Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN 2018)

An Insightful Experimental Study of a Sophisticated Interest Flooding Attack in NDN

Lixia Zhao*#, Guang Cheng*#, Xiaoyan Hu*#, Hua Wu*#, Jian Gong*#, Wang Yang*#, Chengyu Fan†
**School of Cyber Science & Engineering, Southeast University, Nanjing, P.R.China*
#Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education
†Computer Science Department,Colorado State University,Ford Collins,USA
Email: {lxzhao, gcheng, xyhu, hwu, jgong, wyang}@njnet.edu.cn chengyu@cs.colostate.edu

***Abstract*—NDN (Named Data Networking), a promising next-generation architecture, puts named content in the first place of the network and is resilient to many existing DDoS attacks. However, Interest Flooding Attack (IFA), a typical NDN-specific DDoS attack, has been widely recognized as a serious threat to the development of NDN. The existing countermeasures against IFA mainly aim at the scenario that attackers send spoofed Interests at a fairly high rate and intermediate routers near the attackers can timely detect the attack by themselves. Instead, this work focuses on a more sophisticated scenario that carefully-crafted attackers send Interests at a respectively lower rate at the beginning but gradually speed up to keep the victims' PIT sizes increasing to eventually deplete the PIT resource for legitimate users. We conduct an insightful experimental study of such sophisticated IFAs on a real-world network topology and our experimental results demonstrate that the statistics of intermediate routers near the attackers change more gradually and slightly in such an attack, which makes it more difficult for an intermediate router near the attackers to detect by itself. Based on the analytical results of this study, we discuss a potential detection and countermeasure mechanism against such a sophisticated IFA in which a central controller monitors the network from a global view.**

Keywords—global view, Interest flooding, experimental study, named data networking

I. Introduction

The Internet has become an important infrastructure supporting the development of modern society and technology. Since created in 1960s, the TCP/IP based Internet architecture has become the most widely used one due to its success in achieving the resource sharing. However, the way people access and utilize the Internet has greatly changed since the 1970s. People's needs for mobility support and content distribution have gradually emerged and received increasing attention.

NDN (Named-Data Networking) [1], an instantiation of Information Centric Networking (ICN), transforms the first entity of network from hosts to named content. Users send an *Interest* packet with the name of desired content to retrieve the *Data* packet and don't need to be concerned with where the content is. There are three necessary components in a NDN router: *Content Store (CS)* used for content caching and retrieval, *Forwarding Information Base (FIB)* to store routing information to route Interests and *Pending Interest Table (PIT)* to store the state information for each forwarded but not satisfied Interest. The state information in PIT, i.e. a PIT entry, guides the matching Data packet of its pending Interest packet back to its requesting consumer(s) and enables a stateful forwarding plane to successfully circumvent prefix hijackers, avoid failed links, and utilize multiple paths to mitigate congestion [2]. A PIT entry will not be removed until its corresponding Data is returned or the lifetime of its pending Interest expires. This feature of PIT may be exploited by attackers to launch a NDN-specific DDoS attack, named Interest Flooding Attack (IFA). In an IFA, attackers send a large number of malicious Interests with fake names to request for non-existent content to exhaust the victim router's PIT. It has been demonstrated that IFA can significantly degrade the performance of NDN and even make it deny services to legitimate users [3][4][5].

In most of the existing countermeasures against IFA, an intermediate router makes an independent decision on whether there is an ongoing attack in the network [4][5][6][7]. These countermeasures work well when faced with a high-speed IFA in which the statistics of a single router, such as the PIT usage and the ratio of unsatisfied Interests on an interface, have significant changes immediately after the attack starts. However, carefully-crafted attackers may manage to launch a more sophisticated attack to keep the changes of router statistics much more slightly, making it more difficult for a single intermediate router to timely detect by itself, at least at the early stage of the attack.

This work describes such sophisticated attack in detail and conducts an insightful experimental study on a real-world network topology to investigate the differences between the proposed scenario and the common one, i.e. a high-speed IFA, as well as its specific characteristics. And we further discuss a potentially novel mechanism with central controller against such sophisticated attack based on the analytical results.

The remainder of the paper is organized as follows. We first summarize the related work about IFA in Section II and describe the proposed sophisticated attack scenario in Section III. Then we conduct an experimental study of the proposed attack scenario in Section IV. Finally, we discuss the future work on our tentative countermeasure against such an attack and conclude in Section V.

II. Related Work

In this section, our work is divided into two parts. First, we briefly introduce several aspects of NDN architecture

978-1-5386-4870-4/18/$31.00 ©2018 IEEE

related to the IFA. Second, we describe the previous researches on IFA in NDN.

A. *NDN background*

There are two kinds of packets in NDN, Interest packet and Data packet, whose names are both hierarchically structured. Interest packet is the request and Data packet is the response. All communication in NDN is receiver-driven, meaning that Data is delivered only in response to an Interest requesting this Data first.

There are different processing schemes for Interest packet and Data packet in a NDN router. When an Interest arrives on an interface of a router, a longest-match is done to the router's CS. If there is no matching Data, the Interest name is checked against the PIT. If there is already a PIT entry for the previous Interests requesting the same content, the incoming interface of this Interest is added to the existing PIT entry and then the Interest is discarded, meaning that no new PIT entry is created and this Interest is not sent upstream in such case. If not, a new PIT entry is created for the Interest, and it will also be forwarded upstream through the interface(s) determined by the forwarding strategy [2] based on the FIB. When a router receives a Data, it sends the Data to all the requesting interfaces in the matching PIT entry, then removes the entry and caches the Data in its CS.

As explained above, the PIT of each NDN router keeps track of all the pending Interests. This feature can be exploited by attackers to launch a NDN specific DDoS attack named Interest Flooding Attack (IFA). In an IFA, attackers flood massive malicious Interests to exhaust the PIT resources at routers reserved for subsequent Interests from legitimate users, which disrupts the service for legitimate users.

The IFA can be divided into three types based on the type of content requested by attackers [8]: (1) existing or static, (2) dynamically-generated, (3) unsatisfiable Interests. In the above three types, type (3) is the most widely studied and is also the type our work focuses on. In this kind of IFA, attackers issue unsatisfiable Interests for unique non-existent content. Such Interests cannot be satisfied by any network nodes nor be collapsed by intermediate routers. Namely, the PIT entries for malicious Interests stored at intermediate routers would stay as long as possible and the PIT space used by such Interests would not be released until their lifetime expires, in order to achieve better attack effect.

B. *Existing countermeasures against Interest flooding*

As a newly proposed future Internet architecture, NDN has been widely recognized to be viable in the future. For the better development of the new infrastructure, many researchers focusing on the security issue have proposed several approaches to identify and mitigate DDoS attacks in NDN, especially the IFA.

Gasti *et al.* [8] made the first step to formulate DoS/DDoS in NDN. They discussed how NDN deals with the existing DoS/DDoS attacks in the current TCP/IP network. NDN's built-in security features protect NDN from certain attacks such as, *black-holing and prefix hijacking*, *reflection attacks* and *DNS cache poisoning*. Then they further introduced two NDN-specific DDoS attacks called *interest flooding attack* targeting the PIT and *content/cache poisoning* aiming at the contents. For IFA, they provided a set of potential countermeasures and classified them into two categories: (1) router statistics and (2) push-back mechanisms, but no assessment or evaluation was presented.

Afanasyev *et al.* [6] presented three countermeasures: (1) *token bucket with per interface fairness*, (2) *satisfaction-based Interest acceptance*, (3) *satisfaction-based pushback*, which all utilize NDN's inherent properties of storing per packet state on each router and maintaining flow balance. Evaluations showed that the third approach, where the Interest limit of each incoming interface directly relies on the interface's satisfaction ratio, is the most effective. This proposal relies on only the local metrics of a router to detect an IFA attack.

In [4], Dai *et al.* assessed the harmful consequences of an IFA and proposed *Interest traceback*. This proposal detects an attack when a router's PIT size exceeds the threshold and then routers generate spoofed Data packets to satisfy long-unsatisfied Interests to trace back to the Interest issuers after detecting an attack. *Interest traceback* detects IFA by simply monitoring the PIT usage, which may classify short burst of Interest as attack and thus cause damage the legitimate Interests.

Al-Sheikh *et al.* [9] classified and compared existing countermeasures against IFA at that time in a consistent setup. The results showed that prefix-based mechanisms work better than all the other approaches which can be a good reference for subsequent researches.

Xie *et al.* [7] claimed that the existing detection methods, mainly based on the PIT statistics, may cause misjudgment, especially in the case of low-rate IFA. Afterwards, they represented a novel scheme based on cumulative entropy and relative entropy theory in NDN which can avoid all the drawbacks of existing countermeasures. However, it is difficult for such a low-rate IFA to take effect as it requires the number of attackers to be huge.

In [5], Compagno *et al.* introduced *Poseidon*, a collaborative approach which is also known as push-back discussed in [8]. *Poseidon* detects the attack when at least one router finds that both the satisfaction ratio and PIT usage of Interests arrived on a particular interface exceed their respective thresholds. When a router identifies an IFA on a certain interface, it limits the rate of incoming Interests from that interface and issues a push-back "alert" message, which contains detailed information about the attack, to the node connected to the offending interface. A node will decrease its thresholds after receiving an alert message, aiming to detect the attack early. However, collaboration of each router in *Poseidon* appears only during the mitigation phase and the negative attack effect may have already last for some time when a router, generally the node directly connected to the data producer and under the most serious attack, first detects the attack.

Salah *et al.* [10][11] proposed a central-control framework called CoMon, aiming to detect and mitigate IFA at early stage based on the aggregated traffic and forwarding states. In CoMon, a set of routers are pointed to be *Monitoring Routers (MRs)* based on their location and closeness to the data producer. *MRs* monitor the traffic passing through them and report their observations to *Domain Controller (DC)*. The *DC* summarizes all the reported information to determine whether there is an ongoing attack. CoMon can work efficiently when the network topology is static. However, it reaches its limits when faced with the IFA in a real-word network because *MRs* in CoMon are all predetermined but the network states, such as the distribution of clients and relationships between different nodes, are always changing in reality. Our tentative countermeasure against IFA may potentially overcome this drawback, as the controller dynamically decides which routers should report their state information based on all the received and constantly incoming abnormal information from access routers.

As one of the most recent works, the work [12] made a comprehensive survey on the proposed detection and mitigation of IFA. The comparable analysis showed that most of the current attack detection schemes are based on the states, especially the satisfaction ratio and PIT size, of either a router or each interface of a router. The proposed countermeasures are mainly limiting the Interests and/or sending an alert to other nodes after detecting an attack.

The commonality of existing works on IFA is that they focus on the scenario that attackers send spoofed Interests at a constant rate. Namely, most of them target at the high-speed IFA and rely on a single router's independent decision based on some metrics, such as PIT usage and satisfaction ratio of Interests, to detect an IFA. However, carefully-crafted attackers may manage to launch a more sophisticated IFA to keep the changes of router statistics much more slightly, making it more difficult for a single intermediate router to timely detect by itself, at least at the early stage of the attack. Therefore, our work focuses on such a sophisticated IFA. We explore the specific characteristics of the sophisticated IFA by an experimental study and further discuss a potentially more effective and timely mechanism against it.

III. Attack Scenario

In this section, we analyze the common IFA, a constantly high-speed one, and then introduce the sophisticated attack scenario we proposed.

PIT is one of the three major modules in a NDN router which contains the state information for each forwarded Interest, i.e. a PIT entry. When a router's PIT is completely filled up with malicious Interests which will never be satisfied, it will have no space available to create PIT entries for legitimate Interests, making the service for legitimate users disrupt.

On the one hand, when attackers send spoofed Interests at a relatively low rate, no router's PIT can be overwhelmed and users' requests will not be significantly affected, which makes no sense for attackers. On the other hand, the NDN-specific feature that stateful routers can easily keep track of much more information about carried traffic makes a router sensitive to the changes of its statistics. When attackers launch a fierce attack directly at an extremely high speed, even a single access router, the closest intermediate router to attackers, can detect abnormalities quickly and then take defensive measures, which prevents the expected attack effect from being achieved.

It is worth noting that if only the rate that the router adds entries to its PIT is higher than the rate that it removes, its PIT will be exhausted. Then the victim router would discard the subsequent incoming Interests, both malicious and legitimate ones, which disrupts the service for legitimate users.

Based on the above analysis, we propose a more sophisticated IFA scenario. In this scenario, carefully-crafted attackers send out malicious Interests at a relatively lower initial rate at the beginning of the attack. In this way, attackers can make sure that the PIT increasing rate is below a certain level. Afterwards, they speed up step by step in order to keep the size of routers' PIT-s gradually growing to exhaust the victim's PIT. In such a case, it is relatively difficult for an intermediate router near the attackers to timely detect the attack by itself due to the inconspicuous changes to its state information between two consecutive intervals.

Fig. 1 illustrates such a sophisticated IFA scenario. The malicious traffic does relatively little effect to each pure access router (i.e. only connected to clients), including R1, R2 and R3. But R7, the router directly connected to the content provider, is under the most serious attack due to the aggregation of malicious traffic. So it is the first to be overwhelmed among all the routers. In such a scenario, attackers are easier to launch a successful IFA because R7 starts to drop legitimate Interests earlier before the intermediate routers near the attackers detect the attack due to the slighter changes of router statistics.

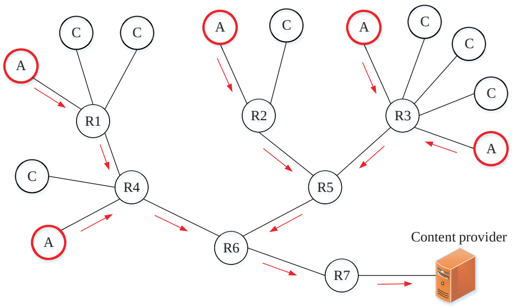

Fig. 1. A sophisticated attack by distributed attackers. Malicious Interests are routed to the same content provider. The nodes with 'A' represent attackers while 'C' represents legitimate clients. And the red arrows beside the line between nodes stand for the routing paths of malicious Interests.

IV. An Experimental Study

This section explores the characteristics of our proposed sophisticated IFA via an insightful experimental study. The work of this section is divided into two parts. First we examine the differences between the sophisticated IFA and the common one (i.e. attackers send malicious Interests at a constantly high speed directly) from different aspects. Second, we investigate the specific characteristics of the proposed scenario.

We used the open-source ndnSIM [13] package, a NS-3 based NDN simulator to run our simulations. Our experiment platform is: Xeon E5-2603 CPU, 1.60GHz, 15G RAM. We ran our simulations under an ISP-like topology which is based on a modified version of Rocketfuel's AT&T topology [14]. The topology comprises of 176 nodes, including 130 clients, 33 gateways (i.e. access routers, which are directly connected to clients), and 13 backbones (i.e. routers that are directly connected to other routers). The PIT sizes for gateways and backbones is equal to, in numeral, the number of tokens (the pending *Interest Limit*) in [6].

In our experiment, we assumed that legitimate users express Interests at constant average rates with randomized time gap between two consecutive Interests, where the random number for the gap follows a uniform distribution. We believe that this traffic pattern can provide a reasonable approximation of traffic mix from all network users without excessive buffering [6].

Before an attack, attackers do as what legitimate users do, i.e. send legitimate Interests at the same rate as legitimate users. After the attack starts, attackers send spoofed Interests at a relatively lower initial rate but speed up step by step.

In our experiments, we randomly picked 13 clients (10% out of 130 clients in the topology) as malicious nodes and randomly place the data producer at either a gateway or a backbone node. The life time of each Interest is set to 1s. The initial rate of spoofed Interests is 1/3 of the legitimate ones and the attacking speed increases at a speed of approximately 3% and 5% higher per second. The attack starts in the 60ths and lasts for 4 minutes. For each experiment, we conducted 10 runs to randomize the results to get an average result.

A. *Differences with the high-speed attack scenario*

In this section, we mainly focus on the different states of gateway nodes, the closest routers to attackers, under different attack scenarios. As it is impractical for each router to constantly maintain the state information of each interface due to the massive amounts of resource consumption, we deal with the statistics at the level of a whole router as the first step. We fix the high attack rate as high as 1000 spoofed Interests per second.

Our comparative results for the same gateway node under different attack speeds are shown in Fig. 2, Fig. 3, Fig. 4 and Fig. 5. The legends shown in the four figures stand for different attack speeds: speedup-3% (approximately 3% higher per second), speedup-5% (approximately 5% higher per second) and high-rate (constantly 1000 Interests per second) respectively. Note that the satisfaction ratio represented in Fig. 2 is for the entire node, i.e. the sum of satisfied Interests divided by the sum of incoming ones of all interfaces. The displayed gateway node is connected to 1 malicious node and 4 legitimate users.

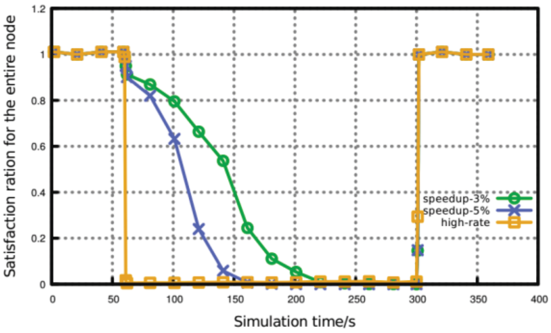

Fig. 2. Satisfaction ration of all the incoming Interests for the entire node

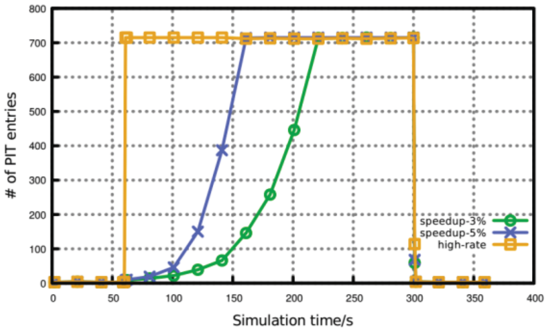

Fig. 3. The # of PIT entries of the node

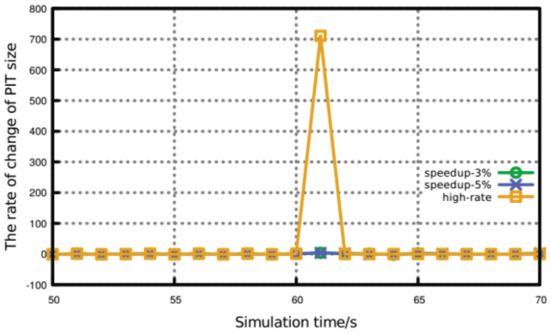

Fig. 4. The rate of change of PIT size of the gateway node (10 seconds before or after the attack starts)

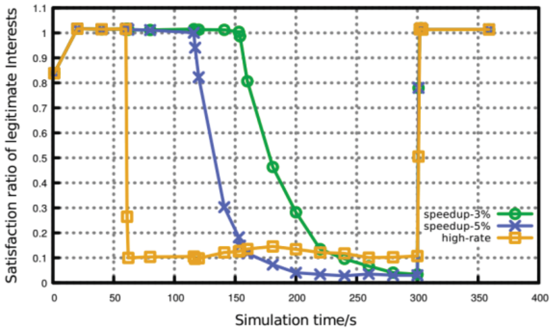

Fig. 5. The satisfaction ratio of legitimate Interests

As Fig. 2 and Fig. 3 imply, when the node is under a fierce attack, there are extremely significant changes to the # of PIT entries and satisfaction ratio of the node within an extremely short time, less than 2 seconds in our simulation. Such significant changes can be detected immediately by the gateway node, the intermediate router closest to attackers, after the attack starts. In this case, the time interval between the start of the attack and the time the attack is discovered and stopped is extremely short, making the attack just have limited effect on the network.

In contrast, in our proposed attack scenario, both the PIT size and satisfaction ratio change gradually and much more slightly. As illustrated in Fig. 5, the satisfaction ration of legitimate users doesn't decrease at the early stage, but begin to decline gradually due to the increasing # of PIT entries after a certain amount of time. What's more, Fig. 4 demonstrates that the fastest increasing rate (711 entries/s) of PIT size under the high-rate attack occurs in the 61ths, the first second of the attack duration. However, there is evidently no significant increase (both 4 entries/s) in the PIT size of the gateway node in such sophisticated attack, which makes the attack much subtler. The higher the speed is, the faster the rate of changes are and potentially the easier for the attack to be detected.

So in such a sophisticated attack scenario, attackers keep the # of PIT entries increasing so subtle that it is difficult for any intermediate router near the attackers to discover the attack. And then the PIT resources of routers are eventually depleted and cannot serve the requests from legitimate users as illustrated in Fig. 3 and Fig. 5.

B. *Specific characteristics of the proposed attack scenario*

In this part, we investigate the specific characteristics of the network in the proposed attack scenario by comparing two typical kinds of intermediate routers on the paths from the attackers to the data producer: one backbone node directly connected to the data producer which is under the most serious attack and three corresponding gateway nodes directly connected to the attacker which are under the least attack. The results of the scenario with 13 attackers and 3% higher speed per second are shown as Fig. 6, Fig. 7 and Fig. 8, in which "bb-579" represents the selected backbone node and the corresponding gateway nodes are "gw-89", "gw-262" and "gw-424". There are three incoming interfaces of "bb-579" in total and the malicious Interests arrive from all the three interfaces.

It is evident that the router statistics of all the selected nodes change gradually and the states of gateway nodes change much more slightly. As Fig. 6 shows, the backbone's PIT size is much larger than the gateways at the same time due to the aggregation of malicious traffic. For each of the selected gateway nodes, the # of PIT entries is no more than 1/6 of the PIT size even when the backbone node's PIT is already exhausted. What's more, the PIT sizes of all selected nodes, even the backbone node under the most serious attack, increase gradually rather than growing sharply in a very short interval. Fig. 7 implies that the max increment speed of PIT size of the backbone node during the attack is 50 entries per second in the 61th s, the first second after the attack starts in our simulation. After overwhelmed by spoofed Interests in the 154th s, the backbone node drops the subsequent Interests. Then the PIT sizes of gateway nodes begin to increase at a higher rate due to the increasing # of PIT entries for dropped legitimate Interests as well as the malicious ones. The same phenomenon of gradual changes is also appeared in Fig. 8, which shows the satisfaction ratio of Interests on each incoming interface of the backbone node.

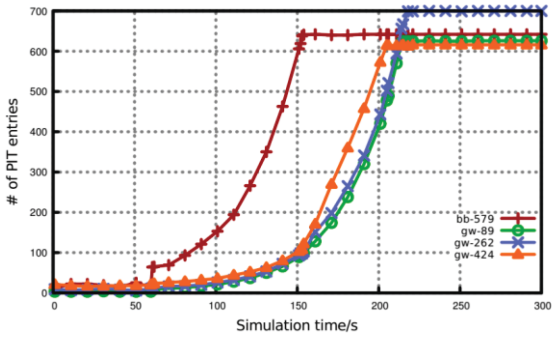

Fig. 6. The # of PIT entries in the backbone node and corresponding gateway nodes

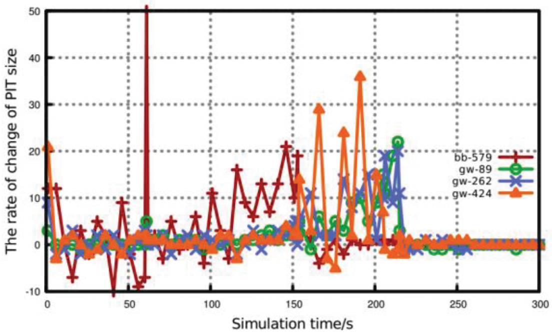

Fig. 7. The rate of change of PIT size of the backbone node and corresponding gateway nodes before or during the attack

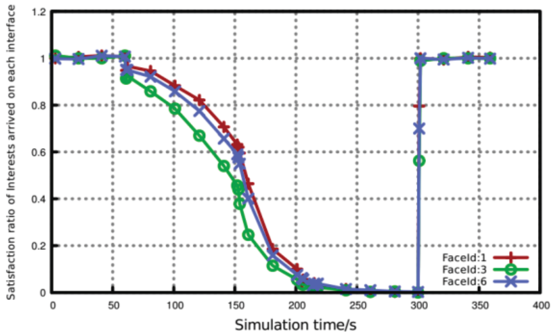

Fig. 8. The satisfaction ratio of Interests arrived on each interface of the backbone node

We tentatively set the same detection phase as [5] (i.e. both the satisfaction ratio and PIT usage of Interests arrived on a certain interface exceed their thresholds respectively) on both the two backbone nodes directly connected to the data producer, which should be the earliest to detect an attack. The time points when the attack is detected are shown as TABLE I. The backbone node "bb-579" is the first to detect the attack on its face 3 in the 156ths when the attack has already last for 96s. The data accesses of legitimate users have been negatively affected for 14s when all the faces of the two backbone nodes can detect the attack. The rest nodes far away from the data producer in the topology would discover the attack even later.

TABLE I. TIME POINTS

Node	**bb-579**			**bb-578**
FaceId	1	3	6	5
Time when the attack is identified	168ths	156ths	166ths	168ths
Timespan from attack starts	108s	96s	106s	108s
Timespan from ratio of satisfied legitimate Interests declines	14s	2s	12s	14s

V. DISCUSSION & CONCLUSION

In this paper, we proposed a new sophisticated attack scenario of IFA, in which compromised hosts start the attack with a relatively low initial rate but speed up step by step afterwards. Our experimental study showed that such an attack is much more sophisticated and furtive, and the existing countermeasures against IFA cannot detect it timely.

Most of the previously proposed countermeasures against IFA identify an attack mainly based on the independent decision of each single router in the topology. That said whether their local statistics, such as the unsatisfied ratio and PIT usage of Interests arrived on an interface, reach specific state at some point if there is an IFA in progress. Such countermeasures may work effectively when faced with the high-speed attacks in which a router's statistics change rapidly and immediately after the attack starts. But they are somewhat limited in a more sophisticated IFA where the changes of router statistics are much slighter, making it harder for a single intermediate router to detect timely by itself.

Our work proposed a more sophisticated scenario that carefully-crafted attackers can keep the increasing rate of PIT size below a certain level by controlling the number and distribution of compromised hosts, and realize the gradual changes of router statistics. Our experimental study showed that the changes of router statistics are subtler in the proposed scenario compared to the high-speed one, making existing countermeasures relying on a single immediate router's independent decision harder to detect in time.

NDN weakens the concept of address, which can protect the privacies of users but makes it difficult to locate attackers. There is no doubt that the earlier to detect an attack and locate attackers, the better performance a countermeasure can achieve and the less harm will be done to the network. The fastest way to locate attackers in NDN is making efficient use of the access routers which attackers are directly connected to. But it is quite difficult for a single access router to detect the attack relying on itself in such sophisticated scenario due to the slighter changes of its router statistics. In addition, in most of the existing countermeasures, even each interface of all the routers is required to perform attack detection and mitigation, which would cause great consumption of computing resources. And collaborative mechanisms would also cause extra high communication overhead because routers in such mechanisms are required to communicate with each other.

Based on the experimental study results, we propose a potential mechanism with central controller against the proposed sophisticated IFA which mainly focuses on the changing trend of the network. The central controller continuously monitors the whole network from a global view and can exchange information with each node in the network. The controller always makes decisions based on the overall situation of the network. In order to perform attack detection close to sources and avoid excessive resource consumption, all access routers which are directly connected to attackers or legitimate users, rather than all routers in the topology, are responsible for monitoring the state of the network. When an access router finds something abnormal, such as the phenomenon that the PIT size keeps increasing over a relatively long period of time as shown in Fig. 3 while the increasing rate of # of PIT entries is always relatively low as shown in Fig. 4, but it is not sure whether there is really an attack in progress, it begins to periodically send alert messages to the central controller. An alert message contains detailed information about the abnormality such as the namespace and rate of the abnormal traffic. With a global view, the controller dynamically determines which nodes in the topology may be under the more serious attack based on the received and continually coming alert messages and makes a comprehensive judgment. If the controller finds that there is indeed an ongoing IFA in the network, it will send commands to related routers under attack, ordering them to take defensive countermeasures. In such mechanism, the controller can potentially detect an IFA timely before the attack causes a bad effect on the network. In addition, it can also directly locate attackers through the access routers, which can prevent malicious Interests from entering the network as soon as possible.

We believe that with a central controller monitoring the whole network from a global view, the mechanism can detect the sophisticated IFA and locate attackers effectively and timely before the attack really takes effects. Our future work is the concrete design and implementation details of the proposed mechanism.

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 Jiangsu Provincial Key Laboratory of Computer Network Technology.

References

[1] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. Braynard, "Networking named content," in *Proceedings of the 2009 ACM Conference on Emerging Networking Experiments and Technology, CoNEXT 2009*, Rome, Italy, December 2009, pp. 1–12.

[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] S. Choi, K. Kim S. Kim and B.h.Roh, "Threat of DoS by Interest Flooding Attack in Content-Centric Networking," *in 2013 International Conference on Information Centric Networking, ICOIN 2013*, Bangkok, 2013, pp. 315-319.

[4] H. Dai, Y. Wang, J. Fan, and B. Liu, "Mitigate ddos attacks in ndn by interest traceback," in *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, April 2013, pp. 381–386.

[5] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating interest flooding ddos attacks in named data networking," in *38th Annual IEEE Conference on Local Computer Networks*, Sydney, Australia, October 2013, pp. 630–638.

[6] 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, May 2013, pp. 1–9.

[7] Y. Xin, Y. Li, W. Wang, W. Li, and X. Chen, "A novel interest flooding attacks detection and countermeasure scheme in NDN," in *2016 IEEE Global Communications Conference, GLOBECOM 2016*, Washington, DC, USA, December 2016, pp. 1–7.

[8] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and ddos in named data networking," in *22nd International Conference on Computer Communication and Networks, ICCCN 2013*, Nassau, Bahamas, 2013, pp. 1–7.

[9] S. Al-Sheikh, M. W ählisch, and T. C. Schmidt, "Revisiting countermeasures against NDN interest flooding," in *Proceedings of the 2nd International Conference on Information-Centric Networking, ICN '15*, San Francisco, California, USA, 2015, pp. 195–196.

[10] H. Salah, J. Wulfheide, and T. Strufe, “Lightweight coordinated defence against interest flooding attacks in NDN,” in *2015 IEEE Conference on Computer Communications Workshops, INFOCOM Workshops,* Hong Kong, China, 2015, pp. 103–104.

[11] H. Salah, J. Wulfheide, and T. Strufe, “Coordination supports security: A new defence mechanism against interest flooding in NDN,” in *40th IEEE Conference on Local Computer Networks, LCN 2015*, Clearwater Beach, FL, USA, October 2015, pp. 73–81.

[12] S. Rai and D. Dhakal, “A survey on detection and mitigation of interest flooding attack in named data networking,” in *Advanced Computational and Communication Paradigms*, 2018, pp. 523–531.

[13] A. Afanasyev, I. Moiseenko, and L. Zhang, “ndnSIM: NDN simulator for NS-3,” NDN, Technical Report NDN-0005, October 2012.

[14] N. T. Spring, R. Mahajan, and D. Wetherall, “Measuring ISP topologies with rocketfuel,” in *Proceedings of the ACM SIGCOMM 2002 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, Pittsburgh, PA, USA, August 2002, pp. 133–145.