Software defined networking

To investigate Traceback of DOS attacks through Packet Marking on SDN Controllers

Research Proposal

Group name: W04_G03

Members: [redacted]

Abstract

Current technology experts are concerned with the threats posed by the Denial of Service (DoS) and Distributed Denial-of-service (DDoS). Today's internet is more vulnerable to these threats that any other time in the history of the internet. It has been established that internet experts find it difficult to address these threats for the attackers often use fake or hidden IP addresses as the source IP address. As such, it is difficult to determine the origin of the attack. However, Packet Marking Techniques have been proven to be effective in addressing this problem by tracing back the DDOS. Probabilistic packet marking algorithm (PPM) [1], allows the victim to trace back the origin of the attackers regardless of problem with hidden IP address or spoofed IP addresses. In this paper, we propose a novel technique of implementing packet marking on SDN controllers, to find out how efficient, and practical this new approach can bring into the SDN network. In theory, this method would be more feasible compare to other approach since it does not cause any overhead or additional content on the IP packet. It actually just modified an "Identification" field of the header of IP packets. It also would be much more practical to apply this solution on SDN hence the number of nodes of SDN in the internet is very much smaller than the number of routers. In order to justify these judgment, an experiment setup will be implemented on Amazon Web Service (AWS) to perform the test. The design of the network testbed will include a number of SDN nodes to meet the complexity of the orchestration of the internet. The structure of a typical SDN will also be implemented. Finally, the goal of this research will be achieved through the tests of the network, controller in terms of performance in this experiment.

I. INTRODUCTION

DDoS attacks cripple institutions' operational ability by inhibiting the seamless flow of information, impairing different activities or totally stopping operations. What makes the problem even more difficult to solve is the fact that DDoS tools are easy to get and use. As such, even an amateur hacker can launch attacks effortlessly [2]. Moreover, it is close to impossible to separate the attack from legitimate traffic. The accurate separation of attack traffic from legitimate traffic can protect users from using corrupt data for personal tasks. The only drawback of this technique is that DDoS attackers often use fake or

hidden IP addresses. For this reason, the attackers can easily hide their identity and present themselves as other hosts. Most importantly, the stateless nature of the World Wide Web makes it even more difficult to trace the origin of attacks and the attackers. This is commonly referred to as the IP traceback challenge is commonly.

Packet marking can be separated into two parts. On the one hand is the deterministic packet marking whilst on the other hand is the probabilistic packet marking [1]. These techniques are used to mark a boundary router's IP address on the moving information packets. Packet marking has been successfully used in non-SDN networks but with demand for greater scalability, performance and reduced administration overhead in carrier grade networks the SDN technology has been advanced to enhance network configuration and management. Security is a key factor for effective deployment of SDN and in this research we set out to test packet marking technique on SDN controllers. This paper gives the aim of the research in Section II and III, a background review of previous works in Section IV. A detail research plan is given in Section V giving the proposed methodology, design of the experiment and our data validation and analysis. Ethical considerations guiding our research are highlighted in Section VI.

II. AIM OF THE RESEARCH

To investigate Traceback of DOS attacks through Packet Marking on SDN Controllers

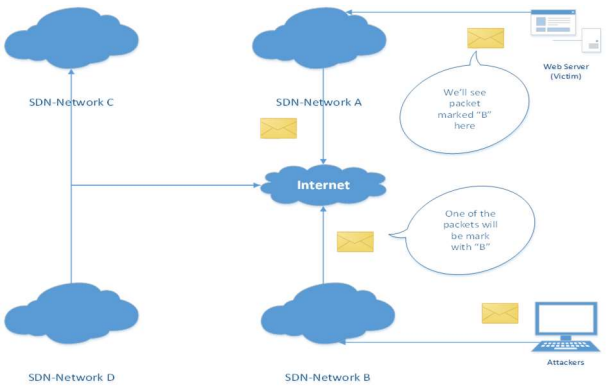

Fig 1. Marking packet technique.

In our research we seek to investigate whether it is possible to mark a packet from a controller in one SDN network and identify the packet through the label from a different network. If we are able to find label "B" as show in Figure 1 above in SDN Network "C" then we are able to confirm that the packet actually passed through a node in SDN Network B, regardless of how attackers use different techniques to hide their identity and location. Packet marking on SDN controllers in a novel technology that we set out to implement and contrast against various state of the art technologies.

III. Research Questions

In our research we seek to identify: -

1. How effective is packet marking when used as a Traceback technique on SDN controllers?
2. How reliable is controller-based marking in comparison to mac-address tracing?

Packet marking has been successfully used for traceback techniques in non-SDN networks. In this study we seek to test the technique in an SDN environment through marking of packets on the controllers. We seek also to contrast the reliability of the techniques previously used to traceback attackers like mac-address tracing and identify what are some of the significant advantages or drawbacks.

IV. BACKGROUND AND LITERATURE REVIEW

There were a substantial number of findings which focused on mitigation of DoS attacks in SDN networks recently. Some of them were working on how to prevent DoS attacks on the controller. Some others focused on the TCAM table of the switches to prevent attackers to overwhelm the table's capacity. However, the common result of those studies was that they all tried to drop the malicious packets inside the

SDN network or right before they come to the network.

For example, the author [3] stated that, the traceback of the packets can be done at the SDN controller hence the controller has knowledge of the entire network. As a result, it can easily detect an attack in the network and drop the packets right at the location of the intruders.

The limitation of this finding would be that the outcome of these approach was not effective since it handles the DoS attack inside its SDN network only. Therefore, when the attacks come from outside of the network, it would be too late to mitigate the attacks since they may already consume all the bandwidth of the network.

There was also another trend of findings in this area in which their approach was trying to prevent the DoS attacks from outside of the network. For instance, in [4] the authors claimed that the intruder can be detected by using MAC binding technique. The idea of this approach can bring a practical solution to mitigation of DoS attacks since most malicious traffic will be drop right at the attacker's location. However, this method may lead to two problems for the SDN network

The first problem with this approach is their assumption, in which IP packets will carry the MAC address of all the end devices that never happen. The reason is that the length of the MAC address is 32 bits, therefore, doing so could significantly cause over head to the IP traffic, reduce the performance of the entire internet.

The other possible issue would be that, by using a MAC binding table, it may become a new target of DoS. For instance, attacker can keep sending fake MAC address to the SDN, overwhelm the MAC binding table, resulting in denial of service, or DoS attack.

In this paper, the second approach will be proposed to overcome the issue with the first approach. The packet marking technique will also being applied to have more efficiency on the performance of the traceback and will be represented in the following sections.

For a start, the probabilistic packet marking [3] is that, every single node of the network may randomly decide to mark a packet. Then, when a DoS attack happen with a great number of malicious packets, the probability of receiving enough marked packet at the victim, can lead to the successful traceback of the attack anywhere outside of the network.

Next, contrast to other approaches, this approach also only uses the currently reserved field of the IP packet, the field namely Identification with 16 bits, therefore, does not cause any overhead to the packets. As a result, it will not affect the performance of the internet in general.

In short, this technique allows network administrators to locate the potential attackers' path as some of the malicious packets will be marked with a controller's ID somewhere on the way they get to the target [1]. Then, from the SDN's API interface, engineers can apply Access Control List to filter those packets as near the attackers as possible.

V. RESEACH PLAN

A. Methodology

In the networking field, experimental method, or the other name, computer simulation, is the method of choice for most research. In this proposed research, this method will also be the experiment of the research for two reasons.

Firstly, it is very cost effective since the use of virtual routers, switches and machine would tremendously reduce the cost for the implementation. For instance, the cost to lease 7 servers to install all those devices will be very affordable as presenting at the end of the report.

Secondly, it would be not feasible to ask one or several Internet Service Providers (ISP) to

implement and perform the experiment. The reason can be security concern, ethical issues and so on. Moreover, if the experiment causes any problem to the network, it will result in a great impact to the availability of the network.

For those above reason, experimental method is the best choice for this research in SDN network.

B. Design experiment

Base on the constrain of the research which will be presented later, the orchestration of network being used for the experiment will includes a number of seven basic SDN nodes as shown in the figure 1. This architecture will warrantee a complexity of paths being used for the test packet marking.

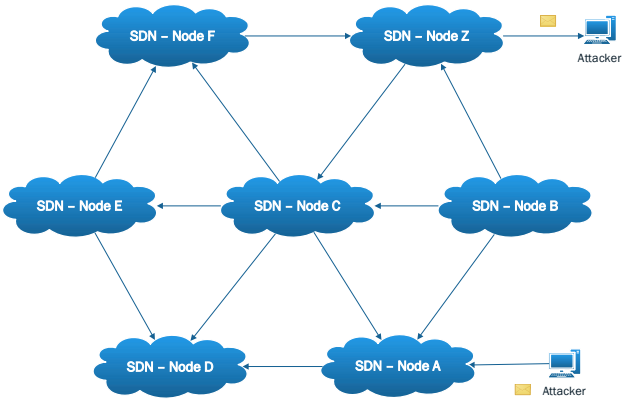

Fig 2. The network layout of experiment

Inside each SDN node, the structure of a typical SDN network will be represented as illustrated in the Fig. 2, with data plane, controller plane and Application Interface.

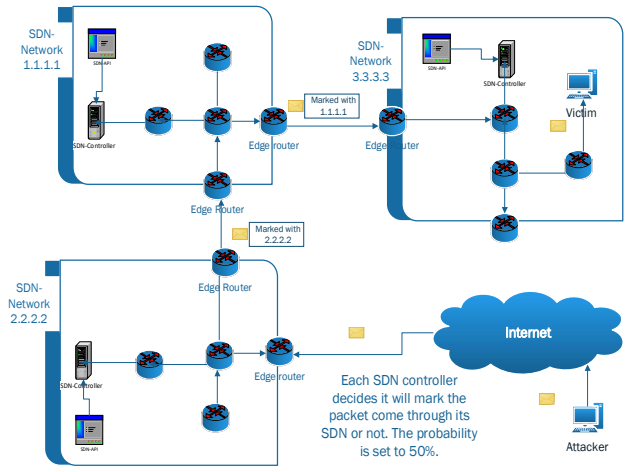

Fig.3 Network Diagram of the experiment

In each plane, the function of it will be implemented. For example, NOX controller will be install and work as a controller for each SDN nodes. At the data plane, the P4 programming language will be used to write the Identification field of the header of the standard IP packets. Those tools will be discussed further in the next research.

C. Implement the experiment

One of the limitations from other experiments [5-7] in this area is the hardware resources when authors tried to implement their experiment on an actual server. To overcome this challenge, this paper proposes a cloud-based environment for the testing, Amazon Web Service (AWS), where a large number of virtual servers using for this research can be configured and run at the same time.

Firstly, a number of seven instances of EC2, Virtual Machines, will be leased to meet the design of the experiment. This number can vary later depends on the need of changes from actual experiment, however, it can be done much easily on AWS.

Then, the following Operating System (OS), software, tools will be installed and configured on those virtual servers.

- Linux Operating System (Ubuntu).
- Open source Mininet software
- Open source NOX controller
- SONiC container or docker
- P4 programming language
- Hping3 or equivalent tools
- Snort (Intrusion Detection System)

Finally, those tools will be used to create a desired network, also generate legitimate traffic as well as DoS attacking packets for the conducting experiment which will be represented in next section.

D. Conduct the experiment

The conducting of the experiment will follow the in-house standard of experimental method [8] with three main parts, the pretest, treatment and post-test.

First of all, the pretest will be performed, and all relevant data will be recorded, such as performance of the network itself, the controller and servers. This is the baseline of the experiment bases on the control groups such as the number of legitimate packets, number of SDN nodes. The result of this test will be used against the followings tests.

Secondly, the main part of experiment will be conducted, the treatment. There will be two experimental groups using for the experiment, ratio of marked packets per total packets and number of malicious packets injecting into the network. Those groups will determine the number of samples for this treatment and will be adjust as followings.

- Ratio of marked packet: varying from 10% to 90% with step of 10%.
- Number of malicious packets: varying from 100 packets to 1,000 packets per second with step of 100 packets.

Consequently, this experimental test will need at least 100 samples to complete this part. It is also worth mentioning that this number may varies upon the study of validating data which will be performed in the next step.

As a final test, the post-test will also be performed to examine the side-effect of marking packet approach on the performance of the SDN network. As such, the malicious packets will not be injected into the network, however, the marked technique will remain for this part.

E. Data collecting, validating and analyzing.

In this section, the proposal report will discuss how data will be collecting, validating, and analyzing toward the results.

For a start, collecting data in computer experiment is quite simple since the tools being used for that process will be provided by AWS's service. For instance, the performance of the controller will be recorded by AWS. The number of packets generating in the network, for another instance, will also be controlled by a script written in Python programming language.

Then, the validating of data would be an essential step before and during the experiment. It is also worth noting that another issue with all the findings that this paper has literately reviewed in previous part is data validation. For example, the size of the network, the number of packets using in the experiments and so on. Being aware of that, this research will study how to validate data in the next stage of the research.

Next, the result achieving from experiment will be used to compare with baseline, the post-test results as well as other peer-research to justify the outcome of the approach.

F. Research Constrains

This research will be conducted for 1 year, including time for research on new technical issues, conducting experiments and result evaluation. As much as DOS attack can be executed from hosts in networks that span across a wide area, in this research we limit the tests to only 7 SDN networks due to financial constraints. DOS attacks can vary in duration, from study conducted by [9] there are no predictable patterns as to how long an assault can last with different organizations giving varied responses as shown in Figure 3.

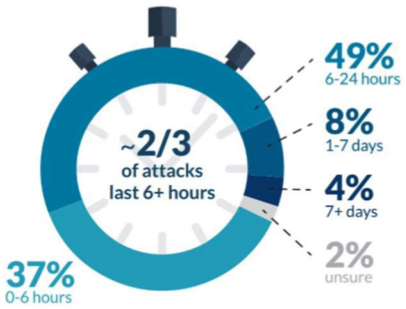

Fig 4. DDOS Attack Duration [9].

Common trends point to shorter duration of attacks but reported as well is attacks that lasted weeks. In our research we focus on shorter duration attacks but we the research findings are expected to still hold true for an attack that lasts for a longer duration. This is because of the nature of computer simulation technique.

It is also worth mentioning that, the experiment will be conducted on virtual environment without the use of actual traffic of an organization thanks to the advancing in network virtualization.

G. Calculate time, budget base on the design

The whole budget is divided by two parts: financial budget and time budget management.

Firstly, Amazon Elastic Compute Cloud (Amazon EC2) will be selected to be the platform to provide scalable computing capacity on AWS. The advantage of EC2 is that can eliminate investigation front of hardware. According to requirements of users, EC2 can also adjust the number of virtual services and storage. According the topology(Fig.2), it requires seven EC2 virtual machines leased on AWS for one year including built and test the network. According to the calculation of Amazon Website Services, it will cost $4905.6 Australia dollars for renting those virtual machines as below:

Fig.5 AWS Calculator.

In addition to the costs from renting virtual machines from AWS, this project also requires four networking engineers to build and test this network. Based on those two parts, the financial budget is fifty thousand Australia dollars. The projection of salary of four engineers is represented in below table:

Position	**Salary / hour**
Engineer (team leader)	$40
Engineer 1	$35
Engineer 2	$30
Engineer 3	$30

Table.1 financial budget - salary

The total time budget is one year, and the schedule detail is displayed on the table 2. According to the topology, it would cost five months for lease and implement this network and install all necessary tools. Moreover, the network should be tested for the outcome of the research, which may last from 2 to 4 weeks. Besides, the challenge on the research of trace-back by using packet marking would take a lot of time in new kind of network, the SDN, projecting up to three months. The study on marking technique using p4 programming language also need that much time. Use of P4 programming language to alter the field Identification of head of IP packet requires in-depth research and may last for 3 months.

Task	**Estimated Time needed**
Built network	5 months
testing	4 weeks
Trace-back study	3 months
Marking technique using P4 language	3 months

Table 2. Time budget

VI. ETHICAL CONSIDERATION

By conducting this experiment, the authors are being aware that there would be some aspect of the ethical issue relating to this area.

One of them is the tools that this report proposed to use for conducting a massive of the fake packets in the experiment which may be mimicked by other people. This therefore may lead to the spreading of DoS attacking on organizations intentionally from intruders.

The other possible issue to take into account is that, if this technique can be applied in the industry, it may be compulsory to ask for the permission to traceback a location of someone, though, he may be a potential attacker.

Being aware of these issues, the conducting of the research will have to comply with not only

Swinburne ethical conduct principle, but also from the government.

VII. SUMMARY

In conclusion, the report has reviewed some related findings in the field "mitigate the DoS attacks in SDN network" recently, justified the advantages of those studies, as well as the limitations of them. Then, this study proposed an innovative approach based on packet marking to overcome these drawbacks to counter DoS attacks. Later, the detail of a proposed research was presented, starting with a brief of the packet marking technique. Afterward, the methodology of the research was discussed with great detail in experiment. How to manage the project in terms of time and budget was also briefly discussed. Finally, the ethical consideration finishes off the report.

It also goes without mentioning that the internet is facing multipronged challenges. Hackers and cybercriminals have perfected their art of stealing information and corrupting systems. DDoS attacks are known to cripple institutions' operational ability by inhibiting the seamless flow of information, impairing different activities or totally stopping operations. Then, we, the authors believe that our novel approach would be practical and feasible to mitigate this kind of attacks in the future of the internet.

Word counts: 3272

REFERENCES:

1. Dynamic Probabilistic Packet Marking Based on PPM - IEEE Conference Publication. of Conference: 6-7 June 2009 Date Added to IEEE Xplore: 04 September 2009 ISBN Information: Print ISBN: 978-0-7695-3646-0 INSPEC Accession Number: 10867123 DOI: 10.1109/WMWA.2009.44Publisher: IEEE Conference Location: Wuhan, China; Available from: https://ieeexplore-ieee-org.ezproxy.lib.swin.edu.au/document/5232521/.
2. Joque, J. and C. Malabou, Deconstruction Machines : Writing in the Age of Cyberwar. 2018, Minneapolis, UNITED STATES: University of Minnesota Press.
3. Cui, Y., et al., SD-Anti-DDoS: Fast and efficient DDoS defense in software-defined networks. Journal of Network and Computer Applications, 2016. **68**: p. 65-79.
4. Eko, O.Y. Mitigating Denial of Service (DoS) attacks in OpenFlow networks - IEEE Conference Publication. 2014; Available from: http://ieeexplore.ieee.org.ezproxy.lib.swin.edu.au/document/6983147/?reload=true.
5. Zhani, L.D.M.F., A holistic approach to mitigating DoS attacks in SDN networks - Dridi - 2018 - International Journal of Network Management - Wiley Online Library. 2018.
6. SLICOTS: An SDN-Based Lightweight Countermeasure for TCP SYN Flooding Attacks - IEEE Journals & Magazine. of Publication: 08 May 2017; Available from: http://ieeexplore.ieee.org.ezproxy.lib.swin.edu.au/document/7920372/?part=1.
7. Fichera, S., et al., OPERETTA: An OPEnflow-based REmedy to mitigate TCP SYNFLOOD Attacks against web servers. Computer Networks, 2015. **92**: p. 89-100.
8. Kai-Tai Fang, R.L., Agus Sudjianto, Design and Modelling for Computer Experiments. 2005. **1st edition**: p. 42.
9. Mathews, T., Incapsula survey: What DDoS attacks really cost business. 2014.