Interest Flooding Attack in Named Data Networking: A Survey

Narayan Chhetry[1], Hemanta Kumar Kalita[2]

[1]Department of Information Technology, North Eastern Hill University
Shillong - 793022, Meghalaya. INDIA.
narayanchhetry@gmail.com

[2]Department of Information Technology, North Eastern Hill University
Shillong - 793022, Meghalaya. INDIA.
hemanta91@yahoo.co.in

Abstract:***Named Data Networking (NDN) is based on the principle of Content-Centric Networking (CCN) that aims to overcome the weaknesses of the current host-based Internet architecture. Like traditional networks, it is identified that NDN is also vulnerable to many security threats including denial-of-service (DoS) or distributed DoS (DDoS) and might offer avenues for new DoS/DDoS attacks. DDoS attacks can be triggered in NDN to exhaust resources within an NDN router or the content producer(s). This survey paper focuses on different types of possible distributed denial-of-service (DDoS) attacks; in particular, we address Interest flooding, where an adversary with limited resources can implement this attack and significantly impact thenetwork performance and their proposed countermeasures.***

Keywords: Named Data Networking, Interest flooding, denial-of-service.

1. Introduction

The current Internet is facing unprecedented challenges in many aspects. It has become extremely difficult to support the ever increasing demands for security, performance, reliability, social content distribution, mobility, etc. [1]. A number of research efforts have sprung up in recent years to design the next generation Internet architecture to address these challenges. One such new architecture is Named Data Networking (NDN) [2] that aims to overcome the weaknesses of the current host-based communication architecture. NDN based on the principle of Content-Centric Networking (CCN) [3], where content rather than hosts occupies the central role in the communications architecture. NDN explicitly names content (data) instead of physical locations (hosts or network interfaces). NDN is one of five research projects funded by the U.S. National Science Foundation (NSF) under its Future Internet Architecture (FIA) Program [1].

Security and privacy are two important requirements of NDN. In the past few years, denial-of-service (DoS) or distributed DoS (DDoS) attacks have grown significantly both in size and frequency, and it remains among the most critical threats on the current Internet. Therefore, NDN must provide better security against these attacks. NDN does not use host-based addressing to established the connection for communication. NDN consumers request desired data by sending Interest packets by names, and the network returns the requested Data packets following the path of Interests. It makes NDN resilience to traditional DDoS attacks, but a new type of DDoS attack can be triggered in NDN to exhaust resources within an NDN router or the content producer(s). A malicious user can attack the network by sending a huge number of Interest packets with spoofed names. These huge number of Interest consumes the bandwidth of the network and exhaust a router's memory. This type of attack is term as Interest Flooding Attack (IFA) and this paper exclusively focus on this problem and their proposed countermeasures.

This paper is structured as follows: Section II presents the overview of NDN architecture. Section III describes Interest flooding attack. Section IV analyzes the related work. Finally, Section V concludes the paper.

2. NDN Overview

NDN is an entirely new architecture whose motivation is the architectural mismatch of today's Internet architecture and its usage. However, its design principles are derived from the successes of today's Internet [4].

The hourglass architecture of Internet centers on a universal network layer (i.e., IP), which implements the minimal functionality necessary for global interconnectivity. The thin waist as can be seen in Figure 1 was the key enabler of the explosive growth of the internet by allowing both lower and upper layer technologies to innovate independently. The NDN architecture keeps the same hourglass shape as shown in Figure 1, but changes the thin waist by using data directly rather than its location.

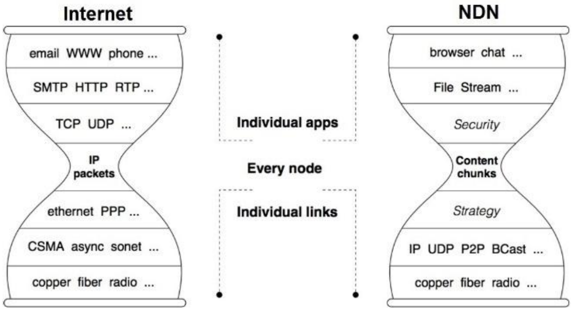

Figure1: Internet and NDN Hourglass Architectures

Communication in NDN uses two types of packets*:* *Interest* and *Data* as shown in Figure 2. A consumer asks for content by sending the *Interest packet*, which carries a name that identifies the desired data, overall available connectivities.

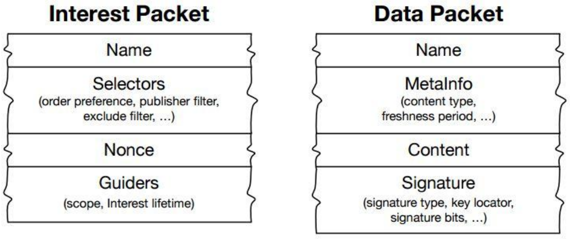
Interest Packet
Name
Selectors
(order preference, publisher filter, exclude filter, ...)
Nonce
Guiders
(scope, Interest lifetime)
Data Packet
Name
MetaInfo
(content type, freshness period, ...)
Content
Signature
(signature type, key locator, signature bits, ...)

Figure2: Packets in the NDN Architecture

Any node having data that satisfies it, a *Data packet* is sent back, which carries both the name and the content of the data, together with a signature by the producer's key as shown in Figure 2. This Data packet travels in reverse the path taken by the Interest to get back to the requesting consumer.

According to [2], each NDN router maintains following three data structures for Interest packet and Data packet forwarding.

i) ***Content Store (CS)-*** Cache of Data packets to serve subsequent Interest packets requesting the same content.

ii) ***Forward Information Base (FIB)***- Routing table of name prefixes and it guides Interests toward data producers. It is almost similar to an IP FIB except it allows for a ranked list of outgoing faces rather than a single best next-hop [5].

iii) ***Pending Interest Table (PIT)***- Table of outstanding (pending) Interest, recording the Interest's name, incoming interface(s) and outgoing interface(s). A PIT entry is created for each requested name.

When a router receives an Interest packet which is not in its cache and there are no pending Interests for the same in its PIT, the Interest is added to the PIT and according to FIB it forwards the Interest to the next hop(s). For each forwarded Interest, a router stores state information, like the Interest name and the interface on which it arrived, in its PIT. If the PIT already contains the name, the router collapses the present and any subsequent Interests and stores only the interface upon which it was received. If and when content is returned, the router forwards it out on all incoming Interest interfaces and removes the corresponding PIT entry and caches the Data in the CS [6]. As Interest and Data packets do not carry any host or interface IP addresses, Interest packets are forwarded toward data producers based on their names and Data packets are forwarded to consumers based on the state information of PIT set up by Interests at each hop [4].

A. Names

NDN names are opaque to the network (that is, routers do not know the meaning of a name) and specific to applications, which allows the naming schemes to evolve independently from the network. But they share the common characteristics; hierarchical structure and explicitly delimited components. For example, a video produced by YouTube may have the name ***/youtube/videos/ndn.mpg***, where / specifies a boundary between name components (it is not part of the name). Thishierarchical structure as shown in Figure 3 is useful for applications to represent relationships between pieces of data.

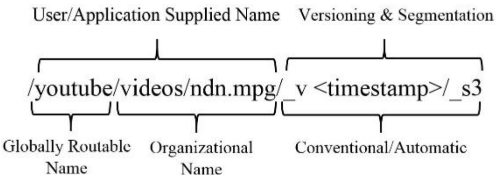
User/Application Supplied Name
Versioning & Segmentation
/youtube/videos/ndn.mpg/_v <timestamp>/_s3
Globally Routable Name
Organizational Name
Conventional/Automatic

Figure3: Hierarchical Naming

B. Security

Current IP networks security is based on where and how the data is obtained, that is, clients must retrieve content directly from the original source to trust it. NDN builds security into data itself by requiring data producers to sign cryptographically every piece of Data with its name [2].

C. Routing and Forwarding

NDN routes and forwards packets based on names.This eradicates fours IP addresses problems: address space exhaustion, Network Address Translation (NAT) traversal, mobility, and address management [4]. There is no Address exhaustion problem since the namespace is limitless. There is no NAT traversal problem since a host does not need to expose its address in order to offer content. Like IP, which needs changing addresses, mobility is not the issue in NDN because data names remain the same during the communication. Finally, address assignment and management is no longer required in local networks.

NDN Routing can be done similar to today's IP routing. Instead of announcing IP prefixes, NDN router announces name prefixes that cover the data that the router is willing to serve. Routers simply treat names as sequences of opaque components and do component-wise longest prefix match of the name in a packet against the FIB. For example, ***/youtube/videos/ndn.mpg*** may match both ***/youtube/videos*** and ***/youtube*** in the FIB, but ***/youtube/videos*** is the longest prefix match. Conventional routing protocols, such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP), can be adapted to route on name prefixes. However, research is going on Named-data Link State Routing (NLSR) protocol [7] and development of efficient data structures and algorithms for fast lookup of variable-length, hierarchical names [4].

3. Interest Flooding Attack

An adversary can take advantage of two features unique to NDN, namely CS and PIT, to mount DDoS attacks [8]. We focus on attacks that exploit the PIT, which keeps track of the unsatisfied Interest packets traversing a router, as well as their arrival interfaces. The adversary uses a large set of zombies, which are possibly geographically distributed, to generate a large number of Interest packets with spoofed name as shown in Figure 4 aiming to (1) overwhelm PIT table in routers, preventing them from handling legitimate Interests and (2) swamp the target content producers [9]. Once the PIT is full,all subsequent incoming interests are dropped as there is no memory available to create PIT entries for new incoming interests. Since the names are spoofed, no Interest packets will be satisfied by the content. These

Interest packets will stay in the PIT for as much time as possible, which will certainly exhaust memory and computing resources on routers. This is the goal of Interest flooding attack.

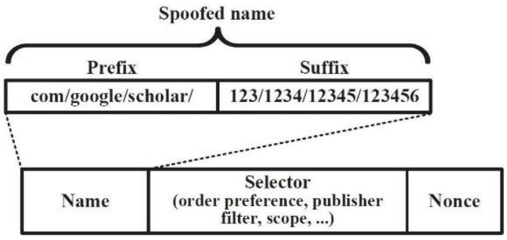

Figure4: An Interest packet with spoofed name: a legitimate prefix concatenated with a forged suffix

Figure 5 shows an example of Interest flooding attack where attacker starts Interest flooding attack and the PIT of the NDN router on the Interest forwarding path is filled with attacker's Interest. As a result, when a legitimate consumer request the content, the router on the path of Interest flooding drops the Interest since the PIT is full and it cannot create PIT entries for new incoming Interests.

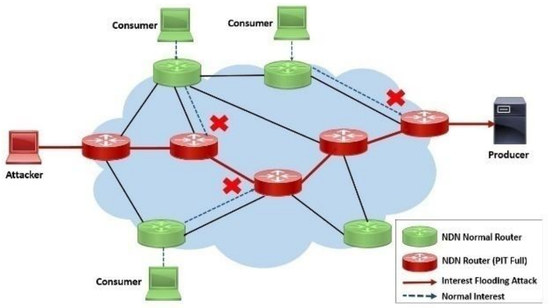

Figure5: Example of Interest flooding attack

As observed in [9], based on the type of content requested, there are three types of Interest flooding attack:

i) ***Existing or Static Content***- The impact of this attack is quite narrow since content caching of NDN provides a built-in countermeasure. If several zombies from different paths generate a large number of Interest packets to attack a producer. After the initial attack, the content settles in all intervening routers' caches. Subsequent Interest packets for the same content cannot propagate to the producer(s) since they are satisfied by cached copies.

ii) ***Dynamically Generated Content***- Since requested content is dynamic, all Interest packets are routed to content producer(s), thus consuming bandwidth and router PIT table. The result of this attack is that the producer may getoverloaded with malicious Interests, and unable to handle requests from other legitimate consumers. The router which is closer to the producer has the greater effect on its PIT.

iii) ***Non-existent Content***- In this attack zombies generate distinct and unsatisfiable Interests for a non-existent content, which means these names cannot match any FIB entry in routers. Therefore, these Interest packets are duplicated and propagated throughout the entire network until they reach the hosts at the edge of the network. On one hand, duplicating such a great amount of Interest packets cost a lot of computing resources; on the contrary, without responding Data packets, these Interest packets will stay in the PIT for as much time as possible, which will certainly exhaust memory and computing resources on routers, degrading routers' performance, or even making them crashed.

4. Related Works

In this section, we present various proposed countermeasures of Interest flooding attack by researchers and analyze those countermeasures. We aim to provide readers a better understanding of Interest flooding attacks and its countermeasures. Gasti et al. [9] performed analysis of NDN's resilience to DDoS attacks and discussed two types of attacks with their effects and potential countermeasures (Router Statistics and Push-back Mechanisms). However, the paper does not analyze DDoS attacks and their countermeasures. Afanasyev et al. [10] proposed three mitigation algorithms (token bucket with per-interface fairness, satisfaction-based Interest acceptance, and satisfaction-based pushback) that allow routers to exploit their state information to stop Interest flooding attack. Among these three mitigation algorithms, satisfaction-based pushback mechanism could effectively shut down attackers and ensure that almost all the Interests from legitimate users are satisfied. This work uses a simple and static attackers model, and it does not consider intermediate router's cache and always forwards all the way to the producer [8]. Compagno et al. [11] proposed a framework, named Poseidon, for mitigation of local and distributed Interest flooding attack for non-existing contents. Authors simulated a simple attackers model, and their countermeasure has been able to use around 80 - 90 % of the available bandwidth in the most cases during the attacks. Dai et al. [13] proposed Interest traceback as a countermeasure against DDoS attacks by generating spoofed Data packets to satisfy the long-unsatisfied Interest packets in the PIT by tracing back to the Interest originators. According to [8], this method is not proactive, makes overhead in the network by increasing made spoofed contents. Another shortcoming is that it assumes long-unsatisfied Interests in the PIT is adversary and others unsatisfied Interest are normal usages. Due to which the router drops the incoming packet rate of the interface that has too many long-unsatisfied Interest packets. As a result of this independent decision, the probability of legitimate Interests being forwarded decreases from that interface. Choi et al. [14] provided an overview of threats of Interest flooding attack for non-existent contents on NDN. Authors simulated and explained the effect of Interest flooding DDoS attacks on the quality of services. However, they do not analyze DDoSattacks and their countermeasures. Karami et al. [8] introduced an intelligent hybrid algorithm for proactive detection of DDoS attacks and adaptive reaction for mitigating. In the detection phase, a combination of multi-objective evolutionary optimization and Radial Basis Function (RBF) neural network has been applied. After constructing the intelligent hybrid classifier (predictor) module, an adaptive reaction mechanism by enforcing explicit limitations against adversaries was proposed to mitigate potential DDoS attacks in NDN.

In Table I, we summarize all countermeasures of Interest flooding attack described in this section.

5. Conclusion

NDN which is one of the promising architecture for future internet, tries to provide better security and privacy support than the current host based internet. Though traditional DDoS attacks in NDN does not have much effect, its more advanced architecture introduces novel attack opportunities. In this paper, we have presented a specific instance of DDoS attacks namely, Interest flooding. We have provided a snapshot of the current state of the art of research in Interest flooding attack. We discussed existing solutions and analyzed those solutions. Perpetrators exploit NDNs Interest packet forwarding rule to send out Interest packets with spoofed names and makes these interest packets as attacking packets. We investigated that the victims of Interest flooding attack is not only the hosts, but also the PIT within routers. However, we find that the PIT is the largest target. In Interest flooding attack, a great amount of Interest packets resides in the routers which exhaust memory and computing resources on routers, degrading routers' performance, or even making them crashed. As NDN is a new Internet architecture proposal, there are very limited research work going for mitigation of Interest flooding attack. Hence, there is a need for detail security analysis before they are actually deployed.

TABLE I: Summary of countermeasures of Interest flooding attack

Authors	Proposed Countermeasures
Gasti et al. [9]	Proposed two type of countermeasures: a) **Router Statistics** can be used to maintain flow balance between Interests and Contents. Routers can limit the total number of pending Interests for a prefix which is under attack and control incoming interface(s) which has sent too many unsatisfied Interests for that prefix. b) **Push-back Mechanisms** to trace back to the source of attack and isolate the attack right at source
Afanasyev et al. [10]	Proposed three mitigation algorithms: a) Token bucket with per interface fairness where Interests forwarded by a router on each interface represent a fair combination of Interests received from neighboring nodes. b) Satisfaction-based Interest acceptance where Interest satisfaction ratio, the ratio of number of forwarded requests to number of satisfied requests, is simply calculated and use to make a decision to forward or avoid the incoming Interest. c) Satisfaction-based pushback where the incoming Interest limit is set by each router in proportion to the calculated Interest satisfaction ratio. Moreover, the router announce this limit to their downstream routers so that they can reconfigure their own Interest acceptance limits in accordance with the announced limit of the upstream node [12].
Compagno et al. [11]	Proposed a framework, named Poseidon, for mitigation of local and distributed Interest flooding attack for non-existing contents with push-back alert mechanism.
Dai et al. [13]	Proposed Interest traceback using spoofed Data packets to satisfy the long-unsatisfied Interest packets in the PIT by tracing back to the Interest originators.
Choi et al. [14]	Presented an overview of threats of Interest flooding attack for non-existent contents and explained its effect on the quality of services.
Karami et al. [8]	Proposed a two-phase framework for mitigating Interest flooding attack in NDN. The first phase being proactive detection and the second one adaptive reaction. In the detection phase, a combination of multiobjective evolutionary optimization and RBF neural network has been applied. The second phase proposed an adaptive reaction mechanism by enforcing explicit limitations against adversaries.

References

[1] J. Pan, S. Paul, and R. Jain, "A survey of the research on future internet architectures," Communications Magazine, IEEE, 2011.

[2] 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," Relat´orio T´ecnico NDN-0001, Xerox Palo Alto Research Center-PARC, 2010.

[3] V. Jacobson, M. Mosko, D. Smetters, and J. Garcia-Luna-Aceves,“Content-centric networking,” Whitepaper, Palo Alto Research Center, pp. 2–4, 2007.

[4] 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.

[5] 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, pp. 1–12.

[6] C. Ghali, G. Tsudik, and E. Uzun, “Elements of trust in named-data networking,” ACM SIGCOMM Computer Communication Review, ACM, vol. 44, no. 5, pp. 1–9, 2014.

[7] A. Hoque, S. O. Amin, A. Alyyan, B. Zhang, L. Zhang, and L. Wang, “NLSR: Named-data link state routing protocol,” in Proceedings of the 3rd ACM SIGCOMM Workshop on Information-Centric Networking, ACM, 2013, pp. 15–20.

[8] 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.

[9] 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), July 2013, pp. 1–7.

[10] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, “Interest flooding attack and countermeasures in named data networking,” in IFIP Networking Conference, May 2013, pp. 1–9.

[11] 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, Oct 2013, pp. 630–638.

[12] 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.

[13] 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, April 2013, pp. 381–386.

[14] 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), Jan 2013, pp. 315–319.

Author Profile

Narayan Chhetryis Research Scholar at Department of Information Technology, North Eastern Hill University, Meghalaya, India. He has acquired MCA degree in the year 2007 from Dibrugarh University. His areas of research interest are Network Securities, Future Internet Architecure,etc.

Hemanta Kumar Kalita is working as Associate Professor and Head of Department of Information Technology of North Eastern Hill University, Shillong, India. He has received Ph.D. from Jadavpur University, Kolkata, India. He has six years of industry/R&D experience and around eleven years of teaching experience in both under graduate and post graduate level. His areas of research interest are Big Data Analysis, Adhoc Network Security, Performance Engineering, Spatial Data Mining, Artificial Intelligence, etc. He has one patent to his name and published several papers in International and National Journal and Conferences. He has received FOSS INDIA AWARD in 2008 awarded by LINUX FOR YOU magazine for his contribution to open source in WANem project