Mitigating Distributed Denial-of-Service Attacks in Named Data Networking

Vassilios G. Vassilakis
Institute for Communication Systems
University of Surrey
Guildford, United Kingdom
e-mail: v.vasilakis@surrey.ac.uk

Bashar A. Alohali
School of Computing and Mathematical Sciences
Liverpool John Moors University
Liverpool, United Kingdom
e-mail: b.a.alohali@2012.ljmu.ac.uk

Ioannis D. Moscholios
Dept. of Informatics and Telecommunications
University of Peloponnese
Tripolis, Greece
e-mail: idm@uop.gr

Michael D. Logothetis
Dept. of Electrical and Computer Engineering
University of Patras
Patras, Greece
e-mail: mlogo@upatras.gr

***Abstract*—Named Data Networking (NDN) is a novel networking approach that aims at overcoming some of the limitations of the current Internet. In particular, NDN aims at providing better privacy and security by focusing on the data items themselves rather than on the location of data. This is achieved by using soft states at the routers, which record the requests/interests for data from users in the Pending Interest Table (PIT). However, this new networking concept opens up avenues for launching Distributed Denial-of-Service (DDoS) attacks on PITs. That is, an attacker may flood the network with a large number of Interest packets that would overflow the PITs at the routers, thus preventing legitimate users from receiving the requested data. This type of DDoS attack is known as the Interest Flooding Attack (IFA) and, if not adequately dealt with, may severely disrupt the normal operation of an NDN system. In this paper, we first show that the basic NDN mechanism is vulnerable to IFA even when the attacker has very limited resources. Next, we propose a mitigation technique that allows routers to quickly identify and block such DDoS attempts, by detecting anomalous user behaviour. We also introduce an additional security layer by using public-key based router authentication. We evaluate our proposed scheme by means of computer simulations and show that a sufficient level of security can be achieved with little processing and storage overhead.**

Keywords–Named Data Networking; Distributed Denial of Service; Interest Flooding Attack.

I. INTRODUCTION

As it has been observed by numerous studies, today the Internet is mainly used for data dissemination to interested users, rather than for connecting hosts. The user is interested in data itself, while the *location* of data is usually of minor importance. However, the Internet was originally designed and has evolved according to the host-centric communication paradigm. Recent studies have shown that the poor performance of the traditional Internet, in the areas of security, efficient content dissemination, etc., lies in its host-centric nature [1].

Information Centric Networking (ICN) [2] is a new effort that aims at eliminating the traditional Internet's limitations. Named Data Networking (NDN) [3] is one of the proposed ICN approaches. Data dissemination in NDN is achieved by using soft states at the routers, which record the interests for data from users in the Pending Interest Table (PIT) [4]. When the requested data is received by the router and forwarded to the user, the corresponding PIT entry is removed. In contrast to the current Internet, where the security measures have been added after its conception, NDN's key target is to embed security and privacy features at the very early design stages. In particular, for protecting user privacy, no source address is carried in the packets [5]. The routers record in PIT the incoming interface for the Interest packet and use it to forward the data to the user. NDN also inherently provides protection against unsolicited data by adopting the receiver-driven data retrieval model [6].

However, in spite of the aforementioned security advantages of NDN, new types of distributed denial-of-service (DDoS) attacks are possible [7]. In particular, one of the most challenging is the DDoS attack on PITs, where an attacker floods the network with a large number of bogus Interest packets. Each such packet causes the router to create and maintain an entry in its PIT, thus wasting router's storage resources and even creating the possibility of PIT overflows. This type of attack is known as the Interest Flooding Attack (IFA) [8] and, if not adequately dealt with, may severely disrupt the normal operation of an NDN system.

In this paper, we first show that the basic NDN mechanism is vulnerable to IFA even when the attacker has very limited resources. Next, we propose an IFA mitigation technique at the router, that detects anomalous user behaviour and also notifies other routers. To secure from bogus notifications by malicious/compromised routers, we propose an authentication scheme that is based on public-key cryptography.

This paper is organized as follows. In Section II, we briefly describe the considered NDN architecture and introduce the necessary notations. In Section III, we define the IFA and briefly discuss other types of DDoS attacks in NDN. In Section IV, we present our IFA mitigation scheme. In Section V, we present our router authentication method. In Section VI, we study the performance of the proposed approach by means of computer simulations. In Section VII, we present the related work on DDoS attacks and countermeasures in NDN and in other ICN mechanisms. We conclude and discuss our future work in Section VIII.

 ISBN: 978-1-61208-411-4

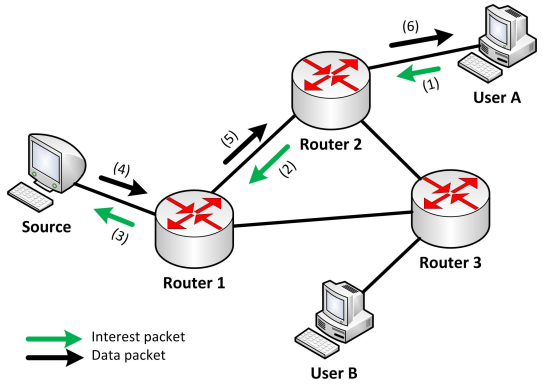

Figure 1. Basic NDN communication model.

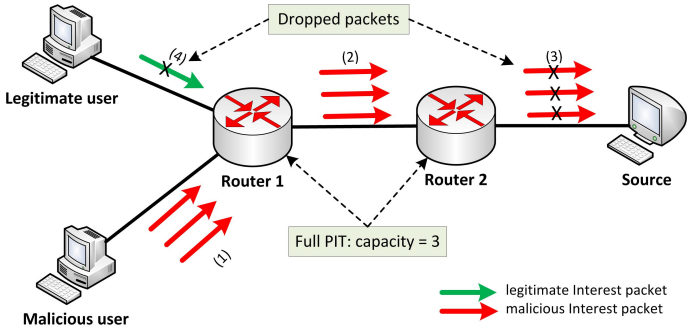

Figure 2. Interest Flooding Attack on NDN.

II. NDN Architecture and Basic Concepts

In this section, we briefly describe the NDN architecture and its basic concepts [3]. Contrary to the traditional host-centric network architectures (e.g., the Internet), the basic abstraction in NDN is the *named content*. Content sources advertise/publish their available content items in the network by issuing the *Publication packets*, which usually include prefix-based content name or some other form of content identifier (ID) [9]. Each router, upon receiving such packets, records the incoming interface and the content name in its Forwarding Information Base (FIB) [10].

ICN also natively supports quality-of-service [11] and content caching. The caching approach could be either opportunistic and transparent to the content resolution function (i.e., not recorded in the FIB) or proactive and similar to the Content Delivery Network (CDN) approach [12]. The latter approach essentially transforms caches into alternative content sources and enables joint optimization of forwarding and caching functions [13].

Users interested in receiving a particular content item, issue the *Interest packets*. These packets are then forwarded via a sequence of routers towards the content source or cache, according to the FIB entries for the requested content. In case that multiple sources (and/or caches) are holding the same content, some kind of mediated topology management function could be used to select the best source [14] or even to enable multi-chunk content delivery [15].

When the source/cache receives the Interest packet it replies with the *Data packet*, which contains the requested content. The Data packet is forwarded via the reverse path towards the user. A simple illustrative example is shown in Figure 1. This is the so-called pull-based communication model and it ensures that the user receives only explicitly requested content.

In order for the routers to be able to deliver Data packets to the users, each router is equipped with a PIT [4]. The latter contains entries for all "not yet satisfied" Interest packets and their incoming interface. Note that this communication scheme does not require any user address (e.g., IP address) carried in the Interest and Data packets. These packets are required to carry only the content name of some other kind of content ID.

III. DDoS in NDN

A. Interest Flooding Attack

Malicious/compromised users may exploit the PIT-based forwarding mechanism of NDN to launch the IFA, which is considered as one of the most serious types of DDoS attacks on NDN [16]. According to IFA, the malicious user (or a group of users) will issue a large number of bogus Interest packets. Each router, upon receiving each of these packets, will create an entry in its PIT and will forward the packet to the next-hop node (router or content source). According to the NDN rules, an entry is removed from the PIT in the following two cases:

- Entry expired (e.g., a typical expiry time is 1s [17]).
- Router received the corresponding Data packet before the entry expiration.

According to the above, the best attacking strategy is to issue Interest packets for non-existent content. In this case, the bogus entries will stay in the PIT as much as possible. The goal of the attacker is to quickly fill in the PIT and to keep it full, so that the Interest packets originated from legitimate users will eventually be dropped.

In Figure 2, we illustrate a simple example of IFA in NDN. Assume that the PIT capacity in each router is 3 entries. The attacker's strategy is to send 3 bogus Interest packets for (different) non-existent content. These packets will fill in the PITs of both routers. The source will drop these packets, since they request non-existent content. However, the corresponding entries will stay in the PITs until they expire. After the expiration, the attacker will issue 3 new Interest packets, aiming at keeping the PITs always full. This way, some, or even all, Interest packets of legitimate users will be dropped. Later, in Section VI, we evaluate the packet dropping probability of legitimate users and show that it could be very high even when the attackers employ limited resources.

B. Other DDoS Attacks

In this subsection, we briefly discuss other possible types of DDoS attacks in NDN, which, however, are out of the scope of this paper.

1) cache poisoning/pollution attack: The attacker is trying to reduce the cache efficiency by filling in the cache with non-popular or even fake content. This can be done by repeatedly requesting the same unpopular content. This aims at increasing the cache misses and forcing the Interest packets to reach the content source. This type of attack is not easy to mitigate,

 ISBN: 978-1-61208-411-4

because the malicious user may appear as a legitimate one for a very long time.

2) mobile interest flooding attack: The attacker may periodically visit different routers and issue bogus Interest packets. This attack is harder to detect and mitigate than the classic IFA. The reason is that retransmission of Interest packets in case of mobility is a normal procedure in NDN. So, to detect a mobile attacker, a complex scheme that involves a large number of cooperating routers would be required.

3) attack on forwarding mechanism: A potentially compromised router may severely degrade the performance of the network by re-directing the Interest packets in wrong direction. In case of cooperating attackers, this could even be exploited for creating forwarding loops in the network.

IV. IFA Mitigation Mechanism

In this section, we describe our proposed mitigation mechanism for IFA in NDN. The aim of this approach is to quickly detect anomalous user behaviour and to restrict, or even block, such user at an early stage of the attack. We distinguish two types of routers:

- *Edge routers*: directly connected to one or more users.
- *Core routers*: directly connected only to other routers or sources.

The edge routers will provide an additional security layer by detecting any anomalous user behaviour and will notify other routers if such an event takes place. The latter is done by sending the *attack notification packets*, that contain the user ID. Core routers will be involved in forwarding the attack notification packets to other routers, but will not themselves contribute in the attack detection process.

Our mitigation mechanism comprises three phases:

- *Attack detection phase*: the edge router detects anomalous user behaviour and identifies the user either as suspicious or as an attacker.
- *Rate reduction and blocking phase*: the edge router reduces the data rate of suspicious users and blocks the attackers.
- *Attack notification phase*: the edge router notifies other edge routers about the detected attack.

In the following, we provide more details about these three phases.

A. Attack detection phase

The set of all users in the network is denoted by U. During the detection phase, the edge router keeps statistics about the expired PIT entries per each user $u \in U$. Two thresholds are used to classify users into: *legitimate*, *suspicious* (possible attackers), and *malicious* (attackers). If the number of expired PIT entries per time unit, $N_{exp}(u)$, of a user u is below the low threshold, T_{low}, user u is considered legitimate. If $N_{exp}(u)$ is above T_{low} but below the high threshold, T_{high}, user u is considered suspicious. Finally, if $N_{exp}(u) > T_{high}$, user u is considered malicious. The sets of legitimate, suspicious, and malicious users are denoted by L, S, and M, respectively.

B. Rate reduction and blocking phase

During this phase, any user that has been classified as malicious, will be blocked, whereas the suspicious users will receive reduced data rate. In particular, the rate adaptation is performed as follows:

$$R_{new}(u) = \begin{cases} R_{old}(u), & \text{if } u \in L \\ \frac{aR_{old}(u)}{T_{high}-T_{low}}, & \text{if } u \in S \\ 0, & \text{if } u \in M \end{cases} \quad (1)$$

where $R_{old}(u)$ and $R_{new}(u)$, are the old and new data rate of user u, respectively; a is some optimization parameter, such that $a + T_{low} < T_{high}$.

C. Attack notification phase

If an edge router detects an ongoing attack, after blocking this user, it will notify other routers about the identity of the malicious user, by sending the attack notification packet. This is done to prevent the Mobile Interest Flooding Attack (MIFA) [7], where a mobile user periodically visits different routers and floods them with Interest packets. In this context, the notion of router is extended and refers to any data-forwarding network element, such as a WiFi Access Point (AP) or a Base Station (BS) in a cellular network.

V. Router Authentication Method

We consider a scenario where edge routers may be deployed by home users or other non-trusted parties. That will most likely be the case in future fifth generation (5G) cellular networks [18], in future generation Internet [19], and in smart grid networks [20]. Also, edge routers may join and leave the network or change their location (e.g., vehicular communications). This introduces new security threats and a good authentication method is needed.

In this section, we propose a public-key based router authentication method (similar to [21]) to protect against bogus *attack notification packets* that could be sent by potentially compromised routers. Our method makes the reasonable assumption that there will be at least one trusted network entity that can act as Certificate Authority (CA). We consider the following two cases:

- *Direct authentication*: Performed when the new router has a direct connection with CA.
- *Indirect authentication*: Performed when the new router has no direct connection with CA. In that case, the authentication of a new router is facilitated by another, already authenticated router, referred to as *mediator*.

A. Direct authentication

Initially, the new router will send the *authentication request* message to CA (see also Figure 3).

This message is encrypted using CA's public key, PK-CA, and includes the following information:

a) identity number of the new router, R-ID,
b) timestamp, TS,
c) symmetric key of new router, SK-R.

CA responds with the *authentication response* message.

 ISBN: 978-1-61208-411-4

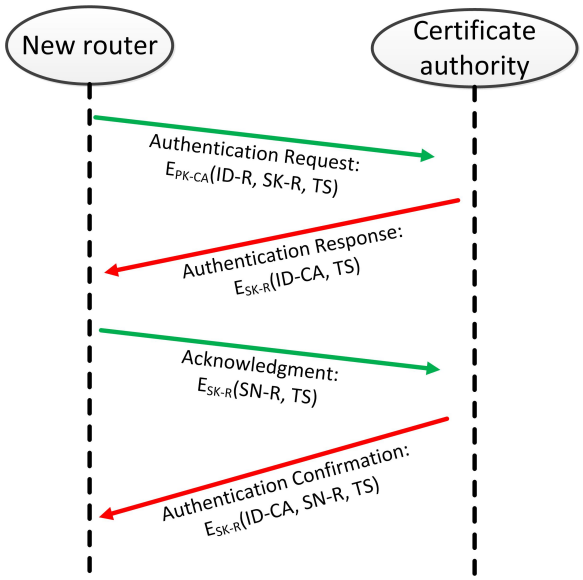

Figure 3. Direct router authentication.

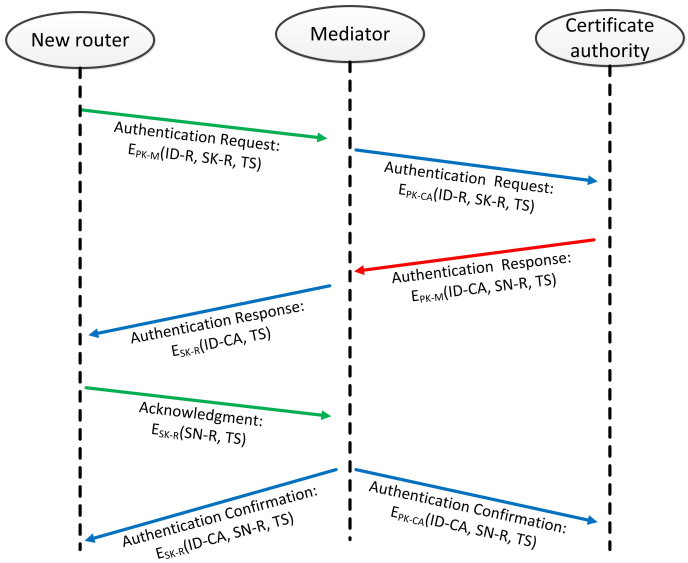

Figure 4. Indirect router authentication.

This message is encrypted using the received SK-R and includes the following information:

a) identity number of CA, ID-CA,
b) timestamp, TS.

Next, the router sends the *acknowledgement* message, which also contains routers serial number, SN-R, so that CA may validate this router as a legitimate one (we assume that CA holds a list of all valid SN-Rs).

This message is encrypted using the SK-R and includes the following information:

a) serial number of new router, SN-R,
b) timestamp, TS.

Finally, CA responds with the *authentication confirmation* message. This message is encrypted using the received SK-R and includes the following information:

a) identity number of CA, ID-CA,
b) timestamp, TS,
c) serial number of new router, SN-R.

B. Indirect authentication

Initially, the new router will send the *authentication request* message to the mediator (see Figure 4).

This message is encrypted using mediator's public key, PK-M, and includes the following information:

a) identity number of new router, ID-R,
b) timestamp, TS,
c) symmetric key of new router, SK-R.

The mediator will decrypt the message using its private key. Next, it will encrypt the message using CA's public key, PK-CA, and will send it to CA.

CA responds to mediator with the *authentication response* message. This message is encrypted using mediator's public key, PK-M, and includes the following information:

a) identity number of CA, ID-CA,
b) timestamp, TS,
c) serial number of new router, SN-R.

The mediator will decrypt this message using its private key. Next, it will remove the SN-R from the message, will store it and will re-encrypt the remaining message using the previously received SK-R and will send the message to the new router. The serial number, SN-R, will be used later by the mediator to verify that the new router is legitimate.

Next, new router sends to mediator the *acknowledgment* message that contains its serial number, SN-R, to be used for validation by mediator.

This message is encrypted using SK-R and includes the following information:

a) serial number of new router, SN-R,
b) timestamp, TS.

Finally, if the authentication is successful, the mediator responds to both new router and CA with the *authentication confirmation* message. This message is encrypted for new router using SK-R and for CA using PK-CA, and includes the following information:

a) identity number of CA, ID-CA,
b) timestamp, TS,
c) serial number of new router, SN-R.

VI. Performance Evaluation

In this section, we evaluate the DDoS vulnerability of the basic NDN mechanism [3] described in Section II. To this end, we have developed an NS-3 based simulator for NDN and implemented our proposed attack mitigation scheme for a randomly generated network topology. We have simulated 1,000 legitimate users generating traffic at a rate of 20 packets/sec. We have also simulated a DDoS attack scenario on PIT, where 50 attackers generate bogus Interest packets at a rate of 1,000 packets/sec. The packet size is selected to be 1KB, so that the attacking capability of each attacker is 1Mbps.

 ISBN: 978-1-61208-411-4

The duration of our simulation is 50s. The attack starts at $t = 5$s and lasts until $t = 40$s. In Figure 5, we show the required size of the PIT of the edge router, as it grows over time due to the launched attack. The results are shown for three different PIT entry expiration times, $t_{exp} = 200$ms, 500ms, and 1s. As discussed in Section III, $t_{exp} = 1$s is the currently adopted value in NDN. The value $t_{exp} = 200$ms is certainly too optimistic (in terms of PIT size requirements) and is shown only for comparison, as the best case scenario for the victim router. With such small t_{exp}, a large number of legitimate requests will not be satisfied, since the corresponding PIT entry of each request will expire before the content arrives. In Figure 5, we observe that during the first 5 seconds, when only legitimate users are active, the required PIT size is relatively small ($\approx$ 20MB). However, shortly after the attack starts, the PIT size increases rapidly and almost reaches 2GB by $t = 40$s, for $t_{exp} = 1$s. These results show that it is relatively easy even for attacking nodes of limited capabilities to quickly occupy large amounts of router's storage and processing resources.

In the second phase, to show the negative impact of the IFA, we evaluate the packet dropping probability of legitimate users due to PIT overflow. We consider the PIT capacity equal to 1GB and use $t_{exp} = 500$ms (with $t_{exp} = 1$s the negative impact on victims would be even worse). The rest of the simulation parameters remain the same as described in the previous paragraph. In Figure 6, we present the results for the basic NDN mechanism and for our threshold-based mitigation scheme of Section IV. In the latter, the attack detection thresholds are chosen to be $T_{high} = 0.5$ and $T_{low} = 0.25$. We consider two cases with different optimization parameters: $a = 1/8$ and $a = 1/12$. When $a = 1/8$, the mitigation scheme reduces the data rate to 50%. That is, $R_{new}(u) = \frac{1}{8}\frac{R_{old}(u)}{0.5-0.25} = 0.5R_{old}(u)$. Similarly, when $a = 1/12$, the mitigation scheme reduces the data rate to 33%. In Figure 6, we observe that when no mitigation scheme is used (i.e., basic NDN mechanism is assumed), 80% of the Interest packets of legitimate users are dropped between around $t = 25$s and $t = 40$s. This is due to the fact that by $t = 25$s the PIT size has reached its capacity of 1GB. When the mitigation scheme is used, the worst-case dropping probability is reduced to 60% and 40%, for $a = 1/8$ and $a = 1/12$, respectively. Also, the negative impact of the PIT overflow is time shifted (by 5s when $a = 1/8$ and by 8s when $a = 1/12$). We have also tried $a = 1/16$ which results in 25% data rate reduction for malicious users and completely eliminates the packet dropping of legitimate users.

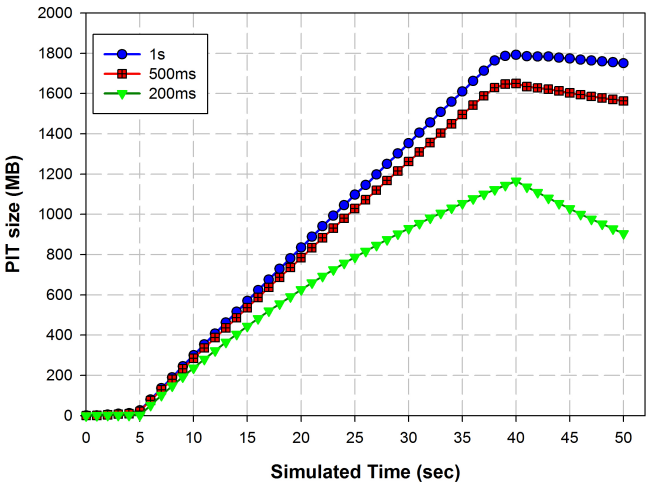

Figure 5. PIT size for different PIT entry expiration times. The attack window is 5-40s.

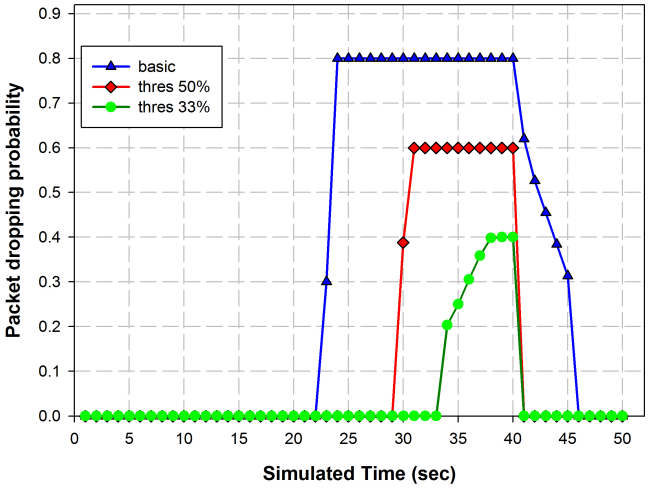

Figure 6. Packet dropping probability of legitimate users for the basic NDN and two threshold-based mitigation schemes.

VII. Related Work

A number of works study DDoS attacks in NDN. In [16], various types of attacks and possible countermeasures are discussed. It is argued that the most difficult to mitigate are the IFA and the cache poisoning attacks. However, no evaluation or assessment is presented. In [22], the *token bucket* method is proposed to mitigate the IFA. According to this method, the routers are restricted in forwarding Interest packets based on the load of their outgoing interfaces. To enable such behaviour, the routers need to keep track of the requested data volume from each interface. The proposed approach has been evaluated using the ndnSIM simulator [23] and shows satisfactory performance in cases of moderate attacking capability. In [24], to alleviate the negative impact of the IFA on PIT, the Disabling PIT Exhaustion (DPE) mechanism is proposed. Interest packets are dynamically diverted out of the PIT if their prefixes are detected as malicious. However, this introduces extra overhead on routers for marking packets and for maintaining a malicious list to be used when the PIT is exhausted. In [25], some attack scenarios similar to [16] are presented and a DDoS attack mitigation technique based on Interest traceback is proposed. According to this technique, when the content source receives a bogus Interest packet, it will send the traceback message on the reverse path to notify the involved routers. The proposed solution is effective when the round-trip time (RTT) is relatively small and if the attacker does not change location (i.e., the solution is not effective against the MIFA). In [17], the Poseidon scheme is proposed, which focuses on early detection of IFA and its subsequent mitigation. The IFA mitigation is performed by reducing the data rate of the incoming interfaces. However, this approach may also degrade the performance of legitimate users and needs further enhancements in terms of user differentiation.

 ISBN: 978-1-61208-411-4

Other ICN approaches, e.g., such as PURSUIT [26], are also vulnerable to DDoS attacks but not to IFA. Contrary to NDN, PURSUIT adopts stateless data forwarding mechanism [27] and, therefore, does not suffer from attacks (such as IFA) that target soft states. In PURSUIT, the content delivery path is included in the packet header, in the form of a Bloom filter (BF). The latter, although provides time- and space-efficient path representation, suffers from the effect of false positives during the packet forwarding [28]. False positives can be exploited to launch DDoS on both network infrastructure and end users. Some of the proposed solutions include advanced encryption [29] and authentication techniques [30], in-packet BF size optimization [31], and false positives reduction [32].

VIII. Conclusion and Future Work

In this paper, we evaluate the DDoS vulnerability of NDN through simulations. In particular, we consider the IFA, where malicious users are trying to saturate the PIT and to disrupt the normal network operation. We show, that, if no adequate countermeasures are taken, it is relatively easy to cause PIT overflow and to achieve an 80% packet dropping rate. Next, we propose an IFA mitigation scheme that is based on anomalous user behaviour detection. If a user exceeds a predefined threshold it is forced to reduce its data rate or may even be blocked. This scheme is shown to be able to significantly reduce the PIT size, in terms of bogus entries, and to improve the QoE of legitimate users, in terms of packet dropping probability. Finally, we present a public-key based authentication scheme to protect the network against malicious notification messages from compromised routers. In our future work, we are planning to develop a stochastic model for PIT and to analytically determine the PIT size and the packet dropping probability.

References

[1] A. Feldmann, "Internet clean-slate design: What and why?," ACM SIGCOMM Computer Commun. Review, vol. 37, 2007, pp. 59-64.

[2] G. Xylomenos, et al., "A survey of information-centric networking research," IEEE Communications Surveys & Tutorials, vol. 16, no. 2, 2014, pp. 1024-1049.

[3] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking named content," Proc. CoNEXT, Rome, Italy, Dec. 2009, pp. 11-18.

[4] H. Yuan and P. Crowley, "Scalable pending interest table design: From principles to practice," Proc. IEEE INFOCOM, 2014, pp. 2049-2057.

[5] S. Arianfar, T. Koponen, B. Raghavan, and S. Shenker, "On preserving privacy in content-oriented networks," Proc. ACM SIGCOMM Workshop on Information-Centric Networking, 2011, pp. 19-24.

[6] C. Ghali, G. Tsudik, and E. Uzun, "Network-layer trust in named-data networking," ACM SIGCOMM Computer Communication Review, vol. 44, no. 5, 2014, pp. 12-19.

[7] M. Wählisch, T. Schmidt, and M. Vahlenkamp, "Lessons from the past: Why data-driven states harm future information-centric networking," IFIP Networking Conference, 2013, pp. 1-9.

[8] S. Choi, K. Kim, S. Kim, and B. Roh, "Threat of DoS by interest flooding attack in content-centric networking," Proc. IEEE International Conference on Information Networking (ICOIN), 2013, pp. 315-319.

[9] F. Li, F. Chen, J. Wu, and H. Xie, "Longest prefix lookup in named data networking: How fast can it be?," Proc. 9th IEEE NAS, 2014, pp. 186-190.

[10] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang, "A case for stateful forwarding plane," Computer Communications, vol. 36, no. 7, 2013, pp. 779-791.

[11] M. F. Al-Naday, A. Bontozoglou, V. G. Vassilakis, and M. J. Reed, "Quality of service in an information-centric network," Proc. IEEE GLOBECOM, Austin, USA, December 2014, pp. 1861-1866.

[12] A. Vakali and G. Pallis, "Content delivery networks: Status and trends," IEEE Internet Computing, vol. 7, no. 6, 2003, pp. 68-74.

[13] V. G. Vassilakis, et al., "A cache-aware routing scheme for information-centric networks," Proc. 9th IEEE/IET CSNDSP, 2014, pp. 721-726.

[14] B. A. Alzahrani, M. J. Reed, J. Riihijärvi, and V. G. Vassilakis, "Scalability of information centric networking using mediated topology management," Journal of Network and Computer Applications, vol. 50, April 2015, pp. 126-133.

[15] L. Wang, S. Bayhan, and J. Kangasharju, "Optimal chunking and partial caching in information-centric networks," Computer Communications, vol. 61, May 2015, pp. 48-57.

[16] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "DoS and DDoS in named data networking," Proc. 22nd IEEE International Conference on Computer Communications and Networks (ICCCN), 2013, pp. 1-7.

[17] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating interest flooding DDoS attacks in named data networking," Proc. 38th IEEE Conf. on Local Computer Networks (LCN), 2013, pp. 630-638.

[18] P. Demestichas, et al., "5G on the horizon: Key challenges for the radio-access network," IEEE Vehicular Technology Magazine, vol. 8, no. 3, 2013, pp. 47-53.

[19] J. Pan, S. Paul, and R. Jain, "A survey of the research on future Internet architectures," IEEE Commun. Mag., vol. 49, no. 7, 2011, pp. 26-36.

[20] J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "Performance evaluation of power demand scheduling scenarios in a smart grid environment," Applied Energy, vol. 142, 2015, pp. 164-178.

[21] B. A. Alohali and V. G. Vassilakis, "Secure and energy-efficient multicast routing in smart grids," Proc. 10th IEEE Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, April 2015, pp. 12-17.

[22] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," Proc. IFIP Networking Conference, 2013, pp. 1-9.

[23] A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM: NDN simulator for NS-3," NDN Project, Tech. Rep. NDN-0005, 2012.

[24] K. Wang, H. Zhou, Y. Qin, J. Chen, and H. Zhang, "Decoupling malicious interests from pending interest table to mitigate interest flooding attacks," Proc. IEEE Globecom Workshops (GC Wkshps), 2013, pp. 963-968.

[25] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate ddos attacks in ndn by interest traceback," Proc. IEEE INFOCOM NOMEN Workshop, NJ, USA, 2013, pp. 22-29.

[26] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, "Developing information networking further: From PSIRP to PURSUIT," Proc. 7th BROADNETS, Oct. 2010, pp. 22-27.

[27] P. Jokela, A. Zahemszky, C. E. Rothenberg, S. Arianfar, and P. Nikander, "LIPSIN: line speed publish/subscribe inter-networking," Proc. ACM SIGCOMM Conference on Data Communication, Barcelona, Spain, 2009, pp. 195-206.

[28] L. Carrea, A. Vernitski, and M. Reed, "Optimized hash for network path encoding with minimized false positives," Computer Networks, vol. 58, 2014, pp. 180-191.

[29] B. A. Alzahrani, M. J. Reed, and V. G. Vassilakis, "Resistance against brute-force attacks on stateless forwarding in information centric networking," Proc. ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS), Oakland, California, USA, May 2015.

[30] C. E. Rothenberg, P. Jokela, P. Nikander, M. Särelä, and J. Ylitalo, "Self-routing denial-of-service resistant capabilities using in-packet Bloom filters," Proc. European Conference of Computer Network Defence (EC2ND), 2009, pp. 46-51.

[31] B. A. Alzahrani, V. G. Vassilakis, and M. J. Reed, "Selecting Bloom-filter header lengths for secure information centric networking," Proc. 9th IEEE/IET CSNDSP, 2014, pp. 628-633.

[32] B. A. Alzahrani, V. G. Vassilakis, and M. J. Reed, "Mitigating brute-force attacks on Bloom-filter based forwarding," Proc. Conference on Future Internet Communications (CFIC), 2013, pp. 1-7.

 ISBN: 978-1-61208-411-4