِ

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged

Date :

Signature

Name : Wisam H A Muragaa
Matric No : 4130037
Address: No3. JLN Taman Universiti Bangi 5, Kajang, 43000, Selangor, Malaysia.

ACKNOWLEDGEMENTS

First and foremost, I would like to thank the "**Almighty ALLAH**" for giving me the strength, knowledge, ability and opportunity to undertake this research study and to persevere and complete it satisfactorily. Without his blessings, this achievement would not have been possible.

I have great pleasure in acknowledging my gratitude to my supervisor **Prof. Dr. Kamruzzaman Seman**. He has been there providing his guidance and support at all times and has given me invaluable suggestions in my quest for knowledge. He has given me all the freedom to pursue my research, while silently and non-obtrusively ensuring that I stay on course and do not deviate from the core of my research. Without his able guidance, this thesis would not have been possible and I shall eternally be grateful to him for his assistance. I would like to express my gratitude to **Dr. Mohd Fadzli Marhusin** the co-supervisor. I would also like to express my gratitude to **Prof. Madya Dr. Nurlida Binti Basir** for her guidance and support.

My acknowledgment would be incomplete without thanking the biggest source of my strength, my family. My parents, whose love and guidance are with me in whatever I pursue. My prime sources of ideas my loving and supportive wife and my three wonderful children who provide unending inspiration. All these important people have contributed significantly to helping me reach this important stage in my life.

ABSTRAK

Sepanjang dekad yang lalu, serangan Pengedaran Penafian Perkhidmatan (DDoS) menjadi salah satu isu keselamatan Internet utama dan senjata pilihan untuk penggodam, pemeras siber, dan pengganas siber. Serangan DDoS mengganggu atau merendahkan perkhidmatan rangkaian (dengan mengurangkan kekurangan jalur lebar rangkaian atau kapasiti pemprosesan penghala) atau sumber mangsa (dengan melumpuhkan lebar jalur cakera atau pangkalan data, deskriptor fail, buffer, soket, kitaran CPU, memori) dan menghentikan pengguna yang sah daripada mengakses perkhidmatan Internet tertentu. Serangan tersebut memberi kesan kepada sumber-sumber mangsa supaya tidak dapat memberi respons kepada perkhidmatan yang diminta oleh pengguna yang disahkan. Di tengah meningkatkan bilangan serangan DDoS dan keupayaan penyerang untuk membangunkan jenis serangan untuk menembusi kaedah perlindungan tradisional, Perangkaian yang ditakrifkan perisian (SDN) telah muncul sebagai persekitaran alternatif untuk meminimumkan kerosakan serangan ini. Membolehkan kawalan rangkaian untuk diprogram secara langsung dan infrastruktur yang mendasar untuk diguna untuk aplikasi dan perkhidmatan rangkaian menjadikan rangkaian lebih fleksibel dan tangkas. Rangkaian yang ditakrifkan perisian merupakan model rangkaian baru yang menarik perhatian ramai penyelidik dalam isu keselamatan rangkaian hari ini. Pengesanan serangan DDoS menjadi lebih mudah jika kita dapat memanfaatkan ciri-ciri khas SDN seperti pemantauan kawalan ke atas infrastruktur, menanggalkan satah kawalan dari pesawat data dan konsep lalu lintas berasaskan aliran. Dalam kajian ini, kami menggunakan pengawal SDN untuk mengesan dan mengurangkan serangan DDoS. Penyelesaian pengesanan DDoS berasaskan SDN yang telah dicadangkan adalah pelbagai tetapi mengalami kemerosotan prestasi terutamanya, penyelesaian berasaskan pembelajaran mesin dan penyelesaian berasaskan entropi. Penyelesaian pengesanan DDoS berdasarkan teknik pembelajaran Mesin dan teknik entropi di SDN menderita sama ada meningkatkan penggunaan CPU atau meningkatkan penggera palsu. Degradasi prestasi dalam penyelesaian yang sedia ada disebabkan oleh kerumitan teknik yang digunakan untuk mengesan serangan DDoS di SDN serta parameter yang digunakan oleh teknik ini untuk membezakan paket DDoS. Penyelesaian yang ada tidak menganggap masa berlalu antara paket serangan berturut-turut sebagai parameter utama dalam mengesan serangan DDoS di SDN sebagai contoh. Selain itu, penyelesaian yang sedia ada hanya memberi tumpuan kepada mengesan serangan DDoS yang banjir dan gagal mencadangkan penyelesaian pertahanan yang dapat mengesan serangan DDoS yang berubah dari volum tinggi ke jumlah yang rendah pada masa serangan itu. Juga, beberapa penyelesaian dianggap sebagai pengesanan serangan DDoS kadar rendah di SDN. Dalam kajian ini, kami mencadangkan skim berasaskan masa yang berlalu, skim yang berkesan dan cekap untuk mengesan dan mengurangkan serangan banjir dan serangan kadar rendah di SDN. Skim berasaskan masa yang berlalu dilaksanakan pada pengawal POX dan dinilai berdasarkan senario serangan yang berbeza. Keputusan eksperimen mengesahkan bahawa, dibandingkan dengan penyelesaian berasaskan pembelajaran mesin yang berbeza dan penyelesaian berasaskan entropi yang disebut dalam penyelidikan ini, skim berasaskan masa yang berlaku mengurangkan overhead sehingga 50%, sambil memastikan 0% penggera palsu dan lebih dari 99.20% ketepatannya.

ABSTRACT

Over the last decade, Distributed Denial of Service (DDoS) attacks became one of the main Internet security issues and the weapon of choice for hackers, cyber extortionists, and cyber terrorists. A DDoS attack disrupts or degrades the network services (by depleting the network bandwidth or router processing capacity) or victim resources (by exhausting disk or database bandwidth, file descriptors, buffers, sockets, CPU cycles, memory) and stops the legitimate user from accessing a specific Internet service. Such attacks hog the victim's resources so that it cannot respond to the services requested by an authenticated user. Amid raising the number of DDoS attacks and the attackers' ability to develop attack types to penetrate traditional protection methods, Software-defined networks has emerged as an alternative environment to minimize the damage of this attack. Enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services make the network more flexible and agile. SDN is an emerging network model that attracted the attention of many researchers in today's networks security issues. The detection of DDoS attacks becomes much easier if we are able to take advantage of the SDN distinct characteristics such as the centralization of control over the infrastructure, decoupling of the control plane from the data plane and the flow-based traffic concept. In this research, we utilize the SDN controller to detect and mitigate DDoS attacks. The SDN-based DDoS detection solutions that have been proposed are various but suffer from performance degradation particularly, machine learning-based solutions and entropy-based solutions. DDoS detection solutions based on Machine learning techniques and entropy techniques in SDN suffer from either increase the CPU usage or increase false alarms. The performance degradation in the existing solutions is caused by the complexity of the techniques used to detect the DDoS attacks in SDN as well as the parameters used by these techniques to distinguish DDoS packets. The existing solutions do not consider the elapsed time between the successive attack packets as a key parameter in detecting DDoS attacks in SDN as an example. Furthermore, the existing solutions are only focused on detecting the flooding DDoS attacks and failed to propose a defense solution can detect the DDoS attacks that change from the high volume to the low volume at the time of the attack. Also, few solutions considered low-rate DDoS attacks detection in SDN. In this research, we propose an elapsed-time based scheme, an effective and efficient scheme to detect and mitigate flooding attacks and low-rate attacks in SDN. Elapsed-time based scheme is implemented on POX controller and evaluated under different attack scenarios. The experimental results confirm that, compared to different machine learning-based solution and entropy-based solutions mentioned in this research, elapsed-time based scheme reduces the overhead up to 50%, while ensuring 0% of false alarms and to more than 99.20% of the accuracy.

ملخص

خلال العقد الماضي ، أصبحت هجمات "رفض الخدمة الموزعة" (DDoS) واحدة من أهم مشكلات أمان الإنترنت والسلاح المفضل للمتسللين وابتزاز الإنترنت والإرهابيين عبر الإنترنت. يؤدي هجوم DDoS إلى تعطيل خدمات الشبكة أو تدهورها (عن طريق استنفاد عرض النطاق الترددي للشبكة أو سعة معالجة جهاز التوجيه) أو موارد الضحية (من خلال استنفاد عرض النطاق الترددي للقرص أو قاعدة البيانات أو واصفات الملفات أو المخازن المؤقتة أو المقابس أو دورات CPU أو الذاكرة) ويمنع المستخدم الشرعي من الوصول خدمة إنترنت محددة. تؤدي هذه الهجمات إلى خنق موارد الضحية بحيث لا يمكنها الاستجابة للخدمات التي يطلبها مستخدم معتمد. وسط زيادة عدد هجمات DDoS وقدرة المهاجمين على تطوير أنواع الهجمات لاختراق أساليب الحماية التقليدية ، برزت SDN كبيئة بديلة لتقليل الضرر الناجم عن هذا الهجوم. تمكين التحكم في الشبكة لتصبح قابلة للبرمجة مباشرة والبنية التحتية الأساسية ليتم استخراجها للتطبيقات وخدمات الشبكة جعل الشبكة أكثر مرونة وخفة الحركة. الشبكات المعرفة بالبرمجيات هي نموذج شبكة ناشئ جذب انتباه العديد من الباحثين في قضايا أمن الشبكات الحالية. يصبح اكتشاف هجمات DDoS أسهل بكثير إذا تمكنا من الاستفادة من الخصائص المميزة لشبكة SDN مثل مركزية التحكم في البنية التحتية وفصل مستوى التحكم عن مستوى البيانات ومفهوم حركة المرور المستند إلى التدفق. في هذا البحث ، نستخدم وحدة تحكم SDN للكشف عن هجمات DDoS وتخفيفها. تعد حلول الكشف عن DDoS المستندة إلى SDN مختلفة ، ولكنها تعاني من تدهور الأداء خاصة ، والحلول المستندة إلى تعلم الآلة والحلول المستندة إلى الإنتروبي. تعاني حلول اكتشاف DDoS المستندة إلى تقنيات التعلم الآلي وتقنيات الإنتروبيا في SDN من زيادة استخدام وحدة المعالجة المركزية أو زيادة الإنذارات الخاطئة. سبب تدهور الأداء في الحلول الحالية هو تعقيد التقنيات المستخدمة للكشف عن هجمات DDoS في SDN وكذلك المعلمات المستخدمة من قبل هذه التقنيات لتمييز حزم DDoS. لا تعتبر الحلول الحالية الوقت المنقضي بين حزم الهجوم المتتالية كمعلمة رئيسية في اكتشاف هجمات DDoS في SDN كمثال. علاوة على ذلك ، تركز الحلول الحالية فقط على اكتشاف هجمات DDoS الفيضانات وفشلت في اقتراح حل دفاعي يمكنها اكتشاف هجمات DDoS التي تتغير من الحجم الكبير إلى الحجم المنخفض في وقت الهجوم. أيضًا ، هناك حلول قليلة تعتبر اكتشاف هجمات DDoS ذات المعدل المنخفض في SDN. في هذا البحث ، نقترح خطة قائمة على الوقت المنقضي ، ونظام فعال وفعال لاكتشاف وتخفيف هجمات الفيضانات والهجمات ذات المعدل المنخفض في SDN. يتم تطبيق مخطط الوقت المنقضي على وحدة تحكم POX وتقييمه وفقًا لسيناريوهات الهجوم المختلفة. تؤكد النتائج التجريبية أنه بالمقارنة مع الحلول المستندة إلى تعلم الآلة المختلفة والحلول المستندة إلى الإنتروبيا المذكورة في هذا البحث ، فإن المخطط الزمني المستغرق يقلل من النفقات العامة بنسبة تصل إلى 50 ٪ ، مع ضمان 0 ٪ من الإنذارات الكاذبة وأكثر من 99.20 ٪ من الدقة.

TABLE OF CONTENTS

LIST OF TABLES

Tables **Page**

LIST OF FIGURES