Isolation Forest-Based Mechanism to Defend against Interest Flooding Attacks in Named Data Networking

Guanglin Xing, Jing Chen, Rui Hou, Lingyun Zhou, Mianxiong Dong, Deze Zeng, Jiangtao Luo, and Maode Ma

The authors introduce the concept of an isolation forest (iForest) to develop an IFA detection mechanism in which the iForest construction process isolates abnormal and legitimate prefixes. This approach enables malicious prefixes to be identified among abnormal prefixes to mitigate IFAs by restricting the forwarding of malicious Interest packets.

Abstract

Interest flooding attacks (IFAs) are widely regarded as being among the most harmful security risks in named data networking (NDN). Through an IFA, the attacker injects numerous Interest packets into a network to drain network resources such as bandwidth, caching capacity, and computational capacity, which can seriously affect the normal data content requests of legitimate consumers and degrade the network quality of service (QoS). To design a high-efficiency IFA mitigation scheme, it is critical to detect attacks accurately and rapidly. Therefore, there is high interest in developing an optimized attack detection scheme. In this study, the concept of an isolation forest (iForest) is introduced to develop an IFA detection mechanism in which the iForest construction process isolates abnormal and legitimate prefixes. This approach enables malicious prefixes to be identified among abnormal prefixes to mitigate IFAs by restricting the forwarding of malicious Interest packets. The results of extensive simulations show that the proposed iForest-based IFA detection mechanism (IFDM) outperforms other related schemes in terms of attack detection accuracy and speed and thus can offer effective support for preserving NDN QoS.

Introduction

Named data networking (NDN) is one type of deployment for information-centric networking (ICN). It is an emerging network architecture widely recognized as a promising next-generation Internet architecture candidate thanks to its distinct features that support name-based content sharing, coupling routing, mobility support, Internet-of-Things, etc. [1–3]. In an NDN, each data object is assigned a unique name that consists of a globally routable prefix and a specific suffix, which is an identifier generated by the data content owner (i.e., the *Producer*). If a user (i.e., a *Consumer*) intends to access specific data content, an Interest packet is generated containing the name of the desired data contents and is sent to the NDN as a request explore the data contents. When the Producer receives the Interest packet, it encapsulates the corresponding data contents requested by the Consumer into a *Data* packet with the same name and returns it to the Consumer along the reverse path of the Interest packet.

As in other types of networking paradigms, security is intensively considered in the NDN protocol stack design. Consequently, NDN is intrinsically able to resist many typical kinds of network attacks, such as bandwidth depletion attacks, reflection attacks, and black-holing by prefix hijacking [4]. However, in recent years, a new type of distributed denial of service (DDoS) attack specifically aimed at NDNs has emerged, called an interest flooding attack (IFA) [5]. IFAs work based on the idea that the information in each Interest packet will be recorded by the pending interest table (PIT) of an NDN router during its forwarding process. The record will be preserved until either the router receives a corresponding Data packet or the PIT timeout interval elapses. Consequently, attackers can create large numbers of Interest packets and inject them into the network to fill up the PIT capacity, link bandwidth, computation capacity, and other network resources and degrade the quality of service (QoS) provided to legitimate Consumers. Depending on the type of data content requested by an attacker, an IFA can be implemented in any of the following three ways.

1. Using a static attack, the attacker generates Interest packets to request an existing content item. In this situation, the NDN distributed caching function can handle the requests, effectively mitigating the harm caused by the IFA.
2. Using a dynamic attack, the attacker creates Interest packets dynamically to request different existing content items. In this case, the NDN routers must handle each request by creating a PIT record and transmitting an Interest packet according to the forwarding information base (FIB) to explore the Producers. This process consumes substantial caching and computation resources of both routers and Producers.
3. Using a non-existent attack, termed a malicious attack in this article, the attacker creates Interest packets that correspond

Guanglin Xing, Jing Chen, Rui Hou, and Lingyun Zhou are with South-Central University for Nationalities; Mianxiong Dong is with the Muroran Institute of Technology; Deze Zeng is with China University of Geosciences; Jiangtao Luo is with Chongqing University of Posts and Telecommunications; Maode Ma is with Nanyang Technological University, Nanyang Technology University. Rui Hou is the corresponding author.

Digital Object Identifier:
10.1109/MCOM.001.2000368

to non-existent content items. To increase the detection difficulty, the names of these Interest packets have the form "/legitimate_prefix/non-existent_suffix/," where "/legitimate_prefix/" is a name prefix that exists in the network, while "/non-existent_suffix/" is a randomly forged suffix. Because no satisfactory Data packets can be generated, the PIT entries of the NDN router will remain occupied until their lifetimes expire. Compared with static and dynamic attacks, malicious attacks have more destructive effects on the NDN core network: they are easy to implement and can cause the NDN routers to malfunction or even become disabled, making such attacks difficult to counteract. Consequently, most attacks on NDNs are malicious attacks.

IFAs are already among the most prevalent and destructive types of network attacks addressed in NDN security research. Consequently, they have attracted increasing attention in the academic community in recent years. The existing research on IFA detection has mainly focused on PIT state information (such as the PIT occupation ratio and the number of received Data packets) to identify abnormal scenarios and determine attacks. However, if the PIT of an upstream router is fully occupied by malicious Interest requests records, it will discard subsequent Interest packets, including both legitimate and malicious Interest packets, which will affect the data content requests of legitimate Consumers and can even result in the routers misjudging legitimate Interest packets as malicious Interest requests. To improve attack detection accuracy, an isolation forest (iForest)-based IFA detection mechanism (IFDM) is developed in this study that reduces misjudgments and enables efficient recognition of attacking Interest requests. When an IFA occurs, the number of Interest packets with specific prefixes increases abnormally, and the IFDM can identify the malicious prefixes used by the attackers by constructing an iForest where routers can compare the characteristics among prefixes. Thus, this approach can reduce the negative effects caused by IFA detection misjudgments.

Related Works

In 2009, Jacobson *et al.* [5] first proposed the concept of an IFA, its generation mechanism, and attack features in a content-centric network. Since then, IFAs have attracted increasing attention. Dai *et al.* [6] proposed an Interest traceback mechanism to mitigate IFAs, by which NDN routers generate spoofed Data packets, that are intentionally created to satisfy the suspicious Interest requests and to identify the interfaces connected with the attackers after a router detects an abnormal PIT status. Afanasyev *et al.* [7] investigated three algorithms to mitigate IFAs based on the idea that an Interest packet corresponds to at most one Data packet. Satisfaction-based pushback algorithms are explored to prevent overreactions and unfair penalization. Similarly, Compagno *et al.* [8] proposed an IFA countermeasure mechanism called Poseidon, in which an NDN router calculates the ratio between the numbers of incoming Interest packets and outgoing Data packets for all interfaces along with the PIT usage. If these two parameters exceed preset thresholds, the router determines that an attack is occurring and mitigates it by restricting the input of Interest packets and sending a warning message to adjacent routers. To locate the attacking source accurately for effective IFA mitigation, Vassilakis *et al.* [9] divided Consumers into three categories, including legitimate Consumers, suspicious Consumers, and attackers, based on the numbers of expired PIT entries at the edge routers. Then, they take different actions for different types of consumers. Furthermore, Xue *et al.* [10] proposed an IFA detection mechanism that works at edge routers directly connected to Consumers and identifies malicious prefixes by calculating the Interest satisfaction ratio (ISR), which is the ratio between the numbers of received Data responses and transmitted Interest requests at each interface of the edge router. Then, malicious Interest packets are restricted according to a preset ISR threshold. To improve the recognition accuracy, Xin *et al.* [11] presented an IFA defense method based on cumulative and relative entropy, in which cumulative entropy is used to calculate the distribution of Interest packet names to detect abnormal requests, and relative entropy is used to identify malicious prefixes and restrict attacker behavior by using an Interest traceback approach. Zhi *et al.* [12] proposed a Gini impurity-based IFA detection method that effectively reduces the misjudgment rate and distinguishes malicious prefixes. Similarly, according to the name distribution of interest packets, Hou et al [13] proposed an IFA defense method based on Theil index, which divides interest packets into intra-group and inter-group, and detects IFA by the variation of intra-group and inter-group differences. However, these mechanisms may have limitations when attackers use more covert interest pakcet names. Zhang *et al.* [14] comprehensively analyzed the benefits of the NDN architecture to defend against DDoS attacks, especially Interest flooding, and proposed a fine-grained Interest traffic-throttling method that limits malicious Interest traffic by offloading negative acknowledgements (NACK) packets to edge routers.

To further reduce misjudgments, improve the attack detection accuracy, and diminish the impact on legitimate Consumers, this paper introduces the idea of IForest which originated in the data mining field [15], and develops an IFDM to enable more effective attack recognition. Regarding the essence and features of the IFA, attackers always use parts of existing prefixes to generate malicious Interest packets and send them at a high rate. Consequently, these prefixes will show characteristics that differ from those of legitimate prefixes. Through the IFDM, an iForest is constructed to categorize malicious and legitimate prefixes based on two considerations: first, the number of malicious prefixes is much smaller than the total number of existing prefixes in the NDN, and second, the representations of malicious prefixes are different from those of legitimate prefixes.

Through the IFDM, an iForest is constructed to categorize malicious and legitimate prefixes based on two considerations: first, the number of malicious prefixes is much smaller than the total number of existing prefixes in the NDN, and second, the representations of malicious prefixes are different from those of legitimate prefixes.

iForest-Based IFA Countermeasure

During IFA detection, according to the name prefix, each NDN router performs a round of attack detection at a fixed time interval to identify malicious prefixes. This section first describes the pre-

When a router detects an attack, an IFA mitigation function will be triggered, after which the NDN router will send notification packets and restrict the forwarding of subsequent malicious Interest packets. That is, after a router detects an attack and has identified a malicious prefix, it generates a notification packet and forwards it to downstream routers.

fix data construction and then discusses IFDM for attack detection in detail.

Prefix Data Construction

During each detection cycle, according to the name prefix, the NDN router counts the number of sent Interest packets (SIP_NUM), received Data packets (RDP_NUM), entries recorded in the PIT (RP_NUM), and expired PIT entries (EP_NUM) in real time. Then, these four statistical values are used as name prefix attributes to construct a prefix data table. For example, during a specific detection period, if a router sends seven Interest packets with the name prefix "/prefix_01/" and receives five Data packets with the same name prefix, then there will be two entries with "/prefix_01/" recorded in the PIT, and no PIT entries where "/prefix_01/" has expired. Thus, the prefix data for "/prefix_01/" can be constructed as follows: SIP_NUM = 7, RDP_NUM = 5, RP_NUM = 2, and EP_NUM = 0.

Detection Process

This section describes how to construct an iForest to separate malicious prefixes from legitimate prefixes in the NDN to achieve IFA detection. An iForest is composed of isolation trees (iTrees) that have a binary tree structure. From the prefix data set, n different prefix data are selected to serve as a training set for iTree construction. The process of building an iTree is as follows. First, an attribute q is randomly selected from SIP_NUM, RDP_NUM, RP_NUM, and EP_NUM and used as an isolation attribute. Then, an isolation value p is randomly selected from the range between the minimum and maximum values of the isolation attribute values in the training set. Here, q and p constitute the isolation information stored in an internal node of the iTree such that the prefix data in the training set with values less than p form the left child node, while those with values equal to or larger than p form the right child node. The prefix data in the left and right child nodes are recursively selected and divided until one of the following three conditions is satisfied:

1. The iTree reaches a predetermined height limit (which is approximately the average tree height) [15]
2. The attributes and values of the remaining prefix data are all identical
3. The prefix data can no longer be divided.

Following this procedure and these rules, an iTree is constructed, and all the prefix data in the training set are stored in the external nodes (leaf nodes). By randomly selecting prefix data many times to form different training sets, many iTrees can be constructed, forming an iForest. Then, when an IFA occurs in the NDN, it is easy to separate the malicious prefixes in the isolation process due to their characteristics: the malicious prefixes will be isolated close to the root node of the tree and have short path lengths, while the legitimate prefixes will be isolated further from the root node and have longer path lengths.

After the iForest is constructed, all the prefix data are traversed through each iTree based on the isolation information in the node, and the path length, which reflects the number of edges that the prefix data must traverse from the root node to the external node, will be recorded. After the prefix data traverse all iTrees, multiple path lengths will be obtained. By using these path lengths, the average path length, which is the ratio of the total path length to the number of trees, can be calculated.

The result is that prefix data with shorter average path lengths are more likely to be malicious, while prefix data with longer average path lengths are less likely to be malicious. To reflect anomalies in the prefix data more clearly, an abnormality score can be calculated to describe the prefix data based on the average path length of an unsuccessful search in a binary search tree (BST) [15]. Then, the abnormal scores of all the prefix data are sorted from large to small, and the following properties exist:

1. If the abnormality score of the prefix data is close to 1, it is highly likely that the prefix is malicious;
2. If the abnormality score of the prefix data is less than 0.5, the prefix can be designated as legitimate;
3. If the abnormality scores of all prefix data are approximately 0.5, there is no malicious prefix.

Based on these properties, if the abnormality score of the prefix data exceeds a threshold Th, then the prefix data are considered abnormal. At the same time, to avoid the effects of traffic fluctuations, a prefix with a PIT occupancy rate higher than Tr among the abnormal prefixes is considered a malicious prefix.

In the iForest construction stage, t iTrees must be built, and therefore the time complexity is $O(tnlogn)$, where n is the size of the training set. In the prefix data traversal and analysis phase, the time complexity is $O(Ntlogn)$, where N is the size of all prefix data.

IFA Mitigation

When a router detects an attack, an IFA mitigation function will be triggered, after which the NDN router will send notification packets and restrict the forwarding of subsequent malicious Interest packets. That is, after a router detects an attack and has identified a malicious prefix, it generates a notification packet and forwards it to downstream routers. The notification packet contains the pertinent information about the detected malicious prefixes to inform the downstream routers of the attack. Moreover, it restricts forwarding of malicious Interest packets after the attack. Therefore, the PIT entries occupied by the malicious Interest packets in the router will expire, and the PIT size will gradually return to normal, minimizing the impact on legitimate Consumer requests.

Simulations

This section describes our evaluation experiments conducted from four perspectives to demonstrate the accuracy and efficiency of the IFDM approach. First, we verify the accuracy of the IFDM method when an attack appears. Then, we investigate the misjudgment avoidance performance during attack detection at different NDN routers. To demonstrate the efficiency of the IFDM approach, in the third experiment, we compare the performance of the IFDM method with three typical IFA countermeasures, i.e., the

expired-PIT-, entropy-, and Gini impurity-based mechanisms. Finally, the capabilities and effectiveness of the IFDM technique against IFAs are verified by changing the number of attackers.

Parameter Settings

As shown in Fig. 1, a binary tree structure is used as the simulation network topology because it is widely used as a typical topology to evaluate the performance of the IFA. It is widely regarded as one of the most delicate topologies and can be seriously affected by IFAs. Therefore, we selected the commonly used typical binary tree topology to verify the accuracy and efficiency of the proposed IFDM. In this topology, Interest packets are sent by both Consumers and attackers, and all the traffic will be forwarded to R1, which is the gateway of the content Producer, resulting in the accumulation of a large number of Interest packets. For simplicity, but without loss of generality, one content Producer, 15 NDN routers, 14 Consumers, and 2 attackers are used in this simulation. The simulation duration is 15 s, attack detection cycle is performed every 100 ms, and packets require 10 ms of transmission time for each hop. The maximum capacity of the PIT is set to 300 entries, and each PIT record has a lifetime of 500 ms. In the iForest, the size of training set n is set to 256, the number of iTrees is 100, and Th and Tr are set to 0.7 and 10 percent, respectively. In this simulation, the Consumers send legitimate Interest packets to request existing data content at a rate of 200 request per second (RPS), while the attackers launch an IFA at the fifth second by randomly sending malicious Interest packets to request non-existent data content at a rate of 1000 RPS.

IFDM Accuracy

To elucidate the effects of IFAs on the NDN and the accuracy of the proposed IFDM approach, the obtained implementation results are shown in Fig. 2, which presents the size of the PIT for router R1. As Fig. 2 shows, under non-attack conditions, the PIT size of R1 remains stable. However, when an attack occurs at an attack rate of 1000 RPS, the PIT will fill up rapidly because no corresponding Data responses will be able to satisfy the recorded Interest request entries. However, when the IFDM approach is applied to a network that experiences an IFA, the network's performance improves significantly, as shown in Fig. 2. The PIT can recover to normal status in approximately only 0.8 s after the attack begins since the IFDM approach detects the attack and mitigates it before the PIT is completely occupied.

IFDM Misjudgment Avoidance

As mentioned earlier, misjudgments often occur when NDN routers rely primarily on PIT status values such as the PIT expiration rate and ISR to identify attacks. In these cases, the router considers that an IFA is occurring when the values of the relevant PIT and ISR parameters exceed a preset threshold or the normal range. Then, the router reduces the Interest packet sending rate, which may affect legitimate users. To explain misjudgment more clearly, we compare the IFDM technique with the expired-PIT-based detection mechanism, as shown in Fig. 3, where "1" and

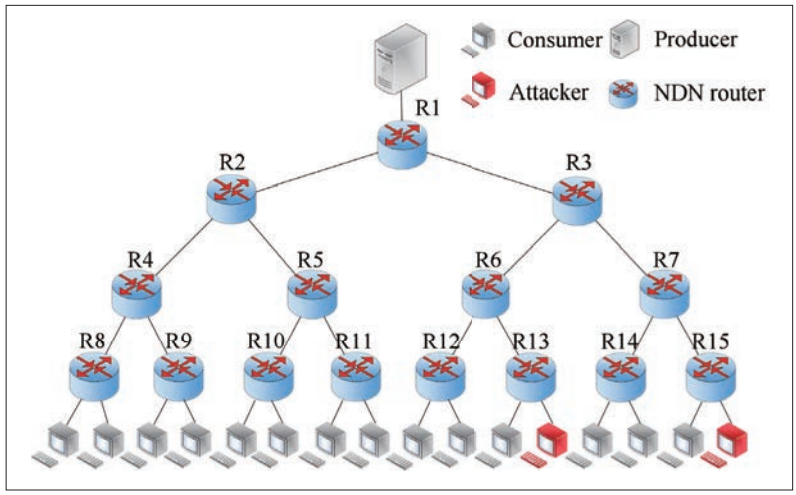

FIGURE 1. Binary tree topology used in the simulation.

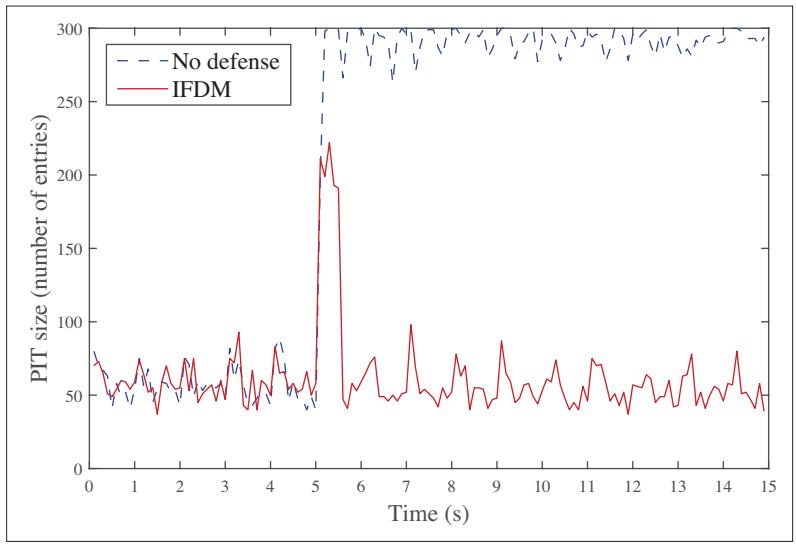

FIGURE 2. PIT size under IFDM and under no defense during attack.

"0" denote a detected attack and no attack, respectively. Although R12 connects with legitimate Consumers, the expired-PIT-based mechanism declares the occurrence of an IFA because malicious Interest packets occupy the PIT of its upstream router, causing no corresponding Data packets to be received and resulting in expired PIT entries in R12. As a result, R12 will make a misjudgment. In contrast, when the IFDM scheme is used, there will be no misjudgment in R12 under the same conditions. From Fig. 3, it is clear that for R13, which is directly connected to an attacker, while both the expired-PIT-based and IFDM mechanisms detect the attack, the IFDM approach achieves detection earlier. In fact, the expired-PIT-based mechanism must wait until the number of expired PIT entries reaches the threshold, resulting in a time delay.

IFDM Efficiency

To demonstrate the efficiency of the IFDM approach, we compare the IFA defense performances by the IFDM scheme with those of three other representative IFA countermeasures in this section. As shown in Fig. 4, at an attack rate of 1000 RPS, the PIT size increases rapidly after the attack is launched at the fifth second, causing the

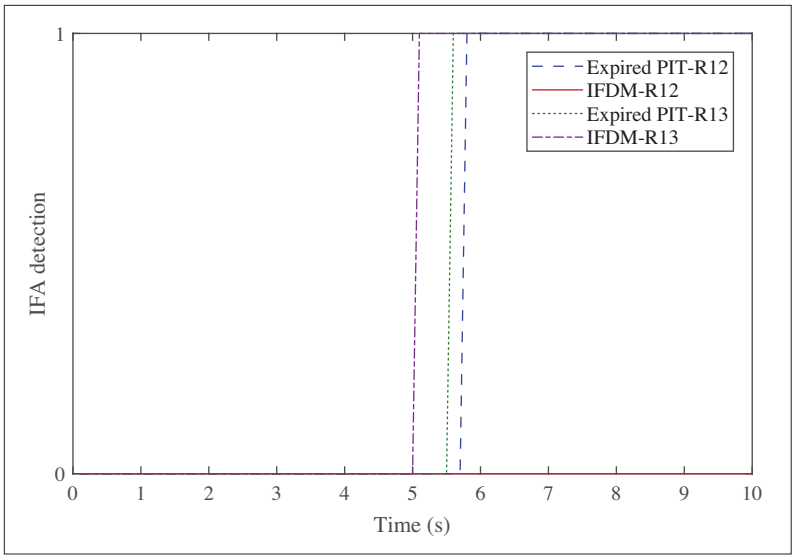

FIGURE 3. Detection of IFAs on routers R12 and R13.

expired-PIT-based mechanism to reach almost 100 percent, while the IFDM approach effectively restrains the rapid PIT size increase. In addition, the IFDM scheme returns the PIT to normality in the shortest time among the four IFA countermeasures. In fact, due to misjudgments, the expired-PIT-based mechanism regards some legitimate Consumers as suspicious Consumers or attackers and subsequently restricts their data requests. Consequently, the PIT size is smaller than normal during the later stage, and the number of Data packets received is greatly reduced. In contrast, the entropy- and Gini impurity-based mechanisms can restore the PIT size to normal after the IFA is detected. However, the entropy-based mechanism must wait for the cumulative entropy to increase continuously and exceed the threshold, leading to a longer detection time and relatively large PIT size. Furthermore, the number of Data packets received at the beginning of the attack is reduced. The performance of the Gini impurity-based mechanism is similar to that of the IFDM technique. Both approaches enable rapid attack detection, suppress the forwarding of malicious Interest packets, and maintain the number of Data packets received at a higher level. However, the PIT size resulting from the Gini impurity-based mechanism is larger than that under the IFDM. As shown in Fig. 4, the PIT size increase under each scheme, but the proposed IFDM scheme yields the smallest PIT size. Furthermore, the IFDM method ensures that data requests from legitimate Consumers are not suppressed; therefore, it effectively prevents IFAs from seriously affecting the network and Consumers.

Capability and Effectiveness of IFDM Against IFAs

The effectiveness of the IFDM scheme in response to different numbers of attackers in the network is verified by the results shown in Fig. 5. When there are two attackers, the IFDM scheme quickly detects the malicious prefixes and takes corresponding actions. As the number of attackers increases, numerous malicious Interest packets pour into the network, and the occupancy rate of the PIT increases substantially. When there are eight attackers, the PIT size increases rapidly, and its occupancy rate reaches 100 percent. Although the PIT size gradually increases as the number of attackers increases, it is still eventually reduced to the normal range, improving the QoS provided to Consumers.

Conclusions

IFAs can cause network security problems that cannot be ignored. This article proposed an IFDM scheme to defend against IFAs. Using the proposed approach, an iForest is used to isolate abnormal prefixes by calculating an abnormality score for each prefix datum. Then, malicious prefixes can be identified among the abnormal prefixes based on the numbers of PIT entries used. Furthermore, rate limitation is utilized to prevent malicious packets from entering the network, providing IFA mitigation. Finally, the simulation results demonstrated that the IFDM approach successfully reduces the misjudgments caused by packet losses after PIT overflow and improves the attack identification accuracy. Compared with several typical mechanisms, the IFDM scheme effectively reduces the occupation of PIT resources and improves the QoS of legitimate Consumers. Thus, the IFDM approach can effectively defend an NDN against IFAs. In future work, we plan to conduct research in more real-

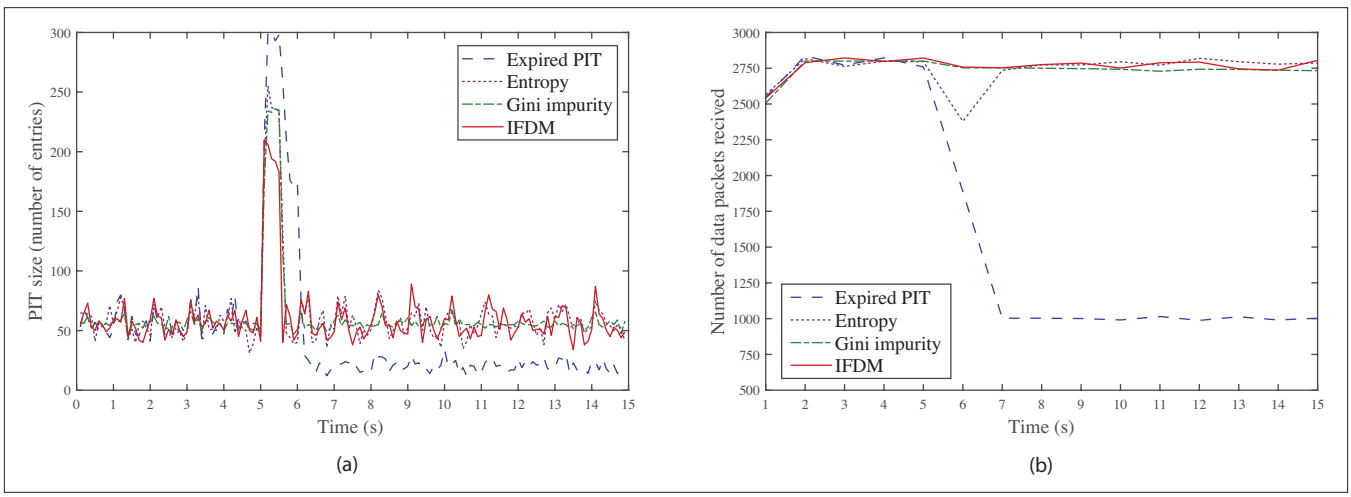

FIGURE 4. Comparison of the proposed IFDM approach with three other mechanisms: (a) PIT size; and (b) number of Data packets received.

istic network environments and with more complex attack models.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grant 61972424, JSPS KAKENHI under Grant JP20F20080, and the Special Fund for Basic Scientific Research of Central Colleges under Grant CZT20025. The authors thank all the anonymous reviewers for their valuable comments.

References

[1] L. Zhang *et al.*, "Named Data Networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, July 2014, pp. 66–73.
[2] D. Kim *et al.*, "Security of Cached Content in NDN," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, Dec. 2017, pp. 2933–44.
[3] M Amadeo *et al.*, "Information-Centric Networking for the Internet of Things: Challenges and Opportunities," *IEEE Network*, vol. 30, no. 2, Mar. 2016, pp. 92–100.
[4] P. Gasti *et al.*, "DoS and DDoS in Named Data Networking," *Proc. 22nd Int'l. Conf. Computer Commun. and Networks (ICCCN)*, Nassau, Bahamas, 2013, pp. 1–7.
[5] V. Jacobson *et al.*, "Networking Named Content," *Proc. 5th Int'l. Conf. Emerging Networking Experiments and Technologies (CoNEXT'09)*, Rome, Italy, 2009, pp. 1–12.
[6] H. Dai *et al.*, "Mitigate DDoS Attacks in NDN by Interest Traceback," *IEEE INFOCOM*, Turin, Italy, 2013, pp. 381–86.
[7] A. Afanasyev *et al.*, "Interest Flooding Attack and Countermeasures in Named Data Networking," *2013 IFIP Net. Conf.*, Brooklyn, NY, 2013, pp. 1–9.
[8] A. Compagno *et al.*, "Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking," *Proc. IEEE 38th Conf. Local Computer Networks (LCN)*, Sydney, NSW, 2013, pp. 630-638.
[9] V. Vassilakis, "Mitigating Distributed Denial-of-Service Attacks in Named Data Networking," *The 7th Advanced Int'l. Conf. Telecommunications (AICT)*, Brussels, Belgium, 2015.
[10] H. Xue *et al.*, "A Mechanism for Mitigating DoS Attack in ICN-based Internet of Things," *1st Int'l. Conf. Internet of Things and Machine Learning*, Liverpool, UK, 2017, pp.1-10.
[11] Y. Xin *et al.*, "A Novel Interest Flooding Attacks Detection and Countermeasure Scheme in NDN," *IEEE GLOBECOM*, Washington, DC, USA, 2016, pp. 1–7.
[12] T. Zhi, H. Luo, and Y. Liu, "A Gini Impurity-Based Interest Flooding Attack Defence Mechanism in NDN," *IEEE Commun. Lett.*, vol. 22, no. 3, Mar. 2018, pp. 538–41.
[13] R. Hou *et al.*, "Theil-Based Countermeasure Against Interest Flooding Attacks for Named Data Networks," *IEEE Network*, vol. 33, no. 3, May/Jun. 2019, pp. 116–21.
[14] Z. Zhang *et al.*, "Expect More from the Networking: DDoS Mitigation by FITT in Named Data Networking," arXiv preprint arXiv:1902.09033.
[15] F. T. Liu, K. M. Ting, and Z. Zhou, "Isolation Forest," *8th IEEE Int'l. Conf. Data Mining*, Pisa, 2008, pp. 413–22.

Biographies

Guanglin Xing (glxing@scuec.edu.cn) earned a Ph.D. in computer software and theory from the Huazhong University of Science and Technology in 2005. His main research fields include information-centric networking and intelligent algorithms.

Jing Chen (chenjing_stu@163.com) is currently working toward a M. Eng. degree at South-Central University for Nationalities. Her interest of research is information security in named data networking.

Rui Hou [M] (hourui@scuec.edu.cn) earned a Ph.D. from Huazhong University of Science and Technology in 2006. He has published over 100 works. His area of research include internetworking techniques, the future network architectures, and internet-of-things techniques. He is a member of CCF, IEEE and IEICE.

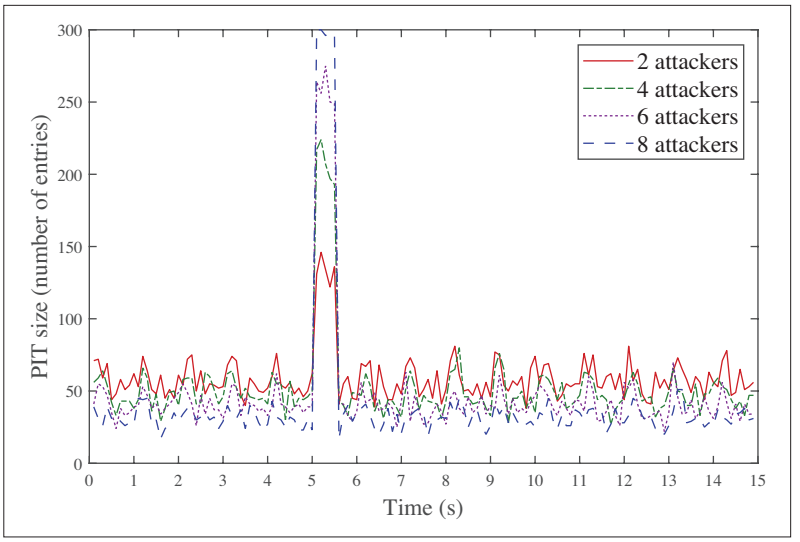

FIGURE 5. PIT size under different numbers of attackers.

Lingyun Zhou (zhouly@scuec.edu.cn) earned a Ph.D. degree in computer science and technology from Wuhan University in 2019. Her main research interests include system optimization and intelligent algorithms.

Mianxiong Dong [M[(mx.dong@csse.muroran-it.ac.jp) earned B.S., M.S. and Ph.D. degrees in computer science and engineering from the University of Aizu, Japan. He is the vice president and the youngest-ever professor at the Muroran Institute of Technology, Japan. He is the recipient of an IEEE TCSC Early Career Award (2016), an IEEE SCSTC Outstanding Young Researcher Award (2017), the 12th IEEE ComSoc Asia-Pacific Young Researcher Award (2017), the Funai Research Award (2018) and the NISTEP Researcher (2018)—making him one of only 11 people in Japan—in recognition of his significant contributions to science and technology by MEXT, Japan. He is also a Clarivate Analytics 2019 Highly Cited Researcher (Web of Science).

Deze Zeng [M] (deze@cug.edu.cn) is a full professor in China University of Geosciences, Wuhan, China. His current research interests mainly focus on edge computing, cloud computing, and cloud networking. He serves on the editorial boards of Elsevier JNCA, FCS, IEEE OJ-CS. He is a member of IEEE.

Jiangtao Luo [SM] (luojt@cqupt.edu.cn) earned a Ph.D. from the Chinese Academy of Science in 1998. His major research interests are network data mining, urban computing, and future Internet architecture. He has authored over 100 papers and holds 21 patents in these fields. He is a senior member of IEEE and a member of ACM.

Maode Ma [SM] (emdma@ntu.edu.sg), a Fellow of IET, earned his Ph.D. degree in computer science from Hong Kong University of Science and Technology in 1999. He has extensive research interests, including network security and wireless networking, and has authored over 400 international academic publications. He has served as conference chair for over 100 international conferences. He currently serves as a senior editor or associate editor for 5 international academic journals. He is a senior member of the IEEE Communication Society and the IEEE Education Society, and a Member of ACM. He is the Secretary of the IEEE Singapore Section and the Chair of the ACM, Singapore Chapter. He has been designated an IEEE Communication Society Distinguished Lecturer from 2013-2016.