Theil-Based Countermeasure against Interest Flooding Attacks for Named Data Networks

Rui Hou, Min Han, Jing Chen, Wenbin Hu, Xiaobin Tan, Jiangtao Luo, and Maode Ma

Abstract

NDN has been widely regarded as a promising representation and implementation of information-centric networking (ICN) and serves as a potential candidate for the future Internet architecture. However, the security of NDN is threatened by a significant safety hazard known as an IFA, which is an evolution of DoS and distributed DoS attacks on IP-based networks. The IFA attackers can create numerous malicious interest packets into a named data network to quickly exhaust the bandwidth of communication channels and cache capacity of NDN routers, thereby seriously affecting the routers' ability to receive and forward packets for normal users. Accurate detection of the IFAs is the most critical issue in the design of a countermeasure. To the best of our knowledge, the existing IFA countermeasures still have limitations in terms of detection accuracy, especially for rapidly volatile attacks. This article proposes a TC to detect the distributions of normal and malicious interest packets in the NDN routers to further identify the IFA. The trace back method is used to prevent further attempts. The simulation results show the efficiency of the TC for mitigating the IFAs and its advantages over other typical IFA countermeasures.

Introduction

With the explosive increase in Internet traffic and services, users are more concerned about data content as opposed to their locations. This trend could shape the future Internet architecture and change the mode of data sharing from address/host-centric into data content-centric. To meet the changes of user demands, several networking techniques, such as information-centric networking (ICN) [1] and software defined networking (SDN) [2], have been developed in recent years. Among these, an ICN paradigm, called named data networking (NDN) [3], was proposed to potentially replace the current Internet protocol (IP)-based Internet architecture. Compared with the current transmission control protocol (TCP)/IP architecture, the NDN is advantageous in terms of location independence, freedom from domain name servers (DNSs), better support for mobile devices, and improved security. Thereby, the NDN is considered as a potential architecture for the next-generation Internet.

However, the security issue remains a crucial concern in any type of network including the Internet. In the current IP-based Internet, denial of service (DoS) and distributed DoS are two malicious attacks, by which attackers can send numerous packets into the network to exhaust the network resources or to a specific node to interrupt its connectivity with other network terminals. Thus, such an attack can collapse the entire network and prevent other users from accessing it. Owing to its inherent character, the NDN is immune to disconnection attacks as it eliminates the concept of data-content address or location. However, it is vulnerable to an interest flooding attack (IFA) [4], which is a resource-related attack. In this attack, the attackers forge numerous interest packets with nonexistent data-content names, which are the malicious interest packets, to send to the NDN routers in an attempt to exhaust their cache memory of the pending interest table (PIT). Thus, it can prevent normal users from sending their own interest packets, and possibly cause a large amount of packet loss.

In this article, we first briefly review the current studies on the countermeasures for IFA, and then introduce the idea of Theil index, which is used to statistically measure economic phenomena [5], to detect IFA in NDN networks. Based on its theory, this article proposes a Theil-based countermeasure (TC) against an IFA in NDNs. The outstanding features of the proposed solution can be summarized as follows. Unlike conventional detection methods that rely on the PIT status to detect attacks, the TC can greatly reduce IFA misjudgment and protect the interest packets of normal users while avoiding excessive reactions to normal traffic fluctuations. The received interest packets will be differentiated and counted as intra-group and inter-group interest packets by an NDN router. In the TC, the distribution of the interest packets in a group and the distribution of the groups in the entire interest package are calculated. Then, at the time of an IFA, the TC detects the attack based on the change of intra-group heterogeneity and the unevenness of the inter-group to achieve higher fault tolerance and lower false positives. Combined with the method of interest backtracking [6], the TC can effectively mitigate the IFA.

The remainder of the article is organized as follows. The following section presents a survey on

Rui Hou, Min Han, and Jing Chen are with South-Central University for Nationalities; Wenbin Hu is with Wuhan University; Xiaobin Tan is with the University of Science and Technology of China; Jiangtao Luo is with Chongqing University of Posts and Telecommunications; Maode Ma is with Nanyang Technological University.

Digital Object Identifier:
10.1109/MNET.2019.1800350

existing solutions. Then the proposed solution is described in detail, and the simulation results are discussed. The final section concludes the article.

Review of Related Works

In NDNs, each data is assigned a globally unique name with a hierarchical structure separated by "/," for example, /google/icn/ndn. To obtain the content, a subscriber, who is a data-content requester, creates an interest packet containing the name of the desired data and sends it to the NDN transport layer to find a potential target data content. The publisher, who is a data-content holder, could send back the required data in the form of data packets through reverse routing of the interest packet. All the packets are forwarded according to the hop-by-hop model in the NDN content routers (CRs). Each CR has three data structures: content stores (CS), PIT, and forwarding information base (FIB). The CS caches the data obtained from publishers. The PIT includes a set of interfaces to handle the interest packets that are waiting to receive data packets. If a data packet is received, the corresponding interest packet will be consumed. Finally, the FIB contains the NDN route entries and maps incoming interest packets to suitable interfaces for searching the target publisher.

Given that NDN relies on data-content names for information search and transport, the interest flooding attackers can forge numerous malicious interest packets (e.g., interest packets with nonexistent data-content names) and inject them into the named data network. As illustrated in Fig. 1, a normal user (S_A) creates and sends an interest packet into the named data network with the data-content name of /google/movie/Transformers to seek a movie named *Transformers*. However, two attackers (S_A and S_B) simultaneously forge a number of malicious interest packets with nonexistent names of google/movie/random strings (a, b, 1, 2, ♯, percent), in which the suffix "random strings" implies randomly created strings with random combinations of letters (a, b), numbers (1, 2), or symbols (♯, percent). As there is no corresponding data content to satisfy malicious interest packets, the malicious interest packets occupy the PIT of NDN routers CR1 and CR2 in Fig. 1 for a long time. Thus, they eventually exhaust the cache memory and network bandwidth, and prevent normal users from accessing the network to reacquire the data packets. If this situation persists for a long time, the entire named data network could eventually collapse. Therefore, owing to the significant threat posed by the IFA, its detection and mitigation have become significantly important to researchers in the ICN/NDN community.

In recent years, many IFA detection and mitigation schemes have been proposed. Dai *et al.* [6] proposed an interest-packet trace-back approach to mitigate the IFA. When the increment rate of the PIT entries exceeds a threshold, the publisher creates corresponding data packets to trace the source of the interest packets to identify the attacker. However, as this approach only relies on the increment rate of the PIT entries, it has a high misjudgment rate. Compagno *et al.* [7] proposed an IFA-detection-and-mitigation scheme named Poseidon, which can detect the interfaces of the CRs in the NDN in real-time, analyze the interest and data traffic, and combine the capacity occupancy rate of the PIT to identify the IFAs. However, it may restrict requests from normal users. Afanasyev *et al.* [8] proposed three IFA-mitigation countermeasures, with the main concept being the calculation of the ratio of the number of the received data packets to that of interest packets sent for each interface of the NDN CRs. This ratio is called the interest satisfied rate, which is compared with a preset attack threshold to determine whether the NDN CRs have suffered an IFA. Following the rule of NDN, requiring load balance between interest traffic and data traffic, Gasti *et al.* [9] proposed the restriction of excessive interest packets in the interface of the NDN CRs to mitigate the IFAs. Wang *et al.* [10] proposed an IFA-mitigation scheme, named disabling PIT exhaustion (DPE), by which a CR in the NDN counts the number of expired interest packets. If the number of interest packets with a specific name exceeds the preset threshold, the excess packets will be removed from the PIT to mitigate the IFAs. However, the DPE approach relies on the number of expired interest packets in the PIT and is thus difficult to implement. Al-Sheikh *et al.* [11] presented two IFA-mitigation schemes called the prefix and satisfaction-based pushback schemes. Similar to the solution in [9], the prefix pushback scheme requires the use of load balance between interest and data packets in CRs to mitigate the IFAs. Although similar to the solution in [10], the satisfaction-based pushback scheme uses the number of expired interest packets to identify and restrict the malicious interest packets. However, these two IFA countermeasures excessively rely on the status of the PIT and may thus result in many misjudgments.

The above-mentioned IFA countermeasures rely on the abnormal status of the PIT to identify IFAs and may misjudge traffic fluctuations caused by normal users. To increase the accuracy of the attack detection, Xin *et al.* [12] proposed a cumulative- and relative-entropy-based IFA-detection-and-mitigation scheme. By counting the distribution of names in the interest packets

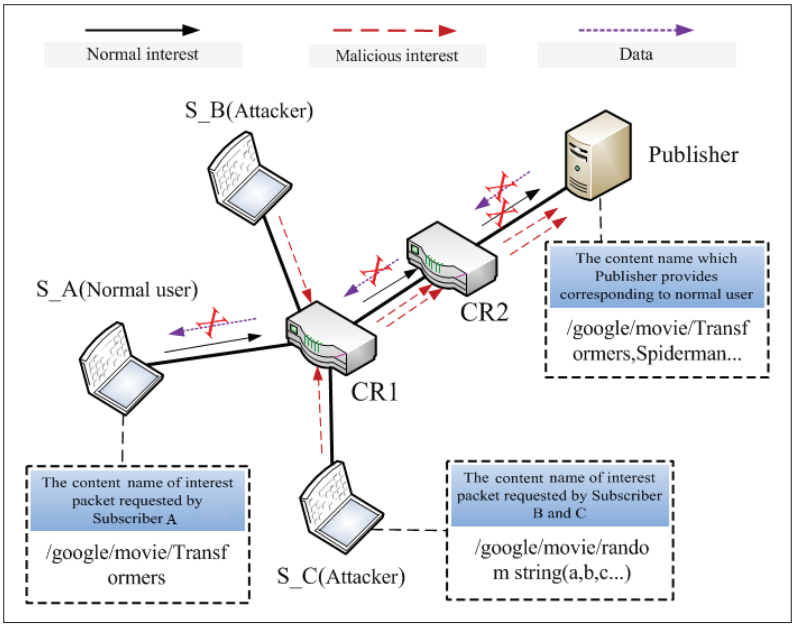

FIGURE 1. Illustration of the IFAs.

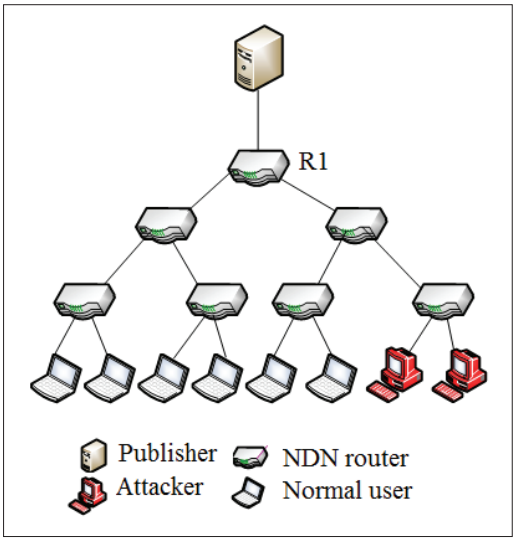

FIGURE 2. Simulation network topology.

and calculating their information-entropy value, attacks can be identified. As this scheme does not rely on the PIT status, it can yield high fault tolerance and low misjudgment rates. However, it excessively relies on the name distribution of the interest packets received from CRs. Thus, it cannot accurately identify complex attacks [13]. Comparatively, Zhi *et al.* [14] presented a Gini-based IFA-detection scheme with relatively better performance in identifying attacks. However, similar to the information entropy-based scheme, the Gini coefficient relies on the proportion of the interest packets with a specific name to all the interest packets. Thus, the CRs become too sensitive to the distribution of the names of the interest packets, this could easily result in misjudgments.

To overcome the aforementioned limitations of the existing IFA-detection-and-mitigation schemes, we proposed the TC in this article. The TC does not rely only on the PIT status to identify attacks to avoid overreaction toward the abnormal traffic fluctuation. As it divides the interest packets into different groups and identifies attacks based on the distribution of the names of the interest packets into inter-groups and intra-groups, the TC can yield a higher fault toleration and lower misjudgment rate compared to previously proposed schemes. With the combination of the track-back approach, TC can efficiently mitigate the IFAs.

The Proposed Theil-Based IFA Countermeasure

IFA Detection

In NDNs, each CR records the name of each interest packet that it received. The CRs can use the statistical distribution of the names of the interest packets to detect the IFA. When an attacker launches an IFA, the occurrence frequency of the forged names in the malicious interest packets will increase significantly. As the Theil entropy value calculated using the names of the interest packets at the CRs decreases abnormally, the change in the value of the Theil entropy can be used to determine the situation of networks. Furthermore, the Theil entropy can divide the interest packets into groups based on a preset rule to evaluate the contribution of intra-group and inter-group differences.

Type	Value
Simulation time duration	300 s
Statistical time duration	1 s
Attack detection time duration	50 ms
Packet transmission time of each hop	10 ms
Interest packet sending rate by normal users	200 packets/s
PIT cache capacity	50 entries
PIT entries' life time	1 s

TABLE 1. Simulation parameters

Given a specific time, suppose a CR has received n interest packets, and they are divided into k groups, denoted as g_k. Then, the intra-group and inter-group degree of unevenness of the name distributions can be defined. The intra-group degree of unevenness of the name distribution denotes the proportion of the interest packets as y_i to all the interest packets within a group. In contrast, the inter-group degree of unevenness of the name distribution denotes the proportion of the number of interest packets in group y_k to the entire number of interest packets when there is no attack in the NDN. Given that users' requests follow the generally stable Zipf distribution [15], the statistical value of the Theil's entropy of the names will remain within a reasonable range. Simultaneously, when attackers send numerous malicious interest packets into the network, the malicious names will affect the distribution names of interest packets. Thus, the statistical value of the Theil's entropy of the names will go beyond the normal range, resulting in the detection of IFAs. The CRs record the distributions of each interest packet to identify the interest packets resulting in the maximum changes in the unevenness degree of the name distributions in the inter-groups and intra-groups and accordingly judge them as malicious interest packets. Given an interest packet's sample D, we can define the Theil entropy T(D) as follows:

$$T(D) = T_b + T_w = -\left(\sum_{k=1}^{K} \frac{y_k}{\mathrm{n}} \log \frac{y_k}{\mathrm{n}} + \sum_{k=1}^{K} \left(\sum_{i \in g_k} \frac{y_i}{y_k} \log \frac{y_i}{y_k} \right) \right)$$

where T_b and T_w denote the inter-group and intra-group unevenness degree of the name distributions, respectively. TC's computation complexity can be evaluated as follows. First, the number of operations for T_b and T_w are determined as k, where k is the required number of additions when calculating from 1 to K, and $y_k + k$, respectively. Thus, the total number of operations is m, which equals to $2k + y_k$. It can be seen that m is a constant to make the computation complexity to be O(C).

Mitigation Measures

When an IFA is detected, a trace-back approach on malicious interest packets can be applied to localize the attacker's position, indicating that the CR that has been attacked and a forged data packet can be created to satisfy the malicious interest packets. Moreover, by using the resource records

of the interest packets of the PIT, the malicious packet can be traced back to the attacker. Subsequent to identifying the attacker, the attacked CR can block its interface to prevent the connection to the attacker with the aim to mitigate the IFA.

Simulation and Discussion

To verify the accuracy and effectiveness of the proposed TC, simulation experiments were conducted on the ndnSIM [16] platform. A binary-tree structure was used as the NDN topology in the simulation, with one content publisher, seven NDN CRs, and eight users, including six normal users and two attackers, as shown in Fig. 2. The simulation parameters are listed in Table 1 with the simulation duration set at 300 s. Normal users send interest packets at a constant rate at the beginning of the simulation, and the IFA initiates at 200 s.

First, we introduced abnormal traffic fluctuations from both normal users and IFA to verify the low false-positive rate or low misjudgment rate and the high accuracy of attack detection by the TC. Then, we compared the performance of the TC with that of other typical IFA countermeasures with respect to two aspects including the number of data packets received by normal users and the occupancy rate of the PIT at CRs.

Accuracy of the TC

When abnormal traffic fluctuations occur due to normal users, the router that is closest to the content publisher, such as R1 in Fig. 2, will experience a PIT overflow, which may result in R1 not being able to receive subsequent interest packets, and the upstream CRs and content publisher will be unable to receive interest packets sent by the downstream CRs. This may cause PIT overflow of the downstream CRs and may thus be misjudged as IFAs by the existing IFA countermeasures.

Figure 3 shows the comparisons among the IFA-detection accuracy of the proposed TC and other typical IFA countermeasures. As shown,

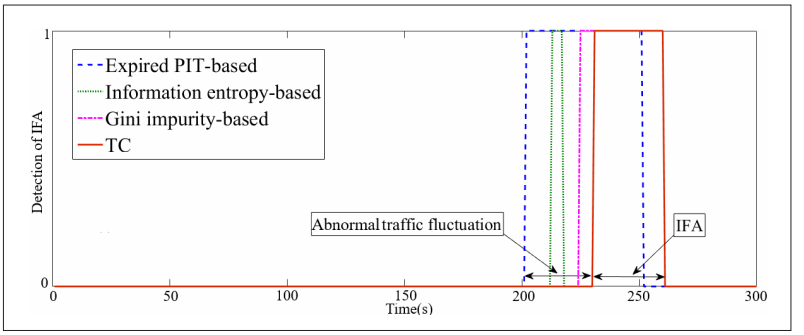

FIGURE 3. Detection of the IFAs.

between 200 s and 230 s, that is, during the abnormal traffic fluctuation, the conventional expired-PIT-based method misjudges the fluctuation as an IFA with its detection result as "1," where value "1" denotes a detected IFA and value "0" denotes no detection of IFA. Similarly, although the information entropy-based method and Gini impurity-based method did not misjudge an IFA at the beginning of the traffic fluctuation, they eventually made a misjudgment. The proposed TC shows "0" during the entire traffic fluctuation period, thus showing an extremely low misjudgment rate. In addition, as shown, from 230 s to 260 s, a real IFA occurs in the named data network, and the TC rapidly detects the IFA in the entire attack period, thus proving its high accuracy. This result shows the advantage of TC over the previous countermeasures in distinguishing between abnormal traffic fluctuation due to normal users and a real IFA.

Efficiency of TC

In general, normal users request existing data content with a Zipf distribution [15], while attackers request nonexistent data with a uniform distribution, and each request differs in most cases. Under different attacking speeds, we compared the IFA mitigation under no-measurement and other typical measurement conditions.

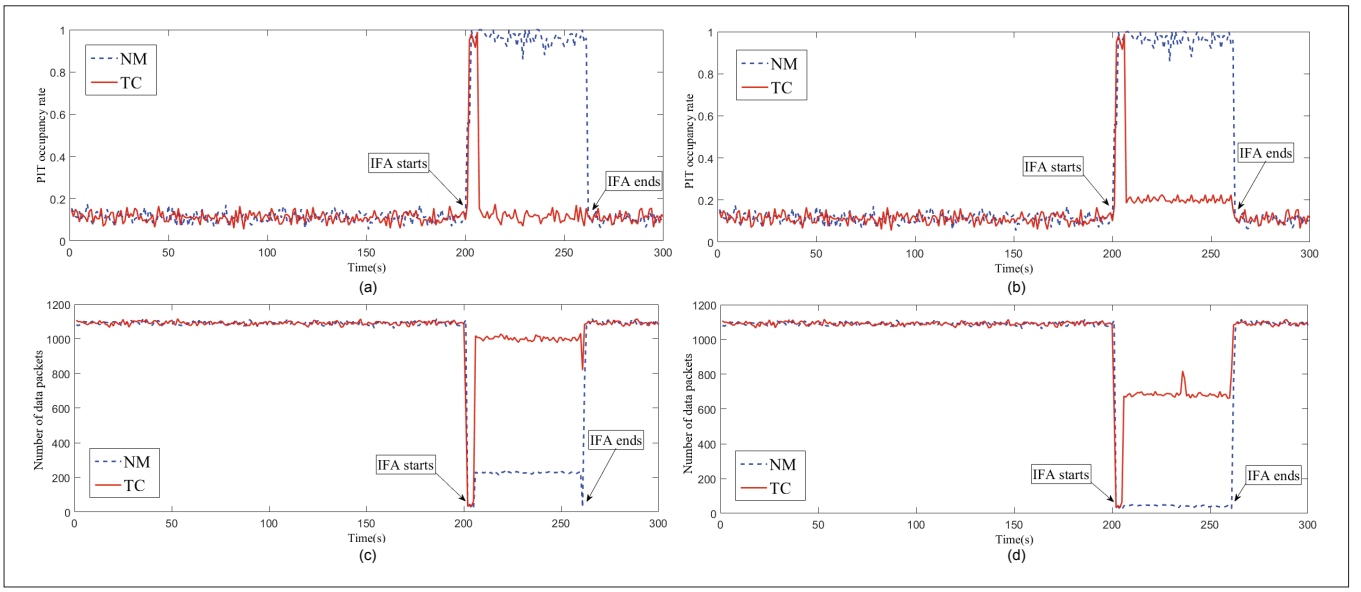

FIGURE 4. Efficiency of attack mitigation at different attack rates: a) PIT occupancy rate of router R1 when the attacker sends 1000 interest packets per second; b) PIT occupancy rate of router R1 when the attacker sends 2000 interest packets per second; c) number of data packets received by normal users when the attacker sends 1000 interest packets per second; d) number of data packets received by normal users when the attacker sends 2000 interest packets per second.

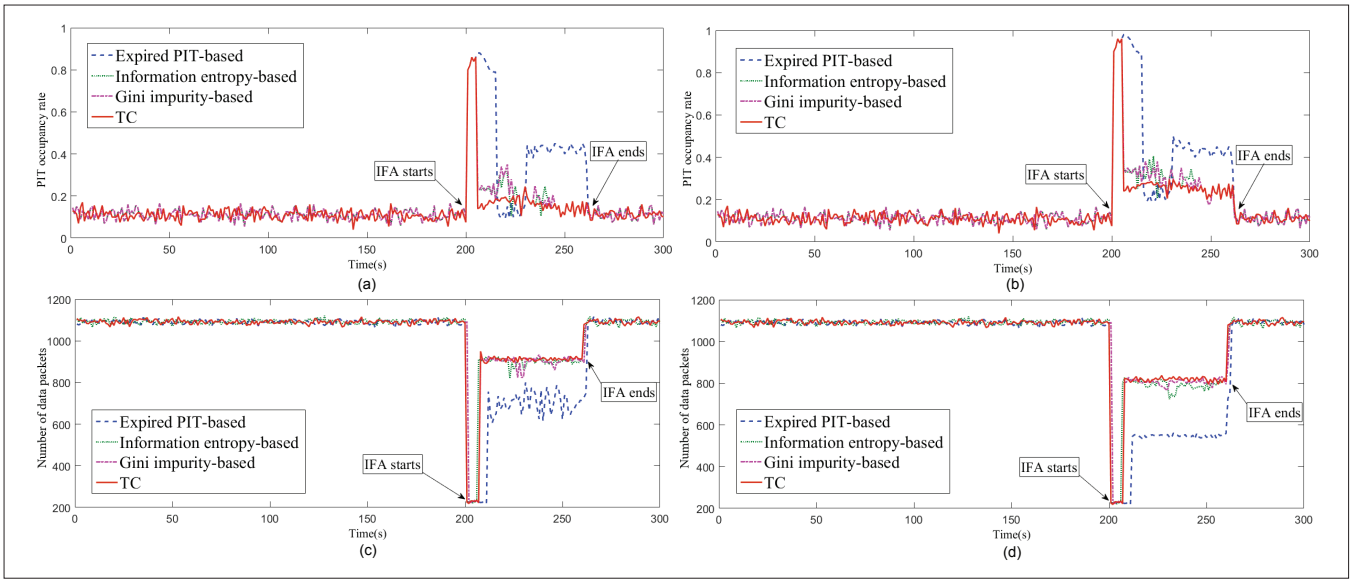

FIGURE 5. Comparison on efficiency of attack mitigation at various attack rates by different approaches: a) PIT occupancy rate of router R1 when the attacker sends 1000 interest packets per second; b) PIT occupancy rate of router R1 when the attacker sends 2000 interest packets per second; c) number of data packets received by normal users when the attacker sends 1000 interest packets per second; d) number of data packets received by normal users when the attacker sends 2000 interest packets per second.

Figure 4 shows the IFA mitigation effect between TC and no-measurement conditions for different attack rates at CR1. Figures 4a and 4b show the PIT occupancy rate of CR1. As shown, when the IFA initiates at 200 s, the PIT occupancy rate of CR1 instantly reaches 100 percent. Furthermore, during the 60-s attacking period, the occupancy rate is maintained at 90 percent to 100 percent. Thus, it results in normal users being unable to receive their data. In the TC, although the PIT occupancy rate also instantly reaches 100 percent when the IFA initiates, it reduces to 10 percent to 20 percent after several seconds, and maintains the same level during the remainder of the attack. When the attack rate is doubled, as shown in Fig. 4b, the TC maintains the PIT occupancy rate of CR1 at approximately 20 percent during the entire attack period, indicating that the TC can effectively mitigate the IFA at different attack rates. Furthermore, Figs. 4c and 4d show the received number of data packets by normal users. At the beginning, the number of data packets received by all the normal users is approximately 1100, which is roughly 91.7 percent. When the IFA is initiated, the number of successfully received data sharply declines. Under the no-measurement condition, the number of data packets received by the normal users reduces at a rate of approximately 80 percent with different attack rates. When the TC was applied, the number of data packets received by normal users reduces to less than 100 with an attack rate of 1000 packets/s. However, after a short period, the number of data packets received by normal users recovers and maintains the received rate at 80 percent to 90 percent of the level before the attack. Even when the attack rate is doubled, the TC can still maintain the received rate at over 50 percent, indicating that the TC can benefit the normal users under the IFA condition.

Figure 5 shows the comparison of CR1 occupancy rates among four typical IFA countermeasures, namely, the expired PIT, information entropy, Gini impurity, and TC. As shown in Figs. 5a and 5b, when an IFA is initiated, the PIT occupancy rate at CR1 instantly reaches its peak after the attack is detected. The four IFA countermeasures are all able to mitigate the attack and reduce the PIT occupancy rate to a stable level. Compared with the other three IFA countermeasures, the expired PIT-based scheme takes the longest time to recover the occupancy to a stable level, given that it requires a certain long period to count the entries of the expired PIT to determine whether the CR has suffered an attack. In contrast, the information entropy-based and Gini-based schemes can obtain relatively ideal results. However, the PIT occupancy rate exceeds 30 percent under the attack rate of 1000 packets/s, and approximates 40 percent under the attack rate of 2000 packets/s in some cases. In contrast to these schemes, during the entire attack period, the proposed TC can maintain the PIT occupancy rate at CR1 between 10 percent and 20 percent under the attack rate of 1000 packets/s, and between 20 percent and 30 percent under attack rate of 2000 packets/s. Additionally, Figs. 5c and 5d show the number of received data packets by normal users under different attack rates. It is obvious that when the IFA is initiated, the number of successfully received data packets by normal users sharply declines. The expired PIT-based scheme can only recover approximately 60 percent and 50 percent data packets by normal users under the attack rates of 1000 and 2000 packets/s, respectively, which is relative to the original value. The remaining three schemes can all recover approximately 80 percent and 90 percent under each of the two attack rates. However, Figs. 5c and 5d show that although the information entropy-based and Gini-based schemes can yield the same results as that of the TC, the TC is more stable during the entire attack period.

Therefore, from Figs. 4 and 5, it can be concluded that the proposed TC is more stable and more effective in blocking attackers' actions, and can thus efficiently mitigate the effects of the IFA for users.

Conclusion and Future Research Directions

IFAs can cause significant impairments to named data networks by preventing normal users from accessing the network and fetching their data. This article proposed the TC, which divides the interest packets into groups and uses the distribution of their intra-group and inter-group names to detect the attacks. The simulation results showed that the TC can not only rapidly detect the IFA but also identify abnormal traffic fluctuations from normal users, and thus reduce the misjudgments to improve attack-identification accuracy. Compared with several typical IFA countermeasures, the TC can effectively reduce the PIT occupy rate and increase the number of data packets received by normal users under the IFAs. This proves that the TC has a much better IFA-detection-and-mitigation performance.

As future work, two aspects can be further investigated:

- A large scale of NDN in a more complex topology, such as the networks in a mesh topology with hundreds of nodes, will be evaluated by various simulation experiments.
- The impacts of complex attacks to the NDN with the countermeasure of the Theil entropy index will be studied. By the complex attacks, the roles of attackers will change between normal user and attacker from time to time.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants 60841001 and 61673360; the Scientific and Technological Projects of Wuhan, China, under Grants 2013010501010125 and 2015010101010008; the Ministry of Education-China Mobile Research Fund Project, under Grant MCM20170203; the Chongqing Municipal Project, under Grant cstc2015jcyjBX0009; and the Special Fund for Basic Scientific Research of Central Colleges, under Grant CZT19011. The authors also would like to thank all the anonymous reviewers for their valuable comments.

References

[1] G. Xylomenos *et al.*, "A Survey of Information-Centric Networking Research," *IEEE Commun. Surv. Tut.*, vol. 16, no. 2, Second Quarter 2014, pp. 1024–49.
[2] S. Fu *et al.*, "Software Defined Wireline-Wireless Cross-Networks: Framework, Challenges, and Prospects," *IEEE Commun. Mag.*, vol. 56, no. 8, Aug. 2018, pp. 145–51.
[3] L. Zhang *et al.*, "Named Data Networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, July 2014, pp. 66–73.
[4] J. Tang *et al.*, "Identifying Interest Flooding in Named Data Networking," *Proc. IEEE Int'l. Conf. Green Computing and Commun. (GreenCom), IEEE Internet of Things (iThings/CPSCom) and IEEE Cyber, Physical and Social Computing*, Beijing, China, 2013, pp. 306–10.
[5] https://en.wikipedia.org/wiki/Theil_index.
[6] H. Dai *et al.*, "Mitigate DDoS Attacks in NDN by Interest Traceback," *IEEE Conf. Computer Commun. Workshops (INFOCOM WKSHPS)*, Turin, Italy , 2013, pp. 381–86.
[7] A. Compagno *et al.*, "Poseidon: Mitigating Interest Flooding DDoS attacks in Named Data Networking," *Proc. IEEE 38th Conf. Local Computer Networks (LCN)*, Cambridge, MA, USA, 2013, pp. 630–38.
[8] A. Afanasyev *et al.*, "Interest Flooding Attack and Countermeasures in Named Data Networking," *IFIP Networking Conf.*, Brooklyn, NY, USA, 2013, pp. 1–9.
[9] 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.
[10] K. Wang *et al.*, "Decoupling Malicious Interests from Pending Interest Table to Mitigate Interest Flooding Attacks," *IEEE GLOBECOM*, Atlanta, GA, USA, 2013, pp. 963–68.
[11] S. Al-Sheikh *et al.*, "Revisiting Countermeasures against NDN Interest Flooding," *Proc. 2nd Int'l. ACM Conf. Information-Centric Networking*, San Francisco, CA, USA, 2015, pp. 195–96.
[12] Y. Xin *et al.*, "A Novel Interest Flooding Attacks Detection and Countermeasure Scheme in NDN," *IEEE GLOBECOM*, Washington, USA, Dec. 2016, pp. 1–7.
[13] D. Wang *et al.*, "Towards Robust and Effective Trust Management for Security: A Survey," *Proc. IEEE 13th Int'l. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom)*, Sept. 2014, pp. 511–18.
[14] T. Zhi, H. Luo, and Y. Liu, "A Gini Impurity Based Interest Flooding Attack Defence Mechanism in NDN," *IEEE Commun. Lett.*, Mar. 2018, pp. 531–38.
[15] V. Maslov, "The Zipf-Mandelbrot Law: Quantization and an Application to the Stock Market," *Russ. J. Math. Phys.*, vol. 12, no. 4, 2005, p. 483.
[16] A. Afanasyev *et al.*, "ndnSIM: NDN Simulator for ns-3," University of California, Los Angeles, Tech. Rep, 2012.

Biographies

Rui Hou [M'09] (hourui@mail.scuec.edu.cn) received the Ph.D. degree from Huazhong University of Science and Technology, China, in 2006. He is currently a professor at the College of Computer Science, South-Central University for Nationalities. He was sponsored by the Chinese Scholarship Council as a National Senior Visiting Scholar, and conducted research in the Lab. Signaling, Communications, and Networking, in the Dept. of ECE, Colorado State University, Fort Collins, CO, USA, from 2014 to 2015. He has authored or co-authored over 100 papers in international publications. His main research interests include computer network architecture, optical switching, and wireless sensor networks. He is a member of CCF and IEICE.

Min Han (hanmin_stu@163.com) is currently working toward an M.Eng. at the College of Computer Science, South-Central University for Nationalities, Wuhan, China. Her area of research is information security in information-centric networking.

Jing Chen (chenjing_stu@163.com) is currently working toward an M.Eng. at the College of Computer Science, South-Central University for Nationalities, Wuhan, China. Her area of research is information privacy and security in information-centric networking.

Wenbin Hu (hwb@whu.edu.cn) is currently a professor with the School of Computer, Wuhan University, Wuhan, China. His main research interests are intelligent simulation and network optimization. He has authored or co-authored over 90 international academic publications. He serves as the guest editor for several international academic journals, and he is a member of CCF.

Xiaobin Tan [M'12] (xbtan@ustc.edu.cn) received the Ph.D. degree from the Dept. of Automation, University of Science & Technology of China, in 2003. He is currently an associate professor with the Laboratory for Future Networks, University of Science and Technology of China. He has authored or co-authored over 40 international academic publications. His main research interests are future Internet architecture optimization and information security.

Jiangtao Luo [SM'15] (luojt@cqupt.edu.cn) received the Ph.D. degree from the Chinese Academy of Science in 1998. He is currently a professor with the Electronic Information and Networking Research Institute, Chongqing University of Posts and Telecommunications. 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 also an ACM member. He was a recipient of the Chinese State Award for Scientific and Technological Progress in 2011, the Chongqing Provincial Award for Scientific and Technological Progress in 2007 and 2010, and the Chongqing Science and Technology Award for Youth in 2010.

Maode Ma [SM'09] (emdma@ntu.edu.sg) received the Ph.D. degree in computer science from The Hong Kong University of Science and Technology in 1999. He is currently an associate professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He has extensive research interests including network security and wireless networking. He has authored or co-authored over 300 international academic publications. He currently serves as the Editor-in-Chief of the *International Journal of Computer and Communication Engineering* and the *International Journal of Electronic Transport*, and a senior editor or an associate editor for five other international academic journals. He is also a fellow of IET, a member of ACM, and the Chair of the IEEE Education Society. He is also serving as a Distinguished Lecturer for the IEEE Communication Society.