Current and New Types of DoS Attacks in Named Data Networking Architecture

Hardik Prajapati

Department of Electronics & Communication
Indus University, Ahmedabad, Gujarat

Abstract—As telecommunication and Internet are becoming an integrated system, user demand is continuously increasing. The forty years old internet has reached its threshold and the current IP based host centric Internet architecture needs to be replaced by an architecture which provides better solution to manage mobility, QoS, Security. Content-Centric Networking is an emerging networking architecture and specific candidate for next generation Internet, which focuses on content distribution which was not served efficiently by IP[1]. Named Data Networking is an example of CCN, a research project under the NSF Future Internet Architectures program[2]. In last few years DDoS attacks have become major threat for current Internet. Resilience to Distributed Denial of-Service (DoS) attacks that plague today’s Internet is a major issue for any new architecture and deserves full attention. In DDoS packets from large number of compromised hosts are sent to victim’s network which overloads the network. In NDN, end users requests the desired data by sending a request and the data producer sends back the requested data upon request only, eliminating existing DDoS attack. In this paper I have shown how NDN architecture’s inherent properties tackle current DDoS attacks and new types of DoS attacks.

Key words: Future Internet; Content Centric Networks; Named Data Networking; Denial of Service; Distributed Denial of Service

I. INTRODUCTION

The current Internet based on IP was designed for conversation between endpoints but since then the world has changed drastically and today content distribution is overwhelming [1]. Instead of communicating between computers, users are demanding large amount of data for entertainment, online shopping, business, banking etc. The internet was neither designed nor expected to support large bandwidth and throughput requirements like store forward email, video streaming and remote computer access [3]. To keep the Internet up and live in future, number of research program to design new Internet architecture have been initiated.

NDN is one of five projects funded by U.S. National Science Foundation under Future Internet architecture program [2]. NDN architecture is based on Content Centric Networking paradigm, which shifts host centric architecture to a data-centric architecture. NDN uses name of content (data) instead of location (source or destination address). NDN architecture supports security by digital signature for each packet generated by data producer. It also offers content store to optimize bandwidth and efficient use of network.

A. DoS and DDoS:

In December 2014 an ISP experienced an NTP reflection DDoS attack that peaked at a router-straining 400Gbps, the largest denial of service event in Internet history [6]. On 31st Dec, 2014, Scandinavian banks had a few days of disruption to online services and processing of bank card transactions due to DDoS attacks[7]. Day by day the list of services affected by these attacks is growing and costing millions of dollars.

In DOS (Denial Of Service) attack, the attacker floods the computer or entire network by malicious requests in such a way that the resources or services provided by the affected network are unavailable or delayed for legitimate users. A DoS attack is when an attacker utilizes a single machine to deplete the resources of his target machine so that it becomes out of order. This attack can be generated in several ways like SYN flooding, Ping of death, Smurf attacks, HTTP flooding, NTP Amplification. There are many software tools available which make servers strong enough to resist DoS attack form a single machine.

So attackers carry out DDoS attacks to increase effectiveness of DoS attack. DDoS is an amplified version of DoS in which an attacker utilizes multiple distributed compromised computers. Attackers infect hundreds or thousands of computers by their vulnerabilities to gain unauthorized control over these machines[8]. These compromised machines are called as “zombies” and the attacker can use them as an army to paralyze one machine or entire network. These attacks are considered as the most destructive attacks but very simple to generate and difficult to detect.

Various forms of DDoS attacks have created major problem against current Internet, so it’s very critical for Future Internet to provide robust solution for these vulnerabilities. A DDoS attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. It also creates bandwidth depletion so legitimate users are not able to access the network.

II. NDN OVERVIEW

Communication in NDN is driven by data consumer [3]. All communication in NDN is done by using two packets, request and data packet. When a consumer wants to access any data, it has to send a request called Interest packet which carries name of the required data. For example a consumer may request youtube/ndn videos. The gateway router makes entry of a interest packet received on the interface and forwards towards data producer by looking the name in its Forward Information Base (FIB). As this interest packet reaches to a router that has the required data, it sends back the data packet with a signature key of data producer to a consumer on the reverse path of interest packet. A content packet will never be forwarded to any machine unless interest is received for that packet.

NDN router has to maintain three components:

- Interest Routing Table (IRT)
- Forwarding Information Base (FIB)
- Interest Data Base (IDB)
A. Forward Information Base (FIB):
Similar to routing table, it contains name prefixes and outgoing interface where Interests can be forwarded.

B. Pending Interest Table (PIT):
A table containing all “not satisfied” interests that have been sent upstream towards the data source and their corresponding incoming one or more interfaces.

C. Content store (CS):
Stores data packets temporarily, allowing efficient data retrieval by different consumers. Both IP router and NDN router buffer data packets, only the difference is NDN router can reuse the data after forwarding and conserve bandwidth.

When a router receives an Interest packet, first it checks the content store whether the request data is present in the buffer or not. If data is present it forwards the matching data to the incoming interface from the request was received. If matching data is not found in CS the PIT is checked, whether request for the same data is present or not, if the name already exist the request is dropped and only incoming interface from which the request is receive is stored in PIT. If the same requested name is not present in PIT entry the request is added into PIT and forwarded to the next hop according to FIB. When content is returned, the router forwards to all interfaces from which it was requested and removes corresponding entries from PIT. Since the data packet follows the reverse path of the interest packet no additional information like “source address” is required. If for a particular interest a router cannot forward it further, or a content producer has not such data, no error packets are generated and the request is discarded.

In NDN, security is built in to data, rather than function of from where and how it is fetched [9]. It is mandatory for contents to have digital signature for authenticity and integrity of data producer. The signature, coupled with data producer information enables determination of data source and whether a public key owner is an legitimate publisher for particular content or not. Public keys are treated as regular data, and as all content is signed, each public key is a simple “certificate”.

III. NDN and CURRENT DOSS ATTACKS
In this section I show how NDN tackles the current DoS/DDos attacks. The unique features, Content Store and PIT makes difficult to generate these attacks. DoS has wide range of attacks targeting different protocols, network resources and applications. A typical DoS attacks is comprised of three elements: (1) a set of zombies under control of master node or nodes, (2) master node/nodes, (3) targeted victim hosts/routers.

A master node/nodes remotely exploits software vulnerabilities and inject malware into one or more hosts and create them in zombies. In IP, it’s relatively easy to exploit unpatched hosts because it uses source and destination address. NDN makes this almost impossible, because hosts are not directly addressable [10].

I now discuss and compare some popular types of DoS attacks in TCP/IP based Internet and NDN.

A. Bandwidth and Resource Depletion:
To saturate bandwidth and network resources in IP based network, the adversary generates DoS attacks like TCP flooding, UDP flooding, HTTP flooding, Ping flooding. This process deCELERates system’s performance, causes system crash by flooding network bandwidth and prevents the legitimate users to access the system.

Similar type of attacks can be launched against NDN by making zombies to request particular data contents from a certain victim. But this attack will not cause much damage to the network, as the data contents are fetched from the producer it will be stored in CS of the router, so if the request comes again the router itself satisfies by sending content from CS. Even if many zombies are requesting data content on multiple interfaces, only one request is forwarded to next router and making remaining interfaces’ entry in PIT. So as the content is received it will be forwarded back to all interfaces on which the request was received. Like this the network itself limits the number of generated interests weather legitimate or malicious reaching the targeted victim [10].

B. Reflection Attacks:
This type of attack involves three entities: the adversary, reflectors and victim host. In this type of attack the adversary floods the victim network or host. The adversary forges the IP packets, it replaces its own source address with address of targeted victim’s address and sends these packets to the reflectors. Responses to these packets are not sent back to adversary but the victim and saturates it’s network.

NDN is resilient to this attack because the data content follows the reverse path established by the interest. However and NDN router can broadcast an incoming interest on some or all of its interfaces. On contrary even if each hop broadcasts the interest the maximum number of content copies a consumer can receive is bounded by the number of interfaces, not by the number of entities that receive the interest. The reflection attack turns out to be effective only when the adversary and the victim are in the same physical network.

C. Black – Holing and Prefix Hijacking:
In prefix hijacking, compromised or malicious router advertises invalid route entries to motivate other routers to add these entries in their routing table. This type of attack is called “black holing” attack, where all traffic is routed via malicious routes and eventually discarded. It’s very effective in IP network as once the route is advertised, the router itself can not identify weather this route is legitimate or not.

NDN offers better solution to black-holling implemented by prefix hijacking. NDN routers contain more information than IP routers, which makes possible to detect any irregularity in content distribution. As the symmetric path is adopted each content follows the same reverse path as the interest that requested it, the router uses the numbers of unsatisfied requests to identify prefix hijacking. Routers also maintain statistics of satisfied and expired entries of each link and interface with respect to a particular prefix and change their FIB according to this statistics.
D. DNS Cache Poisoning:
DNS server is backbone for current Internet, as it translates the ip address to human readable and vice versa. To make efficient use of this service, DNS stores the output of previous requests in cache. In DNS cache poisoning, the adversary corrupts the cache by inserting malicious entries in order to control the server’s response for particular set of DNS names.

In NDN, the name resolution in DNS server is not required as the packet name is routed directly instead of converted to IP addresses.

IV. NEW DOS ATTACKS
Even if their ineffectiveness and lack of impact, variations of mentioned DoS attacks may cause serious problems against NDN.

NDN has advantage over current Internet due to two important features, PIT entries and the use of content store. In following section I discuss two new attacks affecting NDN- Interest flooding and content poisoning.

A. Interest Flooding Attacks:
In IP network SYN flooding is very well known type of attack, which is not possible in NDN but almost same effect can be generated by interest flooding. The difference between SYN flooding and interest flooding is the victim: the primary victims in interest flooding are routers whereas in SYN flooding it’s end hosts. Routing of content and interests is performed according to PIT’s entries. The adversary can take advantage of this method to generate an effective DoS attacks, known as interest flooding in NDN. The adversary controlled zombies generate a large volume of interests that saturate the victim router’s PIT. If the rate of entries satisfied/removed from PIT is lesser than the incoming interests, once the PIT is completely full all subsequent incoming interests (whether legitimate or compromised) are dropped. This is the goal of interest flooding attacks.

Interest flooding attack in NDN can be mount by three techniques. The adversary can generate closely-spaced interests for: (1) existing static content, (2) dynamically generated content, or (3) non-existing/fake content [10]. In type (1) the adversary overwhelms the router by sending requests for distinct contents. If the flooding rate is very high, the producer starts dropping packets. If the victim’s capacity to satisfy these interest is lacking this strategy may cause damage. Network caching content feature can give some relief, after initial wave of interests from adversary, content is stored in cache of all routers. So all following interests for same request will be satisfied by router and not propagated to data producer.

Type (2) is similar to (1) except that contents are never returned from cache, and this strategy can cause more damage. To make interest flooding effective it is important to: (a) the requests are routed to data producer as close as possible and (b) new PIT entries are created for these interest and stored in NDN routers as long as possible. Strategy (2) satisfies both these conditions, as the requests are dynamic the intermediate routers don’t have contents in their caches, due to this all requests are routed towards data producer. All interests requesting the same content are combined into one PIT entry but each distinct request will result in one individual PIT entry. And as these requests are dynamic will be forwarded to the content producer and they will remain in PIT until satisfied. The result of these attacks is the producer waste resources to satisfy compromised interests rather than legitimate.

In strategy (3) the by generating requests for non-existing contents, the adversary creates entries in victim’s PIT entries for which no content will ever be returned. These requests are stored in PIT until they are satisfied or expire. If the incoming fake requests rate is higher than the expiring rate, PIT will be exhausted and after that all incoming requests will be dropped. So if the adversary performs DDoS attack by generating dynamic fake entries, network performance degrades at alarming level.

V. INTEREST FLOODING MITIGATION METHODS
The mitigation strategies vary according to level of complexity and effectiveness, the higher the implementation complexity the higher effectiveness against interest flooding attacks. Interest flooding attack results by flooding compromised requests, so the simplest solution to this attack is restrict the number of interests forwarded to data producer. One of the features of NDN is – flow balance between Interest and Data packet. This allows intermediate routers to control the inbound traffic by controlling the number of outstanding interests in the network. One simple solution is to limit the number of forwarded interests out of each interface based on the capacity of each interface [11]. In this method NDN router keeps track of the incoming interests and after the limit has been reached, it stops to forward new incoming requests. The biggest drawback of this algorithm is it may serve the purpose of DDoS, if a router has reached it’s limit to forward malicious interests it stops forwarding interests from legitimate users till the malicious interests expire. One way to solve this issue is to impose a per interface fairness, so that malicious Interests are not allowed to entirely consume the limits of a specific interface.

A. Setting Limit of Forwarded Requests per Interface:
In this strategy, the interests forwarded by a router on each interface must be fair mix of interests received from adjacent nodes. To achieve this strategy, interests should not be sent immediately, there should be fair mixing of interests from different interfaces. This mechanism is essentially a class based queuing [12], with classes for each outgoing and incoming interface. Unlike normal queuing, Interest queues do not actually store a packet, but bi-directional pointer to the existing PIT entry. Thus, a PIT entry can be quickly updated when the Interest is actually forwarded, and the element can be easily removed from the queue when the Interest expires. By setting appropriate queue size, the amount of recourses utilize at a router can be controlled.

This algorithm provides a partial relief from Interest flooding attacks, and allows legitimate users to successfully retrieve data for 15-20% of their interests. This algorithm provides reasonable fairness in an NDN network and ineffective in protecting legitimate users. The main drawback of this method is it still satisfy relatively large number of interests from malicious users. This algorithm attempts to ensure that each interface does not forward more than its fair share of Interests, but in doing so, it drops both
legitimate and malicious Interests both. It fails in identifying and differentiating between malicious and legitimate users. So it’s very important to devise a method which allows router to differentiate between good and bad interests.

B. Decide Based On Router Statistics:
The above strategy solves the threat of DoS only if it is able to distinguish between malicious and legitimate interests. One unique feature of NDN architecture, symmetric flow of interests and data packets resolves this issue [11]. As data packet is routed through reverse path of the corresponding interest, a router can maintain the status of each request that weather the interest resulted in matching data content or expired. This statistics helps the NDN router to differentiate between attack and legitimate traffic. One major problem in this method is router can’t decide whether to forward or discard particular request until it’s forwarded.

However, routers can maintain up-to-date statistics of how many interest request are forwarded and how many are satisfied. Based on this it can decide whether to forward or discard. If router maintains statistics per incoming and outgoing interface, name prefix of the interest that can improve the prediction. The ultimate goal of the router is to satisfy the legitimate interests and drop attacks as fast as possible. If all requests are legitimate the percentage of unsatisfied interests is zero, as the attack starts the router starts to build the statistics rapidly. And when the percentage of unsatisfied interest reaches 100% router starts to drop all request packets.

C. Interest Acceptance/Rejection Based On Individual Router Statistics:
As stated above, each router will decides to forward the request packet based on the request satisfaction ratio. A drawback of this method is each router will take it’s decision based on it’s own statistics only [10]. And if the number of hops between the consumer and data producer is more, the probability of forwarding the request will decrease. As an example, if there are three hops between consumer and data producer and the interest satisfaction ratio is for router 1 is 40%, router 2 is 50% and router 3 is 60% then, the request has only 12% probability that it will be forwarded. To avoid such high rejection ratio, the decision taken by each router should be dependent of the decision taken at preceding routers.

D. Pushback Mechanism:
In the satisfaction based interest acceptance strategy, the number of interests forwarded by a router depends on interest satisfaction ratio [10]. In pushback mechanism, the data producer sets the limit of interests and based on the interest satisfaction ration of routers the producer distributes that how many interests can be forwarded by each interface of the router. As shown in fig1. the limit L of the data producer is 20. The current satisfaction ratio for eth0 interface of router A is 50% and for eth 1 is 0%. For router B the ratio is 30% for eth0. Now as the limit decided by producer is 20, router B will set and announce incoming interface limit 30% x 20= 6. Router A receives the limit from router B and sets limit for eth0 to 3 and eth1 to 0. Based on this statistics eth 1 of router A is under attack and not forward any request until the satisfaction ratio improves. This pushback mechanism improves the satisfaction ratio on both routers and gradually they are able to utilize full incoming interest limits.

For Future Internet, it’s very important to have detection and prevention methods for the security threats which are destructing current IP based network. The DoS attacks have become smarter and the methods are more complex, which makes very difficult to detect them. In this scenario the Internet desperately needs novel architecture which can withstand against these attacks. The roots of DoS attacks are in IP address, as the addresses are known the attacker easily manipulates software vulnerabilities and security hole of a machine. In NDN all communication is performed on basis of interest and data packets, so it is equipped with remedy to most of the current DoS attacks. But in NDN also the purpose of DoS can be served by generating large numbers of fake and dynamic requests. Based on successful completion of consumer’s requests, routers can maintain statistics of failed and succeeded requests. These statistics can be used as benchmark to decide whether to forward or block request. So one protocol is required by which routers can share their statistics with each other and based on the aggregate information decision should be taken.

REFERENCES


