Detecting and Mitigating A Sophisticated Interest Flooding Attack in NDN from the Network-wide View

Guang Cheng[1,2,3], Lixia Zhao[1,2,3], Xiaoyan Hu[1,2,3], Shaoqi Zheng[1,2,3], Hua Wu[1,2,3], Ruidong Li[4], Chengyu Fan[5]
[1]School of Cyber Science & Engineering, Southeast University, Nanjing 211189, China
[2]Key Laboratory of Computer Network and Information Integration of Ministry of Education of China, Southeast University
[3]Key Laboratory of Computer Network Technology of Jiangsu Province
[4]National Institute of Information and Communications Technology, Tokyo 184-8795, Japan
[5]Computer Science Department, Colorado State University, Fort Collins, USA
Email: {gcheng, lxzhao, xyhu, sqzheng, hwu}@njnet.edu.cn, lrd@nict.go.jp, chengyu@colostate.edu

***Abstract*—Interest Flooding Attack (IFA) is one of the main security threats for the Named Data Networking (NDN). Most of its existing countermeasures enable intermediate routers near the attackers to independently detect the attack and consider the typical attack scenario in which attackers directly send malicious Interests at a constant and relatively high rate. Moreover, they may also throttle legitimate Interests when enforcing the existing defence measures at intermediate routers as it is still difficult for them to distinguish the Interests issued by attackers from those issued by legitimate consumers. Instead, this work aims at a more sophisticated attack scenario in which attackers start the attack at a relatively lower rate but gradually speed up to keep the Pending Interest Tables (PITs) of the victims increasing to finally deplete the PIT resources for legitimate consumers. It is relatively difficult for intermediate routers to independently and timely detect such a sophisticated IFA. To solve this problem, we propose a mechanism to detect the sophisticated IFA from the network-wide view. A central controller monitors the network and makes a comprehensive and prompt decision on whether there is an ongoing IFA based on the overall state of the whole network collected from the abnormity information reports sent by the first-hop routers of attackers. Attack sources can be directly located after an IFA is determined and then the malicious Interests can be prevented from entering the network without throttling legitimate Interests. We conduct an experimental study to evaluate the performance of the proposed mechanism and explore the parameter settings of the attack detection algorithm at access routers. The experimental results validate that our mechanism can timely detect and mitigate the sophisticated IFA without throttling requests from legitimate consumers.**

***Keywords*—network-wide view, Interest flooding attack, named data networking**

I. Introduction

Named Data Networking (NDN) [1] is one of the most promising future Internet architectures. NDN names the content in the network and transforms the first entity of the network from hosts to named content. NDN communication is driven by a consumer issuing an Interest packet which specifies the name of the desired content segment. Then intermediate nodes route the Interest by the content name and the matching Data packet with the desired content segment returns along the reverse path of the Interest. NDN supports stateful forwarding. Each NDN router should maintain the state information of each forwarded but not yet satisfied Interest in its Pending Interest Table (PIT). A PIT entry will not be removed unless the corresponding Data packet for the recorded Interest returns or its lifetime expires. This feature brings many advantages to NDN [2]. However, it can also be exploited by attackers to launch an NDN-specific DDoS attack – Interest Flooding Attack (IFA). IFA attackers usually send a great number of unsatisfiable Interests to exhaust routers' PIT resources to make them unable to create new PIT entries for subsequent incoming Interests. Therefore, requests from legitimate consumers will be discarded [3].

The existing mechanisms against IFA [4–10] have one or more of the following features. First, the existing mechanisms mainly enable intermediate routers near the attackers to independently detect and mitigate the attack and focus on the typical IFA scenario in which attackers directly send malicious Interests at a constant and relatively high rate. They may suffer performance degradation to a certain extent when a more sophisticated IFA is launched as an independent decision on attack detection and mitigation may lead to relatively high detection latency, poor sensitivity to low intensity attack and overreaction. Second, the requests from legitimate consumers may also be throttled as the existing mitigation methods cannot accurately distinguish requests issued by attackers from those issued by legitimate consumers. Third, it is difficult for most existing mechanisms to trace back to attackers since an Interest contains no information about its issuer.

Instead, this work focuses on the more sophisticated IFA scenario proposed in our previous work [11], i.e., attackers start the attack at a relatively lower rate but speed up step by step to keep the PITs of the victims increasing to exhaust their PIT resources, which is relatively difficult to be timely detected by the existing countermeasures. We propose a mechanism with a central controller to detect and mitigate such sophisticated IFA from the network-wide view. In our proposed mechanism, each access router (i.e., the router that directly connected to consumers/attackers) in the network is responsible for detecting the state of its each interface. When an access router finds there is something abnormal on its certain interfaces but is unsure whether there is an IFA, it will notify the controller and report its abnormal observations according to the controller's requests. Attack detection at access routers can make it easier to locate attackers after an IFA is determined. The controller collects all the abnormal information and detects the attack from the network-wide view based on the overall state of the whole network, aiming to timely detect the attack before the network suffers significant damage. When the controller determines that there is actually an ongoing IFA, it will further locate the attackers and then inform the access routers under attack of their malicious interfaces. Afterwards, access routers can take targeted countermeasures on the identified attackers at source according to the feedback from the controller, which

978-1-7281-4371-2/19/$31.00 ©2019 IEEE
DOI 10.1109/NMIC.2019.00007

can avoid throttling requests from legitimate consumers.

The remainder of this paper is organized as follows. We analyse the state of the art mechanisms against IFA in Section II. Section III introduces the overall framework and design specifications of our proposed mechanism. We conduct an experimental study on the proposed mechanism to evaluate its performance and explore the parameter settings in IV. Finally, we conclude the paper in Section V.

II. Related Work

Most existing mechanisms against IFA focus on the typical IFA scenario in which attackers directly send malicious Interests at a constant rate, especially at a relatively high rate. The IFA detection and identification of malicious prefix or/and interfaces in these mechanisms are mainly based on PIT-related statistics, such as the satisfaction ratio of Interests and PIT usage. Afanasyev *et al.* [4] presented three countermeasures to limit the number of Interests forwarded in the network based on NDN's inherent properties of storing per packet state on each router and maintaining flow balance. Dai *et al.* [5] proposed *Interest traceback* to trace back to the originators of malicious Interests after detecting an IFA. It detects the attack only based on routers' PIT sizes, which may misjudge small bursts of Interests as IFAs. Vassilakis *et al.* [7] proposed a mitigation mechanism that allows routers to quickly identify and block attackers by detecting abnormal user behavior. Compagno *et al.* [6] proposed *Poseidon*, in which an router determines an IFA when both the unsatisfaction ratio and PIT usage of Interests from a certain interface exceed their thresholds respectively. Afterwards, the router will limit the rate of incoming Interests from its malicious interfaces and issue a push-back "alert" message to the node connected to the offending interface. However, the collaboration between routers in *Poseidon* appears only during the mitigation phase. Salah *et al.* [12, 13] adopted a new framework to assign a predetermined set of routers as monitoring routers which will detect and mitigate an IFA with the help of a central controller. This framework can work efficiently when the network is static. However, the network state is always changing in the real world, such as the distribution of clients and the connections between different nodes, but the monitoring routers in this framework are predetermined.

The mechanisms based on PIT-related statistics may cause misjudgment. For example, the prefix hijacking attack can also lead to high PIT expiration ratio, which may be mistakenly classified as an IFA. Xin *et al.* [14] proposed to detect an IFA based on cumulative entropy by monitoring the content request abnormal distribution and then introduced the malicious prefix identification method by relative entropy theory. Zhi *et al.* [15] proposed a Gini impurity-based IFA detection mechanism using the statistical properties of the name field in the Interests to detect and mitigate IFAs. These two mechanisms above can detect the IFA fast and avoid certain misjudgment.

Most existing solutions distinguish Interests issued by attackers from those issued by legitimate consumers by identifying the malicious prefix or/and interfaces. The most frequently used mitigation method against IFA is limiting the rate of incoming Interests from the malicious interfaces or under the malicious prefix or filtering out all the relevant Interests, which can obviously reduce the number of malicious Interests in the network. However, such method may mistakenly drop requests from legitimate consumers, since Interests coming from the identified malicious interfaces or under the malicious prefix can also be issued by legitimate consumers. Ding *et al.* [8] presented a retransmission forwarding mechanism to ensure legitimate consumers' requests. Wang *et al.* [16] proposed an approach called *Disabling PIT Exhaustion (DPE)* to decouple all the malicious Interests from PIT, by directly recording their state information (e.g., incoming interface) in the name of each malicious Interest rather than PIT. The authors also introduced a packet marking scheme to enable Data packet forwarding without the help of PIT. These two solutions can ensure that requests from legitimate consumers under malicious prefix or from malicious interfaces can still be satisfied when defence measures are taken after an IFA is detected. However, the complex processing operations should be performed on all the potential malicious Interests, such as changing Interests' names, which will bring about heavy burden to the network due to the large scale of malicious Interests.

This work focuses on the more sophisticated IFA scenario proposed in our previous work [11]. We propose a mechanism against such sophisticated IFA with a central controller monitoring the network from the network-wide view, aiming to timely detect the attack at an early stage and then locate the attackers to mitigate the attack at source to avoid throttling legitimate consumers' requests.

III. Attack Detection and Mitigation

In this section, we show the overall framework and design specifications of attack detection and mitigation of our proposed mechanism.

A. Overall Framework

In our proposed mechanism, there is a central controller which monitors the network from the network-wide view, aiming to timely detect the sophisticated IFA and then locate the attack sources to take targeted defence measures to avoid throttling requests from legitimate consumers. The overall framework of the mechanism is shown as Fig. 1. The routers directly connected to consumers/attackers are referred to as access routers, and the rest routers are referred to as intermediate routers. The dotted lines represent the interaction of attack-related information between the central controller and all the routers in the topology.

NDN routers (including access routers and intermediate routers) in the network are responsible for monitoring their real-time states. When something abnormal is detected, such as low satisfaction ratio of received Interests, abnormal distribution of received requests, excessive speed of incoming Interests and so on, if the router can independently determine that there is an IFA, it can immediately take defence measures. Otherwise, if the router finds an abnormity but is unsure whether there is an ongoing IFA only based on its local observations, it will notify the central controller that there exists an abnormity and then wait for the decision from the controller. The router can report its detailed observations about the detected abnormity to the controller based on the demand of the controller and is also required to take corresponding measures based on the final decision of the controller.

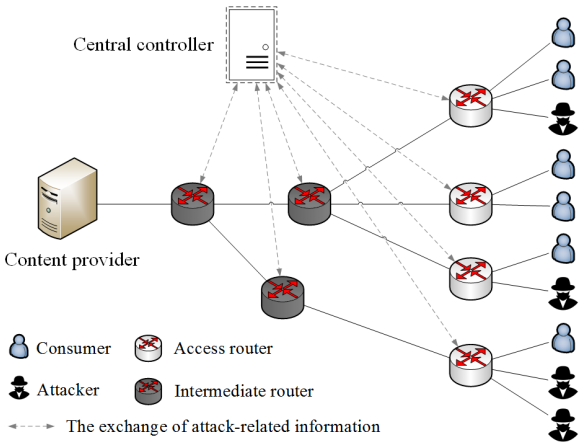


Fig. 1: The overall framework of the proposed mechanism

The central controller constantly monitors the network from the network-wide view and is logically connected to all the routers in the network. The controller can collect all the reports after receiving attack-related notifications from routers which have found something abnormal, and can also proactively request the information of any router as required. The controller will analyse all the reports it has obtained and make a comprehensive and prompt decision on whether the network is under an IFA based on the overall state of the whole network. Afterwards, the controller will notify relevant routers of the final decision about the attack.

B. Attack Detection

The attack detection in our mechanism is comprised of two parts, local attack detection at NDN routers and network-wide attack detection at the central controller.

In most existing mechanisms against IFA, the attack detection is required to be performed on each router in the network, which will bring about heavy burden to the network. Moreover, it is difficult to locate attackers after an IFA is determined since an Interest contains no information about its issuer to protect users' privacy. Obviously, the most efficient way to trace back to attack sources is making good use of access routers that attackers are directly connected to. Therefore, in our proposed mechanism, all the access routers in the network are selected as monitoring routers, which will periodically detect whether there is an abnormity on each of their interfaces.

1) ***Local attack detection at access routers****:* In order to launch an effective IFA, attackers should issue a large number of spoofed Interests to make sure that the speed at which a victim adds entries to its PIT is higher than that it removes, so that PIT resources of the victim can eventually be exhausted. For an access router, it is obvious that the speed of incoming Interests on a malicious interface connected to an attacker is certainly different from that on a legitimate interface connected to a legitimate consumer. Based on the above, we use the concept of non-parametric cumulative sum (CUSUM) [17], which is one of the change point detection algorithms and is widely used to detect abnormities, to detect whether the speed of incoming Interests on each interface of an access router is abnormal and thus to detect an IFA.

We define the sequence $\{X_n\}$ representing the average speed of incoming Interests on an interface of an access router in a series of continuous time window Δt. We assume that the upper bound of the average speed at which legitimate consumers send Interests is β and $\beta = (\alpha{+}1)\overline{v}$, where $\overline{v}$ is the mean value of the speed of Interests from legitimate consumers observed in normal traffic conditions (where there is no attack or network congestion) and α is a constant greater than 0 that indicates the percentage above the mean value that is considered an indication of abnormal behavior. It is necessary to transfer $\{X_n\}$ into a new sequence $\{Z_n\}$ by $Z_n = X_n - \beta$, which must be negative during normal conditions. Further, we can define another sequence $\{Y_n\}$ as follows:

$$\begin{cases} Y_n = (Y_{n-1} + Z_n)^+, & n > 0 \\ Y_0 = 0, & n = 0 \end{cases} \tag{1}$$

where

$$x^+ = \begin{cases} x, & x > 0 \\ 0, & otherwise \end{cases} \tag{2}$$

When the observed average speed of incoming Interests on an interface of an access router is larger than β, Y_n becomes larger than 0 and will keep accumulating if the speed of incoming Interests still keeps high. A large value Y_n indicates that there may be an ongoing IFA on the monitored interface. A threshold $T_{suspicious}$ is set for Y_n. Moreover, small bursts of Interests can also lead to a large Y_n value. In order to avoid mistakenly classifying it as an IFA, an access router will also record the number of expired Interests on each of its interfaces during each time window and another threshold $T_{timeout}$ is set.

For each interface $inFace$ of an access router, when Y_n exceeds $T_{suspicious}$ and the number of expired Interests exceeds $T_{timeout}$, the access router will judge that $inFace$ may be under an IFA and then send an Interest with specific name */ndn/ddos/flooding/controller/routerId/abnormityNotification* to notify the central controller that something abnormal has been found, where the name component *routerId* refers to the identifier of the access router so that the controller can learn which access router the notification is sent by. Then, the access router will report its latest abnormal observations according to the subsequently received requests from the controller. The reported observations mainly include the time when the report is produced and the collection of the information of incoming Interests on each suspicious interface at the access router. The information of incoming Interests on each suspicious interface includes the identifier of the interface, the prefixes and corresponding average speed of incoming Interests under each prefix.

2) ***Network-wide attack detection at the central controller****:* As soon as receiving the attack-related notification from an access router, the controller replies with a Data packet expressing that it has already received the notification and begins to periodically send Interests with specific name */ndn/ddos/flooding/routerId/report/reportSeq* to request the latest observations at the access router *routerId*. The controller will wait for a period of time to make sure that all the reports from access routers produced at the latest observation

period have already arrived. Note that if the number of access routers that have found an abnormity is significantly large, the controller will stop waiting and immediately analyse the reports it has already received.

Based on all the already received abnormal observations, the controller determines whether there is an ongoing IFA. As the central controller monitors the network from the network-wide view, it can observe the overall topology of the network. Moreover, each link in the network has its capacity limit. We express such limit as the number of forwarded Interests out of each interface based on the physical capacity of the corresponding interface (i.e., pending *Interest Limit*) as [4], which will be proportional to the link's bandwidth-delay product (BDP) [18]. The value of Interest limit can be formalized as follows:

$$\text{Interest Limit} = Delay[s] \cdot \frac{\text{Bandwidth [Bytes/s]}}{\text{Data packet size [Bytes]}} \quad (3)$$

where *Delay* is the expected time for the Interest to be satisfied and *Data packet size* is the size of the returning Data packet.

For each report, the controller finds out the corresponding content provider of the reported suspicious Interests and then calculates the paths that suspicious Interests traverse from the access router to the content provider. Afterwards, the controller will further calculate the total number of suspicious Interests transmitted on each link. If the controller finds that there is one or more links on which the number of data requested is going to reach the corresponding link capacity limit (i.e., $the\ number\ of\ requested\ data \geq \theta \cdot Interest\ limit$, where θ is a constant and $0 < \theta \leqslant 1$), it determines that there is an ongoing IFA in the network and then finds out the sources of suspicious Interests on that link, i.e., access routers whose reported suspicious Interests pass through that link and through which interfaces these Interests enter the network (i.e., their corresponding malicious interfaces). Otherwise, if there is always no such link in a certain period of time, the controller determines that there is no an ongoing IFA. Afterwards, the controller notifies relevant access routers of its decision. If an IFA is determined, the controller sends an Interest with specific name */ndn/ddos/flooding/routerId/attackACK/MaliciousInterfacesList*, to notify the access router *routerId* that its interfaces listed in *MaliciousInterfacesList* are malicious. Otherwise, an Interest with name */ndn/ddos/flooding/routerId/noAttack* is issued by the controller to notify the access router *routerId* that it is not under an IFA. After receiving the feedback from an access router (i.e., a Data packet) expressing that it has already received the notification and taken actions according to the controller's decision, the controller will stop requesting the access router's observations.

Note that all the attack-related Interests exchanged between the controller and access routers are signed to avoid bringing new security issues to NDN.

C. Attack mitigation

In most existing mechanisms against IFA, requests from legitimate consumers may be mistakenly throttled when performing existing IFA mitigation methods at intermediate routers, since it is difficult for them to accurately distinguish Interests issued by attackers from those issued by legitimate consumers only based on the identified malicious prefix or interfaces.

In view of the problem above, the attack mitigation in our proposed mechanism is performed at access routers. As soon as receiving the attack-related notification from the controller expressing that there is an IFA on its certain interfaces, an access router will immediately block the nodes directly connected to its malicious interfaces determined by the controller, i.e., dropping all the incoming Interests from its malicious interfaces. Mitigating an IFA at source can directly prevent malicious Interests from entering the network and can also avoid throttling the requests from legitimate consumers, since for an access router, the node directly connected to a malicious interface must be an attacker and Interests from the malicious interfaces are all issued by attackers.

IV. Evaluation

In this section, we present the experimental studies on our proposed mechanism. We evaluate its performance in three aspects, the satisfaction ratio of legitimate Interests, the average number of PIT entries at intermediate routers and the delay of legitimate Interests (time interval between first Interest sent and Data packet received, i.e., including time of Interest retransmissions), and explore the parameter settings of the attack detection algorithm at access routers.

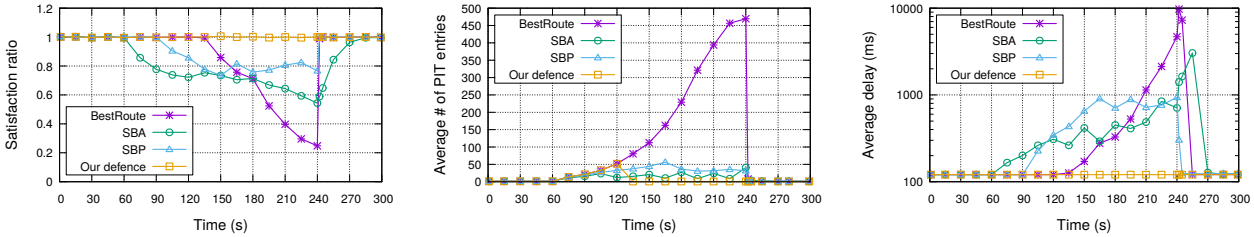
A. Experimental Setup

We use the open-source ndnSIM [19], a NS-3 based NDN simulator, to run our simulations. The topology we used is based on a modified version of Rocketfuel's AT&T topology [20]. The topology consists of 182 nodes, including 80 leaf nodes (i.e., consumers), 25 gateway nodes (i.e., access routers, which are directly connected to consumers), 77 intermediate nodes (i.e., intermediate routers, which are directly connected to other routers). Moreover, we additionally create a new node serving as the central controller, which is connected to a randomly selected intermediate router. The central controller will not participate in the routing of packets between consumers and producers.

In our experiments, 40% of the consumers are randomly selected as attackers, and we randomly pick either an intermediate node or a gateway node as the content provider. Before the attack starts, attackers do as what legitimate consumers do, i.e., send satisfiable Interests at the same speed as legitimate consumers. The initial attack speed of attackers is 1/3 of the speed of Interests from legitimate consumers and the attack speed increases at a speed of approximately 3%, 5%, 7% or 10% higher per second in different simulation runs. The $Delay$ used for the calculation of capacity limit on each link in (3) is set to 300ms (the largest RTT in the used topology). Each simulation is repeated for 10 runs to randomize the results to get an average result. The detailed parameter settings are shown in Table I.

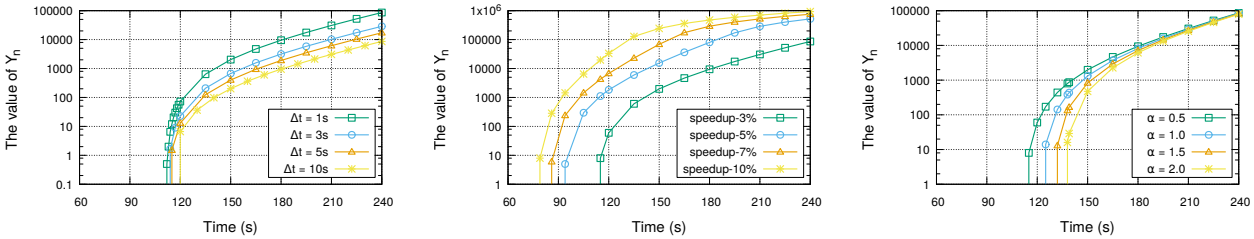
B. Performance of the proposed mechanism

In this subsection, we evaluate the performance of the proposed mechanism and compare it with *Satisfaction-based*



(a) Satisfaction ratio of legitimate Interests (b) Average # of PIT entries at intermediate routers (c) Average delay of legitimate Interests

Fig. 2: Performance of the proposed mechanism



(a) The value of Y_n versus time window (b) The value of Y_n versus attack speed (c) The value of Y_n versus the factor α

Fig. 3: Behavior of the non-parametric CUSUM algorithm at access routers during the attack

TABLE I: Parameter Setting

Parameter	Values
Maximum PIT size	2000 PIT entries
The lifetime of Interests	1s
Size of each content item	1100 bytes
Forwarding strategy	BestRoute
Rate of legitimate consumers	40 Interests per second
Simulation time	300s
Duration of attack	60 - 240s
Time window (Δt)	1s, 3s, 5s, 10s
$T_{suspicious}$	$3\overline{v}$
$T_{timeout}$	$0.2\ \overline{v} \cdot \Delta t(s)$
Factor α for access routers	0.5, 1.0, 1.5, 2.0
Factor θ for the controller	0.7

Interest acceptance (SBA) and *Satisfaction-based pushback (SBP)* presented in [4], and *BestRoute* strategy which represents the state of the network with no defence mechanism. The attack speed is 3% higher per second, the factor α is set to 0.5 and the time window is set to 1s. The results are shown as Fig. 2.

When there is no defence mechanism, the number of PIT entries keeps increasing gradually after the attack starts. In the early stage of the attack, though the PIT usage at intermediate routers becomes larger than that in the normal condition, there is still no router's PIT resources exhausted. Therefore, the satisfaction ratio and delay of legitimate Interests keep unchanged. But with the increase of the attack speed, malicious Interests continue to accumulate in the PITs of routers under attack. Finally, the PIT resources of victim routers will be exhausted by malicious Interests, which makes them cannot create new PIT entries for subsequently incoming legitimate Interests, so the satisfaction ratio of legitimate Interests begins to decline and the delay of legitimate Interests begins to increase after the attack lasts for a period of time.

In SBA and SBP, the probability that a router accepts the received Interest is based on the satisfaction ratio of incoming Interests on the arrival interface of the received Interest. After the sophisticated IFA starts, the satisfaction ratio of incoming Interests on intermediate routers' interfaces which malicious Interests pass by begins to decline. Therefore, some legitimate Interests will be dropped mistakenly and the delay of legitimate Interests becomes larger, even when there is still no router's PIT resources exhausted in the early stage of the attack. Though the PIT usage is improved, it is still higher than that in the normal condition. Since there are still a proportion of malicious Interests forwarded successfully and some requests from legitimate consumers dropped mistakenly, such Interests will pend in routers' PITs until their lifetime expires.

However, in our proposed mechanism, the satisfaction ratio and average delay of legitimate Interests are always the same as those before the sophisticated IFA starts. Though the PIT usage at intermediate routers becomes larger at the beginning of the attack, it is still relatively low and will return to its normal level after the attack is detected. Since the proposed mechanism can detect the sophisticated IFA timely before the victims' PITs are overwhelmed, and then mitigate the attack at source, i.e., directly dropping all the Interests from the malicious interfaces at access routers (i.e., attackers), which can directly prevent malicious Interests from entering the network and will not throttle the requests from legitimate consumers.

C. Exploration on the parameter settings of the non-parametric CUSUM algorithm at access routers

In this subsection, we explore the parameter settings of the attack detection algorithm at access routers. Fig. 3 shows the behavior of the non-parametric CUSUM algorithm on a malicious interface at an access router during the sophisticated IFA.

Fig. 3(a) shows the value of Y_n under different time windows where the attack speed is 3% higher per second and the factor α is set to 0.5. It can be seen that the value of Y_n is always equal to zero when the attack speed is relatively low in the early stage of the attack. With the increase of the attack speed, the average speed of incoming Interests on a malicious interface at an access router becomes larger and the value of Y_n begins to continuously accumulate and keeps increasing. Since the value of Y_n is calculated and accumulates at the end of each time window, the smaller the time window is, the more frequently the value of Y_n accumulates and the faster the value of Y_n grows. Fig. 3(b) shows the value of Y_n under different attack speeds where the time window is 1s and the factor α is set to 0.5. It is obvious that the faster the attackers speed up, the larger the value of Y_n is at the same time and the earlier the access router can find an abnormity on the malicious interface. Fig. 3(c) presents the value of Y_n while the factor α ranges between 0.5 and 2.0, where the time window is 1s and the attack speed is 3% higher per second. The smaller the factor α is, the smaller β is and the earlier the value of Y_n becomes larger than zero and begins to keep increasing. Since the attackers speed up gradually, the attack speed becomes significantly larger than the mean value of the speed of Interests from legitimate consumers (i.e., $\overline{v}$) and the difference in the value of Y_n under different values of the factor α becomes smaller.

V. Conclusion & Future Work

In this paper, we propose a mechanism with a central controller to detect and mitigate a more sophisticated IFA from the network-wide view. In our proposed mechanism, each access router monitors the state of each of its interfaces. When an access router finds an abnormity but is unsure whether there is an IFA, it will notify the controller and report its abnormal observations. The central controller monitors the network from the network-wide view and makes a comprehensive decision on whether an IFA exists in the network based on all the reported observations. If an IFA is determined, the controller will further locate the attackers and notify the access routers under attack of their malicious interfaces respectively. Afterwards, access routers can refuse to accept any Interest from the malicious interfaces determined by the controller, which can directly and immediately prevent malicious Interests from entering the network as well as avoid throttling requests from legitimate consumers. The experimental studies validate that our proposed mechanism can detect the sophisticated IFA before it causes great damage to the network and legitimate consumers can still retrieve the desired content. In our future work, we will evaluate the proposed mechanism with more metrics, the effects of different parameter settings on the performance, and the overhead of using the central controller.

Acknowledgment

The authors would like to thank anonymous reviewers. The research work leading to this article is supported by the National Key Research and Development Program of China under Grant No. 2017YFB0801703, the National Natural Science Foundation of China under Grant No.61602114, CERNET Innovation Project No.NGII20170406, and JSPS KAKENHI Grant Number JP19H04105.

References

[1] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, c. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[2] 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.

[3] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and ddos in named data networking," in *Proc. ICCCN, Nassau, Bahamas*, 2013, pp. 1–7.

[4] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *IFIP Networking Conference, Brooklyn, New York, USA*, 2013, pp. 1–9.

[5] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate ddos attacks in ndn by interest traceback," in *Proc. INFOCOM Workshops, Turin, Italy*, 2013, pp. 381–386.

[6] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating interest flooding ddos attacks in named data networking," in *Proc. LCN, Sydney, Australia*, 2013, pp. 630–638.

[7] V. G. Vassilakis, B. A. Alohali, I. Moscholios, and M. D. Logothetis, "Mitigating distributed denial-of-service attacks in named data networking," in *Proc. AICT, Brussels, Belgium*, 2015, pp. 18–23.

[8] K. Ding, Y. Liu, H. Cho, H. Chao, and T. K. Shih, "Cooperative detection and protection for interest flooding attacks in named data networking," *International Journal of Communication Systems*, vol. 29, no. 13, pp. 1968–1980, 2016.

[9] J. Tang, Z. Zhang, Y. Liu, and H. Zhang, "Identifying interest flooding in named data networking," in *Proc. GreenCom, Beijing, China*, 2013, pp. 306–310.

[10] K. Wang, H. Zhou, Y. Qin, and H. Zhang, "Cooperative-filter: countering interest flooding attacks in named data networking," *Soft Computing*, vol. 18, no. 9, pp. 1803–1813, 2014.

[11] L. Zhao, G. Cheng, X. Hu, H. Wu, J. Gong, W. Yang, and C. Fan, "An insightful experimental study of a sophisticated interest flooding attack in ndn," in *Proc. HotICN, Shenzhen, China*, 2018, pp. 121–127.

[12] H. Salah, J. Wulfheide, and T. Strufe, "Lightweight coordinated defence against interest flooding attacks in NDN," in *Proc. INFOCOM Workshops, Hong Kong, China*, 2015, pp. 103–104.

[13] ——, "Coordination supports security: A new defence mechanism against interest flooding in NDN," in *Proc. LCN, Clearwater Beach, FL, USA*, 2015, pp. 73–81.

[14] Y. Xin, Y. Li, W. Wang, W. Li, and X. Chen, "A novel interest flooding attacks detection and countermeasure scheme in NDN," in *Proc. Globecom, Washington, DC, USA*, 2016, pp. 1–7.

[15] T. Zhi, H. Luo, and Y. Liu, "A gini impurity-based interest flooding attack defence mechanism in NDN," *IEEE Communications Letters*, vol. 22, no. 3, pp. 538–541, 2018.

[16] K. Wang, H. Zhou, Y. Qin, J. Chen, and H. Zhang, "Decoupling malicious interests from pending interest table to mitigate interest flooding attacks," in *Proc. Globecom Workshops, Atlanta, GA, USA*, 2013, pp. 963–968.

[17] H. H. Takada and U. Hofmann, "Application and analyses of cumulative sum to detect highly distributed denial of service attacks using different attack traffic patterns," *IST INTERMON Newsletter*, vol. 7, pp. 1–14, 2004.

[18] A. Afanasyev, N. Tilley, P. L. Reiher, and L. Kleinrock, "Host-to-host congestion control for TCP," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 3, pp. 304–342, 2010.

[19] The ndn simulator ndnsim. Http://ndnsim.net/.

[20] N. Spring, R. Mahajan, and D. Wetherall, "Measuring isp topologies with rocketfuel," in *Proc. SIGCOMM, New York, NY, USA*, 2002, pp. 133–145.