2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)

Self-Adjusting Share-Based Countermeasure to Interest Flooding Attack in Named Data Networking

Cong Pu, Nathaniel Payne, and Jacqueline Brown
Weisberg Division of Computer Science
Marshall University
Huntington, WV 25755, USA
{puc, payne219, brown1062}@marshall.edu

***Abstract*—Due to the rapid growth of Internet traffic, increasing mobility, and stronger security requirements, today's Internet shows signs of aging. To keep pace with changes and move the Internet into the future, Named Data Networking (NDN), a future Internet architecture, was proposed and has been demonstrated as a viable architecture for content distribution and widely recognized as a promising architecture for future Internet. However, NDN is not originally designed to consider the security requirement for all potential attacks, thus, NDN is vulnerable to a well-known Distributed Denial-of-Service (DDoS) attack that primarily targets service availability by flooding the network and obstructing the service received by legitimate users. In this paper, we propose a self-adjusting share-based countermeasure, also referred to as *SSC*, against Interest flooding attack in NDN, where the attacker issues an excessive number of non-satisfiable Interest packets to drop legitimate Interest packets by overwhelming Pending Interest Table in NDN routers. In the *SSC*, each router maintains an Interest unsatisfaction ratio and dynamically adjusts the share of forwarded Interest packets for each incoming interface accordingly. In addition, the Interest packets that pass the assigned share of forwarded Interest packets are used as scouts to investigate unknown paths to complement routing information. We conduct extensive simulation experiments for performance evaluation and comparison with the existing constant share based approach. The simulation results show that the proposed countermeasure can not only improve the Pending Interest Table utilization ratio of legitimate Interest packets, but also reduce the number of accepted malicious Interest packets, indicating a viable approach against Interest flooding attack in NDN.**

***Index Terms*—Network Security, Named Data Networking, Interest Flooding Attack, Distributed Denial-of-Service Attack**

I. Introduction

Today's Internet is a unique and unprecedented global success story, connecting hundreds of millions of users all over the world. However, core ideas behind the design of today's Internet were developed in the 1970s, when telephony, a point-to-point conversation between two entities, was the only successful example of effective global communication technology. Today, the way people access and utilize the Internet has changed dramatically since the 1970's, and communication and network paradigm of Internet has shifted from the connections between two entities to the global content distribution and content retrieval. Unfortunately, due to the rapid growth of Internet traffic, increasing mobility, stronger security requirements, new service and application as well as different usage models, today's Internet shows signs of aging. To keep pace with changes and move the Internet into the future, Named Data Networking (NDN) [1], a future Internet architecture, was proposed and has been demonstrated as a viable architecture for content distribution and widely recognized as a promising architecture for future Internet.

NDN is based on the principle of information-centric networks [2], where content (or data), rather than physical locations (or hosts), occupies the central role in the communication architecture. NDN also stipulates that each piece of content must be digitally signed by its producer to realize the goal of "security by design", which allows for decoupling of trust in content from trust in the entity that might store and/or disseminate that content. These elegant features facilitate caching of content to optimize bandwidth use and enable effective simultaneous utilization of multiple network interfaces. However, NDN was not originally designed with the consideration of the security requirements to defend against all potential cyber attacks, as a result, NDN is definitely vulnerable to a well-known Distributed Denial-of-Service (DDoS) attack that primarily interrupts service availability by flooding the network and obstructing the service received by legitimate users [3], [4].

In this paper, we investigate an Interest flooding attack and propose its corresponding countermeasure in NDN, where the attacker issues an excessive number of non-satisfiable Interest packets to drop legitimate Interest packets by overwhelming Pending Interest Table in NDN routers. The Interest flooding attack primarily targets the vulnerabilities of Interest forwarding mechanism in NDN by violating an implicit assumption, i.e., all routers faithfully and collaboratively route the Interest packets towards data sources. Unlike a traditional flooding-based DDoS attack, where a large number of compromised hosts are amassed to send useless packets to jam a victim or its Internet connection, it is a nontrivial problem to detect and differentiate to some extent malicious Interest packets from legitimate ones. Thus, we propose a lightweight countermeasure integrated with other corresponding techniques against Interest flooding attack in NDN, where its security resiliency and performance trade-off are measured through extensive simulation experiments. The contribution of this paper is summarized in the following:

- We propose a self-adjusting share-based countermeasure,

978-1-7281-2980-8/19/$31.00 ©2019 IEEE
DOI 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00045

also called *SSC*, against Interest flooding attack in NDN. In the *SSC*, each router maintains an Interest unsatisfaction ratio and dynamically adjusts the share of forwarded Interest packets for each incoming interface accordingly. In addition, the Interest packets that pass the assigned share of forwarded Interest packets are used as scouts to investigate unknown paths to complement routing information.

- We present the basic operations of NDN forwarding plane, analyze its potential vulnerabilities, and investigate the performance impact of Interest flooding attack with a preliminary result. For performance comparison, we modify and implement a prior constant share based approach to work in our simulation framework.

We develop a customized discrete event-driven simulation framework by using OMNeT++ [5] and evaluate its performance through extensive simulation experiments in terms of Pending Interest Table utilization ratio and the number of accepted Interest packets. The simulation results show that the proposed countermeasure can not only improve the Pending Interest Table utilization ratio of legitimate Interest packets, but also reduce the number of accepted malicious Interest packets, indicating a viable approach against Interest flooding attack in NDN.

The rest of the paper is organized as follows. Prior schemes and mechanisms are presented and analyzed in Section II. In Section III, the basic operations of NDN stateful forwarding plane and its potential vulnerabilities are summarized and analyzed with a preliminary result. The proposed self-adjusting share-based countermeasure is presented in Section IV. Section V focuses on simulation results and their analyses. Finally, concluding remarks are provided in Section VI.

II. Related Work

Even though Named Data Networking is a newly proposed Internet architecture, it has attracted a significant amount of attention from the security community. In [6], a Gini impurity based detection mechanism is proposed to measure the dispersity of the requested Interest names in an NDN router, and then detect potential Interest flooding attack. When there is no attack in the NDN network, the Gini impurity of the Interest names varies in a normal range, since the Interest requests have a relative stable distribution. However, when the attackers start to send malicious Interest to the network, the Gini impurity of the Interest names will be influenced and exceed the normal range. The [7] proposes an Interest flooding attack detection scheme based on cumulative entropy by monitoring the content request abnormal distribution and then provide the malicious prefix identification method by relative entropy theory. In addition, an Interest traceback countermeasure is also used to restrain the attacker after detection. In [8], an advanced Interest flooding attack that mimics real content names and varies the attack characteristics over time in order to remain undetected by routers is designed to reassess the most effective state-of-the-art countermeasures. The evaluation shows that those countermeasures fail to cope with the novel attack model and that different countermeasures need to be designed as future works.

The [9] proposes a coordinated defense mechanism against Interest flooding attack based on their previously proposed coordinate caching-related decisions in NDN, where a few routers that are selected by a novel heuristic observe the entire traffic at an early stage and aggregate the knowledge of traffic and forwarding states to detect Interest flooding attack. The [10] first analyzes the traffic model of collusive Interest flooding attack that is mostly concentrated in the low frequency bands, and then proposes a detection scheme to warn the collusive Interest flooding attacks based on the wavelet analysis of the Interest packets collected on each router with low computational complexity and high accuracy. In [11], NDN forwarding daemon operations are first analyzed, and then a monitoring plane design that captures the state of NDN routers by instrumenting 18 metrics with dedicated probes are presented. Through correlating these metrics with a Bayesian network, the potential abnormal behaviors, such as Interest flooding attack, can be detected. The [12] introduces Poseidon, a new mechanism for detecting and mitigating Interest flooding attack. Poseidon relies on both local metrics and collaborative techniques for early detection of Interest flooding attack. First, routers rely only on local metrics to identify an attack. Then, nearby routers collaborate to determine whether an attack is in progress and mitigate it.

In summary, most of prior Interest flooding attack detection mechanisms rely on Interest satisfaction ratio to determine whether an incoming Interest packet should be forwarded or dropped. However, little attention has been paid to a countermeasure that maintains an Interest unsatisfaction ratio, dynamically adjusts the share of forwarded Interest packets for each incoming interface accordingly, and uses the Interest packets that pass the assigned share of forwarded Interest packets as scouts to investigate unknown paths to complement routing information.

III. NDN Forwarding Plane Overview and Interest Flooding Attack

In this section, we briefly review the basic operations of NDN forwarding plane, analyze its potential vulnerabilities, and present the Interest flooding attack with a preliminary result.

A. Overview of NDN Forwarding Plane

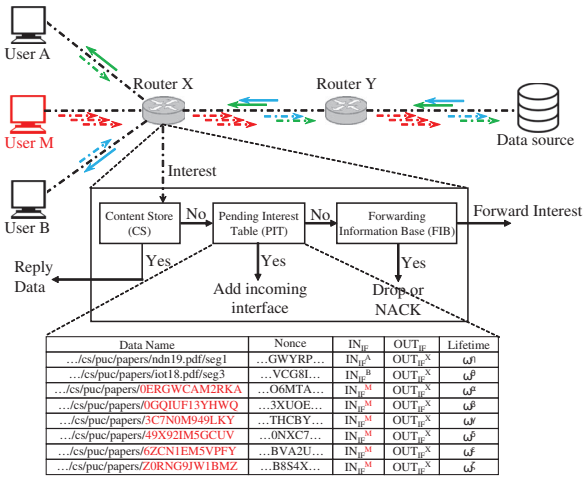
In NDN, all communications are performed by using two different types of packets, *Interest* and *Data*, both of which carry a name to uniquely identify a piece of data in the packet. Names in NDN have a hierarchical structure which is composed of one or more components. For instance, an example name for the first segment of author's paper would look like */marshall.edu/cs/puc/papers/ndn2019.pdf/seg1*. In order to retrieve data, a data consumer sends an Interest packet piggybacked with the name of desired data to the network. Routers use the piggybacked data name in the Interest packet to route the Interest packet towards data source, and a Data

packet whose name matches the name in the Interest packet is returned to the data consumer along the reverse path of the Interest packet.

When a router receives an Interest packet, it first checks whether there is a matching data in its Content Store (CS). In NDN, Content Store (CS) temporarily buffers Data packets that pass through this router, which allows efficient data retrieval by different data consumers. If the CS buffers the requested data, router generates a Data packet with the requested data and sends it back to data consumer through the incoming interface of the Interest packet. If not, the data name is checked against each entry in the Pending Interest Table (PIT) which stores the forwarded Interest packets but have not been satisfied yet. Each entry in the PIT contains a data name, a list of nonces indicating different Interest packets, a set of incoming interfaces indicating the same data is requested by multiple downstream consumers, and a set of outgoing interfaces indicating the Interest packets with the same data name have been forwarded along multiple paths. If the data name and nonce in the received Interest packet exist in the PIT, the Interest packet will be automatically dropped since it is a duplicated Interest packet. If the data name exists in the PIT but the nonce does not, the incoming interface of the received Interest packet is added to the list of incoming interfaces of the existing PIT entry. However, if the data name does not exist in the PIT, a new entry is created and added into the PIT, and then the Interest packet is forwarded along the outgoing interface according to the forwarding strategy module that makes forwarding decisions for each Interest packet based on the information stored in the Forwarding Interest Base (FIB).

In the FIB, each entry records the working status of each outgoing interface with regard to data retrieval and maps name prefixes to one or multiple outgoing interfaces, specifying directions where Interest packets can be forwarded [13]. When a new outgoing interface is added to a FIB entry, the interface's initial status is marked as Yellow, meaning it is unknown whether the new outgoing interface may bring data back. The Yellow interface will turn Green when the requested data flows back from it. Here, the Green interface indicates that it can bring data back. However, a Green interface may turn Yellow when a forwarded Interest packet experiences a timeout, or upon the receipt of NACK. A NACK packet indicates that the upstream routers or data source does not have the requested data and has no path to forward the Interest packet further. When a outgoing interface goes down, it will be marked as Red, indicating it cannot bring data back.

When a router receives a Data packet which is returned by an intermediate router or data source, the piggybacked data name in the Data packet is used to lookup the entry in the PIT. If an entry with matching data name is found, the router forwards the Data packet to all interfaces in the set of incoming interfaces, caches a copy of data content in the CS, and removes the matching PIT entry. Otherwise, the Data packet is unsolicited, and will be discarded. In order to purge the stale entry in the PIT, each entry has an associated lifetime. When the lifetime expires, the entry is removed from the PIT.



Data Name	Nonce	IN_{IF}	OUT_{IF}	Lifetime
…/cs/puc/papers/ndn19.pdf/seg1	…GWYRP…	IN_{IF}^{A}	OUT_{IF}^{X}	ω١
…/cs/puc/papers/iot18.pdf/seg3	…VCG8I…	IN_{IF}^{B}	OUT_{IF}^{X}	ω٢
…/cs/puc/papers/0ERGWCAM2RKA	…O6MTA…	IN_{IF}^{M}	OUT_{IF}^{X}	ω٣
…/cs/puc/papers/0GQIUF13YHWQ	…3XUOE…	IN_{IF}^{M}	OUT_{IF}^{X}	ω٤
…/cs/puc/papers/3C7N0M949LKY	…THCBY…	IN_{IF}^{M}	OUT_{IF}^{X}	ω٥
…/cs/puc/papers/49X92IM5GCUV	…0NXC7…	IN_{IF}^{M}	OUT_{IF}^{X}	ω٦
…/cs/puc/papers/6ZCN1EM5VPFY	…BVA2U…	IN_{IF}^{M}	OUT_{IF}^{X}	ω٧
…/cs/puc/papers/Z0RNG9JW1BMZ	…B8S4X…	IN_{IF}^{M}	OUT_{IF}^{X}	ω٨

Fig. 1. NDN forwarding plane and an example of Interest flooding attack.

B. Interest Flooding Attack

When a legitimate user requests a data, it puts the name of desired data into the Interest packet and sends it to the network. Routers will use the piggybacked data name to forward the Interest packet towards the data source to retrieve the data. If any intermediate router already caches the requested data in its CS, it will reply a Data packet piggybacked with desired data to the legitimate user. Otherwise, the Interest packet could finally reach the data source who replies a Data packet with the desired data. For example, as shown in Fig. 1, suppose that user A and B are interested in author's papers which are stored at the */marshall.edu/cs/puc/papers* namespace. So both A and B will create Interest packets with the desired data name, such as */marshall.edu/cs/puc/papers/ndn19.pdf/seg1* and */marshall.edu/cs/puc/papers/iot18.pdf/seg3*, respectively, and send them to the network. If the data source is the exclusive owner of */marshall.edu/cs/puc/papers* namespace, each intermediate router along the forwarding path, e.g., router X, would receive the Interest packet. When router X receives the Interest packet, it first checks whether the requested data is buffered in its CS. If the requested data name does not match with any entry in the CS, route X will add new entry, e.g., */marshall.edu/cs/puc/papers/ndn19.pdf/seg1*, into its PIT, and then forward the Interest packet to upstream router, e.g., route Y. If all intermediate routers along the forwarding path between user and data source do not have the requested data, the Interest packet finally reaches the data source who will reply a Data packet piggybacked with desired data back to the user along the reverse path of Interest packet.

Although NDN is designed to be resilient against several long-standing DDoS attacks, such as direct flooding and reflector attacks through source address spoofing in traditional Internet, the attackers still can attack the network by taking advantage of the NDN's idiosyncrasies. For example in Fig. 1, suppose that user M is a malicious attacker who targets the */marshall.edu/cs/puc/papers* namespace, it can construct a large volume of malicious Interest packets with a variable-length random name component, e.g., *.../0ERGWCAM2RKA*,

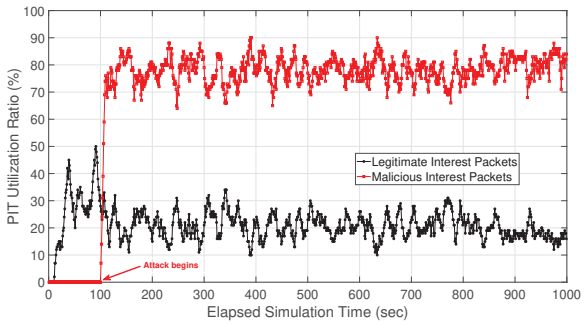


Fig. 2. The Pending Interest Table (PIT) utilization ratio against the elapsed simulation time under Interest flooding attack.

and send them to the network. Since the data source is the exclusive owner of */marshall.edu/cs/puc/papers* namespace, and each router along the forwarding path, e.g., router X or Y, has to receive and forward all malicious Interest packets, which will cause network congestion and lead to legitimate Interest packets being dropped in the network. In addition, since each router, e.g., router X, maintains an entry for each forwarded Interest packet in its PIT, an excessive amount of malicious Interest packets can cause router X quickly fill up its PIT and exhaust its memory storage. As a result, route X is unable to create new PIT entry for any incoming legitimate Interest packet, and finally causing the denial of service in NDN.

We measure the PIT utilization ratio against the elapsed simulation time in Fig. 2, where the Interest flooding attack begins at 100 seconds. As shown in Fig. 2, the PIT utilization ratio of malicious Interest packets is 0 before the Interest flooding attack begins. However, after 100 seconds, the PIT utilization ratio of malicious Interest packets significantly increases, and fluctuates between 65% and 90%. This is because the attacker sends a large amount of malicious Interest packets with a variable-length random name to the network, and the router will add a large number of new entries for each received malicious Interest packet into its PIT, a larger PIT utilization ratio of malicious Interest packets is observed. In addition, the malicious Interest packets request the data that actually does not exist in the network, thus, the entry of malicious Interest packets in the PIT will be removed whenever the associated lifetime of entry expires. On the other hand, the PIT utilization ratio of legitimate Interest packets is very low, which is around 20%. This is because an excessive amount of malicious Interest packets fill up the router's PIT, and the router cannot add any entry into the PIT when it receives the legitimate Interest packet. As a result, a much lower PIT utilization ratio is observed for legitimate Interest packets.

IV. The Proposed Self-Adjusting Share-Based Countermeasure

The basic idea of the proposed self-adjusting share-based countermeasure, also referred to as *SSC*, is that each router maintains an Interest unsatisfaction ratio and dynamically adjusts the share of forwarded Interest packets for each incoming

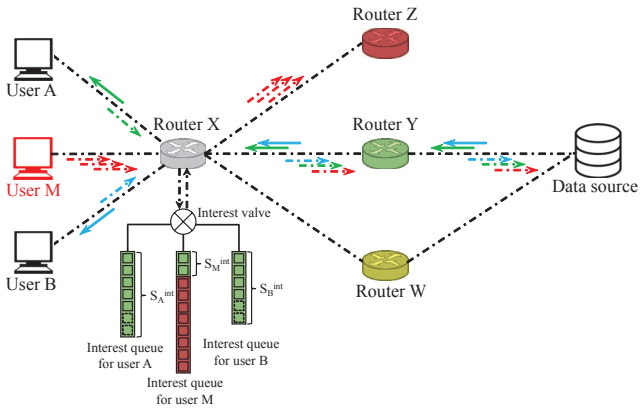


Fig. 3. A set of snapshot of the proposed *SSC* scheme, where user M is a malicious attacker and user A and B are legitimate users. The assigned share of forwarded Interest packet for user A, M, and B is S_A^{int} = 7, S_M^{int} = 2, and S_B^{int} = 6, respectively.

interface accordingly. In addition, the Interest packets that pass the assigned share of forwarded Interest packets are used as scouts to investigate unknown paths to complement routing information.

First, each router maintains an operation trace table (OPT) to record a trace of Interest receiving and forwarding operations related to each incoming interface executed during an observation window ω. Here, observation window ω is a system parameter. Each entry in the OPT consists of seven components: incoming interface id (I_{id}), the number of received Interest packets (rip), the number of replied Data packets (rdp), the number of received NACK packets (rnp), the number of expired Interest packets (eip), and the assigned share of forwarded Interest packets (S^{int}). For example, suppose that user M sends an Interest packet to router X as shown in Fig. 3, thus router X increases $OPT_X[M].rip$ by one. If router X receives a Data packet corresponding to the forwarded Interest packet before the lifetime of Interest packet expires, it increases $OPT_X[M].rdp$ by one. If user M is a malicious attacker and sends malicious Interest packet that cannot be satisfied, the data source will reply a NACK packet back to user M along the reverse path of the malicious Interest packet. When router X receives the NACK packet, it increases $OPT_X[M].rnp$ by one. If any packet, e.g., Interest, Data, or NACK packet, gets lost during transmission due to bad network condition, the lifetime of Interest packet will expire and router X increases $OPT_X[M].eip$ by one.

Second, at the end of observation window, each router examines operation trace table OPT, and calculates the Interest unsatisfaction ratio for each incoming interface and dynamically adjusts the share of forwarded Interest packets accordingly. The Interest unsatisfaction ratio of incoming interface *i*, denoted as R_i^{un}, is calculated based on the recent receiving and forwarding operations within observation window according to

$$R_i^{un} = \frac{eip \cdot \alpha + rnp \cdot (1-\alpha)}{rip}. \quad (1)$$

Here, α is the efficiency coefficient used to control the weight

of the number of expired Interest packets and the number of received NACK packets. Then, the Interest unsatisfaction ratio of each incoming interface is compared with the average Interest unsatisfaction ratio of all incoming interfaces to adjust the share of forwarded Interest packets in the next observation window. If the Interest unsatisfaction ratio of incoming interface is larger than the average Interest unsatisfaction ratio, the difference between two ratios is the amount of the share that should be reduced from the incoming interface in the next observation window. And the total amount of reduced share from all incoming interfaces will be reallocated to all incoming interfaces equally. Here, the total amount of reduced share, denoted as RS_{total}^{int}, is calculated as

$$RS_{total}^{int} = \sum_{i=I_{id}}^{N} RS_i^{int}. \quad (2)$$

And RS_i^{int} is represented as

$$RS_i^{int} = (S_i^{int} \cdot (R_i^{un} - R_{avg}^{un})), \quad \text{if } R_i^{un} > R_{avg}^{un} \quad (3)$$

where N is the total number of incoming interfaces. And the average Interest unsatisfaction ratio of all incoming interfaces is calculated as

$$R_{avg}^{un} = \frac{\sum_{i=I_{id}}^{N} R_i^{un}}{N}. \quad (4)$$

Thus, the newly assigned share of forwarded Interest packets for incoming interface *i* in the next observation window is calculated according to

$$S_i^{int} = \begin{cases} (S_i^{int} - RS_i^{int}) + \frac{RS_{total}^{int}}{N}, & \text{if } R_i^{un} > R_{avg}^{un} \\ S_i^{int} + \frac{RS_{total}^{int}}{N}, & \text{if } R_i^{un} <= R_{avg}^{un} \end{cases} \quad (5)$$

Third, given the information of Interest unsatisfaction ratio and the assigned share of forwarded Interest packets, each router's forwarding strategy module determines which outgoing interface to use to forward an Interest packet, making forwarding decisions adaptive to recent forwarding operations of each incoming interface. Our initial design is that the Interest packets that pass the assigned share of forwarded Interest packets within each observation window will be forwarded to Red outgoing interface, which is unlike to bring data back based on the historical trace of record. Thus, those Interest packets are being used for different purposes, e.g., used as scouts to investigate unknown paths to complement routing information. However, in some cases it is best to simply discard these Interest packets to reduce the network congestion. For example, as shown in Fig. 3, the assigned share of forwarded Interest packet for user A, M, and C is S_A^{int} = 7, S_M^{int} = 2, and S_B^{int} = 6, respectively. Router X has received and forwarded 5, 2, and 4 Interest packets from user A, M, and B, respectively. As a result, user M has run out of its assigned share of forwarded Interest packets. Thus, if user M still generates and sends a larger volume of Interest packets that passes the assigned share to router X, router X will use those Interest packets as scouts and forward them to Red outgoing interface to investigate unknown paths to complement routing information. However, user A and B still have not run out of the assigned share of forwarded Interest packets, thus, their newly generated Interest packets will be forwarded to Green outgoing interface to retrieve the data. Major operations of the proposed *SSC* scheme is summarized in Fig. 4.

Notations:
- RS_i^{int}, R_{avg}^{un}, RS_{total}^{int}, S_i^{int}, and ω: Defined before.
- N, Υ_i: The total number of incoming interfaces, the number of forwarded Interest packets.

◇ At the end of observation window ω:
  for $i \in N$
    Calculate RS_i^{int} according to Eq. 3;
  Calculate R_{avg}^{un} according to Eq. 4;
  Calculate RS_{total}^{int} according to Eq. 2;
  for $i \in N$
    Calculate S_i^{int} according to Eq. 5;

◇ When router x receives an Interest packet from incoming interface i:
  if $\Upsilon_i < S_i^{int}$
    Forward Interest packet to *Green* outgoing interface;
  else
    Forward Interest packet to *Red* outgoing interface;

Fig. 4. The pseudo code of the proposed *SSC* scheme.

V. Performance Evaluation

We conduct extensive simulation experiments using OMNeT++ [5] to evaluate the performance of the proposed scheme. We consider a small-scale binary tree network topology, where all Interest packets will be forwarded to upstream routers and data source. An exponential legitimate Interest packet rate with mean 1.0 and 0.1 is adopted by the legitimate users to request data content. The malicious Interest packet rate is set to exponential 0.1. The total simulation time is 1000 seconds. In this paper, we measure the performance in terms of PIT utilization ratio and the number of accepted Interest packets. For performance comparison, we revisit the prior constant share based approach, referred to as *EQ*, and modify it to work in the developed framework.

We first measure the PIT utilization ratio against the elapsed simulation time in Fig. 5, where the observed router accepts the Interest packets from four incoming interfaces, three legitimate interfaces and one malicious interface. And the Interest flooding attack begins at 100 seconds. In the *EQ*, since the router accepts the same amount of Interest packets from each incoming interface regardless of the Interest unsatisfaction ratio, the PIT utilization ratio of malicious Interest packets maintains at 25% after the Interest flooding attack begins. This is because the malicious attacker keeps sending the malicious Interest packets to the router, which quickly runs out of the assigned share of PIT entries. Since there are four incoming interfaces, and only 25% PIT entries are assigned to malicious incoming interface, the PIT utilization ratio of malicious Interest is observed at 25%. For the PIT utilization ratio of legitimate Interest packets, it fluctuates between 45% and 15% because the legitimate users have low Interest packet rate exp(1.0). As shown in Fig. 5, the proposed

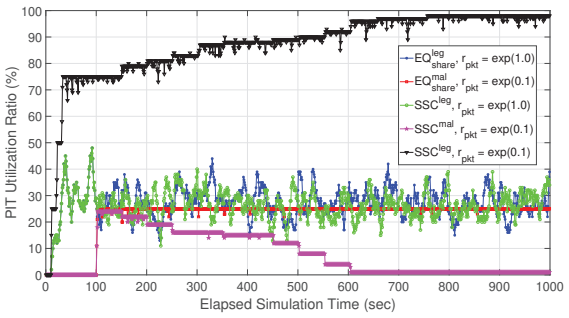


Fig. 5. The performance of PIT utilization ratio against the elapsed simulation time.

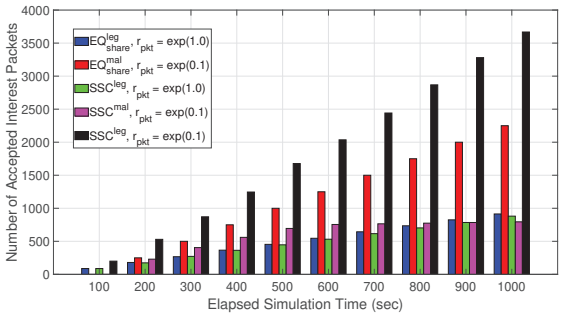


Fig. 6. The performance of the number of accepted Interest packets against the elapsed simulation time.

SSC scheme can significantly reduce the PIT utilization ratio of malicious Interest packets. As the simulation time elapses, the PIT utilization ratio of malicious Interest packets is linearly decreases to 2% at 600 seconds, and maintaining 2% PIT utilization ratio until the end of simulation. This is because the router dynamically adjusts the assigned share of forwarded Interest packets from each incoming interface based on the Interest unsatisfaction ratio. If the incoming interface has very high Interest unsatisfaction ratio, a low share of forwarded Interest packets will be assigned to it in the next observation window. Since the malicious Interest packets cannot bring data back, the Interest unsatisfaction ratio of malicious incoming interface is keeping decreasing, and a less share of forwarded Interest packets will be assigned to it. As a result, the PIT utilization ratio of malicious Interest packets is decreasing. When the Interest packet rate of legitimate users is increases to exp(1.0), the PIT utilization ratio of legitimate Interest packets significantly increases and reaches to 98% at 600 seconds. This is because the legitimate Interest packets can bring data back, thus, the Interest unsatisfaction ratio will be significantly reduced. As a result, a larger share of forwarded Interest packets will be assigned to legitimate users and more legitimate Interest packets will be accepted.

Second, the number of accepted Interest (malicious or legitimate) packets is observed against the elapsed simulation time in Fig. 6. In the *EQ*, as the simulation time elapses, the number of accepted malicious and legitimate Interest packets increases linearly. However, the number of accepted malicious Interest packets is larger than that of legitimate Interest packets, because the malicious attacker sends out malicious Interest packets with a larger packet rate exp(0.1), and more Interest packets will be accepted by the router. In the proposed *SSC* scheme, the number of accepted malicious Interest packets is significantly reduced. This is because the share of forwarded Interest packets depends on Interest unsatisfaction ratio, and the malicious Interest packets cannot bring data back and a lower Interest unsatisfaction ratio will be observed. As a result, a less number of Interest packets from malicious incoming interface will be accepted.

VI. Conclusion

In this paper, we proposed a countermeasure against Interest flooding attack in NDN, where the attacker issues an excessive number of non-satisfiable Interest packets to drop legitimate Interest packets by overwhelming Pending Interest Table in NDN routers. The potential vulnerabilities of NDN stateful forwarding plane are summarized and analyzed with a preliminary result. Then, a self-adjusting share-based countermeasure, also referred to as *SSC*, is proposed to efficiently mitigate the Interest flooding attack in NDN. Extensive simulation results indicate that the proposed approach achieves better performance, not only improving the PIT utilization ratio of legitimate Interest packets, but also reducing the number of accepted malicious Interest packets.

Acknowledgment

This research was supported by Startup grant in the Weisberg Division of Computer Science at Marshall University.

References

[1] L. Zhang *et al.*, "Named Data Networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, 2014.
[2] G. Xylomenos *et al.*, "A Survey of Information-Centric Networking Research," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1024–1049, 2014.
[3] P. Gasti *et al.*, "CRUV: Connectivity-based Traffic Density Aware Routing Using UAVs for VANets," in *Proc. ICCCN*, 2013, pp. 1–7.
[4] C. Pu and S. Lim, "A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation," *IEEE Systems Journal*, vol. 12, no. 1, pp. 834–842, 2018.
[5] A. Varga, *OMNeT++*, 2014, http://www.omnetpp.org/.
[6] T. Zhi *et al.*, "A Gini Impurity-Based Interest Flooding Attack Defence Mechanism in NDN," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 538–541, 2018.
[7] Y. Xin *et al.*, "A Novel Interest Flooding Attacks Detection and Countermeasure Scheme in NDN," in *Proc. GLOBECOM*, 2016, pp. 1–7.
[8] S. Signorello *et al.*, "Advanced Interest Flooding Attacks in Named-Data Networking," in *Proc. NCA*, 2017, pp. 1–10.
[9] H. Salah *et al.*, "Coordination Supports Security: A New Defence Mechanism Against Interest Flooding in NDN," in *Proc. LCN*, 2015, pp. 73–81.
[10] Y. Xin *et al.*, "Detection of Collusive Interest Flooding Attacks in Named Data Networking Using Wavelet Analysis," in *Proc. MILCOM*, 2017, pp. 557–562.
[11] T. Nguyen *et al.*, "A Security Monitoring Plane for Named Data Networking Deployment," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 88–94, 2018.
[12] A. Compagno *et al.*, "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking," in *Proc. LCN*, 2013, pp. 630–638.
[13] 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, pp. 779–791, 2013.