Detection and mitigation of ddos attack essay

ASSIGN BUSTER

A Survey on Detection and Mitigation of Distributed Denial of Service attack in NamedData Networking

Sandesh Rai1*, Dr. Kalpana Sharma 2, and Dependra Dhakal 3

1Sikkim Manipal Institute of Technology, Student, Computer Science & Engineering, Rangpo, Sikkim.

2Sikkim Manipal Institute of Technology, Head of Department, Professor, Computer Science & Engineering, Rangpo, Sikkim

3Sikkim Manipal Institute of Technology, Assistant Professor, Computer Science & Engineering, Rangpo , Sikkim

Abstract. There are various number of on-going research are taking place that’s aims to provide next best Internet architecture although there are varieties of scope and maturity. This research is mainly based on to provide better security and better privacy as basic requirements of the protocol. Denial of Service Attacks which is a major issue in current Internet architecture also plays a critical issue in any new upcoming internet architecture and requires major focus for the same. The paper focus on the Interest flooding attack which is one the different type of Distributed Denial of service attack (DDOS). NDN incorporates better security features that detect and mitigate certain attack in the networks. But its resilience to the attacks has not analyzed yet. It presents the Distributed Denial of Service (DDOS) in Named Data Networking where an adversary sends out Interest packet with spoof names as an attacking packet to the NDN router.

Keywords: NDN, DDOS, Content store, Pending Interest Table, Cache pollution.

1A A Introduction

Clearly internet has become a part of the day todays life of the people. Millions of people around the world use it to do various type of day todays task. It connect millions of people around the world via wired , wireless, mobile or fixed computing devices and host huge amount of information(which is in the digital form) to be used by people. Internet provides information to be exchanged and has exponentially grown over time. The main ideas of the Todays internet architecture were developed in 70’s. The telephone where conversation was point to point. The utilization of the Internet has dramatically changed since 70’s and current internet has to adapt well with new usage model, new application and new services. To cope up with these changes, a variety number of research is taking place to design a new Internet architecture.

Named Data Networking (NDN) [1] is one of the ongoing research . Its main objective is to developed a next best Internet architecture for upcoming generation. It’s an instantiation of the of the Information Centric approach (ICN) or Content Centric approach (CCN) [1][2][3]. The main objective of the CCN is to provide more flexibility, security and scalability. A CCN provide more security by securing the individual pieces of content rather than securing the connection. It provides more flexibility by using content name instead of using IP addresses. A NDN is one of the instances of Information Centric Networking (ICN). NDN is based on the working principle of Content-

Centric Networking (CCN) [3], where content instead of hosts are the main focus in the communications architecture. NDN is one of the research projects funded by the United State of National Science Foundation (NSF) which is under Future Internet Architecture (FIA) Program [3]. NDN focus on the name rather than the location of the host. In NDN every pieces of the data is digitally signed by its source producer. The signing in data allows the producer to be trusted and authenticated. Caching of the data is one of the core features of the NDN which helps to optimum use of network bandwidth use in the network . NDN provide an attractive architecture for the data distribution, anonymous communication.

1. 1A A A Distributed Denial of service attack:

As the years goes by, Distributed denial of service (DDOS) attack have become common and dangerous and it remains among the most critical threats on the current Internet. They are very difficult to detect and mitigate. Any new architecture should detect and mitigate DoS attack or at least minimum their effeteness. NDN appear to be efficient for the distribution of the content for the legitimate parties but unknown to malicious parties. Instead of using single host computer and single connection for the internet, the DDOS attack utilizes various number of host computers and various number of internet connections. The host computers for an attack are distributed across the whole wide world. The difference between a DOS attack VS a DDOS attack is that the victim host will be overloaded by thousands number of resources requests. In the attacks process, the adversary host node in the network sends request a huge number of zombie for the attack to take place. A malicious user attacks the network host by

requesting resources in a huge number in the form of Interest packets with spoofed names or without spoofed name. These huge numbers of Interest consumes the bandwidth of the network and exhaust a router’s memory. This type of attack is known as Interest Flooding Attack (IFA) and this paper exclusively focus on this problem and their proposed countermeasures.

2A A Overview of NDN Architecture

Named data networking is an new and ongoing research architecture whose motivation is the architectural mixed of current internet architecture and its various usage. However the architecture design and principles are motivational derivation from the successes of today’s Internet architecture [4]. The thin waist as can be seen in Figure 1 of hour glass architecture was the key service of the enormous growth of the internet by allowing both upside layer and bottom layer technologies to innovate independently. The NDN architecture contains the same hourglass shape as shown in Figure 1. 2. 1, but changes the thin waist by using data directly rather than its location.

Figure 2. 1 [4]: A NDN Hourglass Architectures

For communication, NDN provide two different packets i. e. Interest and Data packets. A user asks for resources by issuing Interest packet to the router in the network, which contains a name for those particular resources that identifies and verifies the desired data for the host. Different fields of a data packet [5]:

1. Signature: To verify data.

2. Key locator: To verify signature.

3. Publisher Public Key Digest: Public key hash of the producer.

4. Content name: Name of the requested data.

5Selector: which includescope: andreserved.

Figure 2. 2 [6]: Packets in the NDN Architecture

Any node having data that satisfies it, a Data packet is issued by the satisfied router [7], each router of NDN contains following different three data structures for Interest packet and Data packet forwarding.

i)Content Store (CS): Recently used data are store.

ii)Forward Information Base (FIB): Routing table of name of the data and it guides Interests toward data producers [8].

iii)Pending Interest Table (PIT): Store unsatisfied data request. It record the requested data name[8].

3A A Interest Flooding attacks

By using the information and state of the Pending Interest Table (PIT), a routing of content by router is performed. In the PIT the name of requesting content is looked up for identifying its entry. The malicious node uses the state of the PIT to perform DDOS attacks. Basically there are three types of Interest Flooding attack [9]:

a)Static: This type of attack attacks the infrastructure of the network and is limited and caching provides a build in solution. The interest is satisfied by the content of the cache [10].

b)Dynamically generated: Here the requested resources is dynamic and all the requested interest reaches to the content producer depleting the network bandwidth and state of the Pending Interest Table (PIT). Since the requested content is dynamic, in build cache does not serve as countermeasure for the attacks[10].

c) Non- existing: This report focus on this attack type where attacker involves non-satisfiable interest for a non-existing content in the network. These kinds of interest are not taken care by the router and are routed to the content producer depleting network bandwidth and router PIT states [11].

In all three types of attacks the malicious host uses a very large number of fake request, which are distributed in nature, An adversary host can useA two features unique to NDN, namely CS and PIT, to perform DDoS attacks [12] in the router. We focus on attacks that overwhelm the PIT, which keeps record which are not fulfill by a router. The adversary host issues a large set of fake request, which are possibly distributed in nature, to generate a large number of Interest packets with spoofed name as shown in Figure 1. 3. 1 aiming to (1) overwhelm PIT table in routers, and (2) swamp the target content producers [13][14].

Figure 3. 1 [15]: Example of Interest flooding attack

Once the PIT is exceed its threshold, all incoming interests are dropped as there will no memory space available to create entries for new resourced interests. Since the names are spoofed, no Interest packets will be satisfied by the content [16]. These packets request will remain in the PIT for as much

as possible, which will definitely exhaust the router memory and router resources on routers. This is the goal of Interest flooding attack.

4A A A Related Works

Gasti et al. [17] analyzed the resilience of Named Data networking to the DDOS attacks. The paper discussed two different types of attacks with their effect and proposed two countermeasure mechanisms: a) Router Statistics and b) Push-back approaches.

Afanasyev et al. [18] addressed the flooding attack. Their works explain the feasibility of the interest flooding attacks and the requirement of the effective solution. In terms of evaluation of the attack the proposed mitigation plan is complementary to Poseidon mitigation . Afanasyev et al. proposed three different mitigation algorithms: a)token bucket with per interface fairnessb)satisfaction-based pushbackc)satisfaction-based interest acceptance. All the three algorithms exploit their own state information to stop Interest flooding attacks. Satisfaction based pushback mechanism among three algorithms effectively detect and mitigate the attack and ensure all the interest form a legitimate user.

Campagno et at. [19] Addressed the flooding attacks and proposed a mitigation algorithm called Poseidon. This algorithm is strictly used for non-existing type of interest flooding attacks. This mitigation algorithm is used for local and distributed interest flooding attacks.

Dai et al. [20] addressed the flooding attacks and proposed a mitigation algorithm. The solution is based on the collaboration of the router and the

content producer. Dai et al. proposed Interest traceback algorithm. The algorithm generates a spoof data packet to satisfy the interest in the PIT to trace the originators. According to the, the algorithm is not proactive, that overhead the network by sending out spoof data packet for the interest depleting the bandwidth of the network and creating traffic. The main shortcoming of this approach is that its take the long unsatisfied interest in the PIT as adversary interest and others as legit interest. So the router drops any long incoming interest packet which may be a legitimate interest.

Choi et al. [21] addressed the overview of the Interest Flooding attacks for strictly non-existing content only on NDN. The paper tries to explain the effectiveness of the attack in the network and in quality of services.

Karami et al. [22] addressed and provide a hybrid algorithm for the solution. The algorithm is proactive. There are two phase 1) detection 2) reaction. In detection phase the attack is detect using combination of multi objective evolutionary optimization and Radial basis function (Neural Network). In the reaction phases an adaptive mechanism for reaction is used to mitigate the attacks.

5A A Analysis of survey

The following table show the analysis of the all the paper and comparison related only on the project. The table is a comparison of different paper which is written by well-known publishers. The Analysis try to provide a possible research gap that is present on the paper.

Table 1. Comparison of different NDN related paper

SLno

Title

Publication Details

Summary

Research Gap

1

DoS & DDoS in Named Data Networking

P. Gasti, G. Tsudik, E. Uzun, and L. Zhang. DoS & DDoS in named-data networking. Technical report, University of California.

Discussed two types of attacks with their effects and potential countermeasures (Router Statistics and Push-back Mechanisms).

1. The paper only put a light on the attack and its possible countermeasures.

2

Interest flooding attack and countermeasures in Named Data Networking

A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang. Interest flooding attack and countermeasures in Named Data Networking. In IFIP Networking.

Proposed three mitigation algorithms. (token bucket with per-interface fairness, satisfaction-based Interest acceptance, and satisfaction-based pushback).

1. Improvements in token bucket with per-interface fairness, satisfaction-based Interest acceptance was less effective than satisfaction based pushback.

3

Poseidon: Mitigating interest flooding DDoS attacks in named data networking.

A. Compagno, M. Conti, P. Gasti, and G. Tsudik, Poseidon: Mitigating interest flooding DDoS attacks in named data networking, Conference on Local Computer Networks.

Proposed a framework, named Poseidon, for mitigation of local and distributed Interest flooding attack for non-existing contents

1. Fixed Threshold.

4

A hybrid multiobjective RBFPSO method for mitigating DoS attacks in named data networking.

A. Karami and M. Guerrero-Zapata, A hybrid multiobjective RBFPSO method for mitigating DoS attacks in named data networking, Neurocomputing.

Introduced an intelligent combination algorithm for the solution.

1. Investigating inter-domain DoS attacks and applying Hybrid approach.

5

Threat of DoS by interest flooding attack in content-centric networking

S. Choi, K. Kim, S. Kim, and B.-H. Roh,: Threat of DoS by interest flooding attack in content-centric networking, in International Conference on Information Networking.

Explain the difficulty for getting a solution flooding attacks in the PIT.

1. Analyzing DDoS attacks and their countermeasures.

6

Mitigate ddos attacks in ndn by interest traceback

H. Dai, Y. Wang, J. Fan, and B. Liu. Mitigate ddos attacks in ndn by interest traceback. In NOMEN.

Introduced a traceback solution where a node sends a spoof data packet to trace the host.

1. Only the request which is long is considered as malicious request.

6A A A Conclusion

This report starts with a brief introduction of the CCN, NDN architecture and which is further followed by common and most critical attacks in today’s internet. NDN mainly focuses on the data security, data privacy for the users. This report clearly represents only the starting step for mitigating DDOS

attacks on the Pending Interest Table in the context of NDN. In this paper, we have explained DDOS attack and its various types namely, interest flooding attack. We have discussed current research regarding the attack, their existing solution, and try to analyze the given solution for detection and mitigation. The adversary tries to exploit interest forwarding rule to make certain interest for the packet with the never existing content name. We analyzed that the victim of the attack is host and PIT of the router. Thus a huge amount of Interest packet will reside on the PIT of the router which use and exhaust the memory of the router and computing resources of the router which will definitely degrade the performance of the router. The NDN is the latest ongoing research topic and a new propose Internet architecture where limited research have been done for the mitigationA and detection of theA interest flooding attack thus there is a very much need for details analysis on the security before the architecture actually deployed.

References

V. Jacobson, M. Mosko, D. Smetters, and J. Garcia-Luna-Aceves.: Content-A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A A centricA A networking, Whitepaper, Palo Alto Research Center, pp. 2-4 (2007)V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard,.: Networking named content, in Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, ACM(2009)L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, C. Papadopoulos et al.: Named data networking (NDN) project, Relatorio Tecnico NDN-0001, Xerox Palo Alto Research Center-PARC(2010)J. Pan, S. Paul, and R. Jain.: A

survey of the research on future internet architectures, Communications Magazine, IEEE (2011)A. Hoque, S. O. Amin, A. Alyyan, B. Zhang, L. Zhang, and L. Wang.: NLSR: Named-dataA A A link state routing protocol, in Proceedings of the 3rd ACM SIGCOMM Workshop7Information-Centric Networking, ACM, pp. 15-20(2013)V. Jacobson, J. Burke, L. Zhang, B. Zhang, K. Claffy, D. Krioukov, C. Papadopoulos, L. Wang, E. Yeh, and P. Crowley.: Named data networking (NDN) project 2013- 2014 report, http://named-data. net, Annual Progress Report(2014)C. Ghali, G. Tsudik, and E. Uzun.: Elements of trust in named-data networking, ACMA A A A SIGCOMM Computer Communication Review, ACM, vol. 44, no. 5, pp. 1-9 (2014)M. Aamir and S. M. A. Zaidi,.: Denial-of-service in content centric (named data) networking: A tutorial and state-of-the-art survey, Security and Communication Networks, vol. 8, no. 11, pp. 2037-2059 (2015)M. WA? ahlisch, T. C. Schmidt, and M. Vahlenkamp.: Backscatter from the data plane threats to stability and security in information-centric networking. CoRR, abs/1205. 4778 (2012)Content centric networking (CCNx) project. http://www. ccnx. org. A. Afanasyev, I. Moiseenko, and L. Zhang.: ndnSIM: NDN simulator for NS-3. Technical Report NDN-0005, 2012, University of California, Los Angeles(2012)Wang R, Jia Z, Ju L.: An Entropy-Based Distributed DDoS Detection Mechanism in Software-Defined Networking. InTrustcom/BigDataSE/ISPA, Vol. 1, pp. 310-317(2013)Kumar, K., Joshi, R. C. and Singh, K..: A distributed approach using entropy to detect DDoS attacks in ISP domain. In Signal Processing, Communications and Networking, ICSCN’07. International Conference on pp. 331-337(2007)Feinstein L, Schnackenberg D, Balupari R, Kindred D. : Statistical approaches to DDoS attack detection and response. InDARPA Information Survivability Conference

and Exposition, 2003. Proceedings Vol. 1, pp. 303-314(2003)Krishnan, R., Krishnaswamy, D. and Mcdysan, D.: Behavioral security threat detection strategies for data center switches and routers. In Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE 34th International Conference on pp. 82-87(2014)Zhang Y.: An adaptive flow counting method for anomaly detection in SDN. InProceedings of the ninth ACM conference on Emerging networking experiments and technologiesA pp. 25-30(2013)P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, DoS and DDoS in named data networking, in 22nd International Conference on Computer Communications and Networks (ICCCN), pp. 1-7(2013)A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang.: Interest flooding attack and countermeasures in named data networking, in IFIP Networking Conference, pp. 1-9(2013)A. Compagno, M. Conti, P. Gasti, and G. Tsudik, Poseidon: Mitigating interest flooding DDoS attacks in named data networking, in 38th Conference on Local Computer Networks (LCN), IEEE, pp. 630- 638(2013)H. Dai, Y. Wang, J. Fan, and B. Liu, Mitigate DDoS attacks in NDN by interest traceback, in Conference on Computer Communications Workshops.(INFOCOM WKSHPS), IEEE, pp. 381-386(2013)S. Choi, K. Kim, S. Kim, and B.-H. Roh, Threat of DoS by interest flooding attack in content-centric networking, in International Conference on Information Networking (ICOIN), pp. 315-319(2013)A. Karami and M. Guerrero-Zapata.: A hybrid multiobjective RBFPSO method for mitigating DoS attacks in named data networking, Neurocomputing, vol. 151, pp. 1262-1282(2015)