ChoKIFA: A New Detection and Mitigation Approach Against Interest Flooding Attacks in NDN

Abdelmadjid Benarfa, Muhammad Hassan, Alberto Compagno, Eleonora Losiouk, Mohamed Bachir Yagoubi, Mauro Conti

ChoKIFA: A New Detection and Mitigation Approach against Interest Flooding Attacks in NDN

Abdelmadjid Benarfa[1], Muhammad Hassan[2], Alberto Compagno[3], Eleonora Losiouk[2], Mohamed bachir Yagoubi[1], and Mauro Conti[2]

[1] University of Laghouat, Algeria. {a.benarfa, m.yagoubi}@lagh-univ.dz
[2] University of Padova, Italy. {conti, hassan, elosiouk}@math.unipd.it
[3] Cisco Systems, France. {acompagn}@cisco.com

Abstract. Named-Data Networking (NDN) is a potential Future Internet Architectures which introduces a shift from the existing host-centric IP-based Internet infrastructure towards a content-oriented one. Its design, however, can be misused to introduce a new type of DoS attack, better known as Interest Flooding Attack (IFA). In IFA, an adversary issues non-satisfiable requests in the network to saturate the Pending Interest Table(s) (PIT) of NDN routers and prevent them from properly handling the legitimate traffic. Prior solutions to mitigate this problem are not highly effective, damages the legitimate traffic, and incurs high communication overhead.

In this paper, we propose a novel mechanism for IFA detection and mitigation, aimed at reducing the memory consumption of the PIT by effectively reducing the malicious traffic that passes through each NDN router. In particular, our protocol exploits an effective management strategy on the PIT which differentially penalizes the malicious traffic by dropping both the inbound and already stored malicious traffic from the PIT. We implemented our proposed protocol on the open-source ndnSIM simulator and compared its effectiveness with the one achieved by the existing state-of-the-art. The results show that our proposed protocol effectively reduces the IFA damages, especially on the legitimate traffic, with improvements that go from 5% till 40% with respect to the existing state-of-the-art.

Keywords: NDN · DDoS attack · IFA · PIT management · Congestion

1 Introduction

Numerous solutions have been proposed to narrow the gap between the Internet design and its current usage. One such potential Future Internet Architecture (FIA), sponsored by NSF, is Name Data Networking (NDN) [14]. NDN explicitly addresses the data (content) itself instead of its physical location (i.e., host) in the network, therefore, transforming data into the "first-class" entity. In NDN, consumer directly requests the name of the *content* by issuing an *interest*. The network then handles the request by efficiently finding and retrieving back the

closest copy of the relevant content. This decoupling of time and space among request resolution and content transfer enables NDN to provide storage, mobility and security as native features belonging to the network architecture [14].

One of the key goals of NDN is "security by design", this paper addresses the most significant NDN-tailored DDoS attack: the *Interest Flooding Attack* (IFA) [6]. In IFA, adversary aims at flooding the network and blocking the network services received by legitimate users via abusing two fundamental NDN features [9], i.e., (i) forwarding grounded on the longest name-prefix match, and (ii) maintaining the record of outstanding forwarded interests in so-called *Pending Interest Table (PIT)* for efficient multicasting. In particular, the adversary issues unique requests for unsatisfiable content name targeting the name-space(s). As a consequence, one PIT entry is created for each request in each on-path NDN router. These entries stays in the PITs till they expire at the end. Succeeding to overload some or all PITs which leads to legitimate interest packets being dropped [6]. Regardless of the substantial quantity of research on NDN security, we identified that the proposed defence mechanisms for IFA [1,3,4,6,9] have one or more of the following limitations. First, the legitimate traffic is likely to be damaged, since most of the proposed countermeasures [1,3,12] limits the rate of incoming traffic and are not able to differentiate between legitimate and malicious packets, thus resulting in unfair punishments. Second, since each router has to perform first an attack detection and then attack mitigation, during the first phase (i.e., inaccurate), most of the approaches are likely to encounter harmful consequences. Finally, the proposed collaborative mechanisms [1, 3, 4, 9] introduces unnecessary overhead given by the extra messages exchanged among routers.

We propose an efficient mechanism, named as Choose To Kill IFA (ChoKIFA), which mitigates the damages caused by IFA by differentiating the malicious traffic from the legitimate one, and by reducing the former, without any collaborative communication or global network monitoring. In order to do so, ChoKIFA exploits the Active Queue Management (AQM) scheme, i.e., CHOose and Keep for responsive flows, CHOose and Kill for unresponsive flows (CHOKe) [8], and without any delay penalizes the malicious traffic by dropping both the new incoming malicious interests and removing the ones already stored in the PIT. Thus, routers are able to independently detect and mitigate the attack in progress as-soon and as-close to the adversary as possible, while maintaining the simplicity of forwarding. We evaluate the effectiveness of ChoKIFA through extensive simulations on ndnSIM simulator [2], and by comparing it with the state-of-the-art mitigation approaches [1]. The results show that ChoKIFA effectively mitigates the adverse effects of IFA in the network. In particular, ChoKIFA is able to guarantee legitimate interest satisfaction rate up to 97% and it shows up to 40% less false positives in comparison with rate limiting mitigation approaches.

Organization: We present the overview of IFA in Section 2. Section 3 illustrates the existing mitigation approaches against IFA. Section 4 briefly describes the proposed protocol including system, adversary model and working methodology

of ChoKIFA. Section 5 present the implementation, evaluation and comparison of ChoKIFA against IFA and state of the art. Finally, Section 6 concludes the paper.

2 Interest Flooding Attacks in NDN

In NDN, routers maintain per-packet state for each interest packet in PIT. Therefore, the immense amount of malicious interests can result in exhaustion of routers memory and resources, and prevent them from creating PIT entries for new incoming traffic, resulting in the disrupt of benign users services. In particular, IFAs are categorized on three types based on the type of content requested by the adversary [6]: (i) existing or static content, where adversary generates a large number of interests for an existing content that propagates through all intervening routers caches. In result, legitimate interests for the same content are not able to reach the producer(s) since they are being satisfied by the cached copies. This type of attack is quite restricted since in-network content *caching* provides a built-in countermeasure. (ii) Dynamically generated content, where adversary issues dynamic requests for existing content, therefore, all interests are propagated towards the producer(s), resulting in bandwidth consumption and PIT exhaustion. Correspondingly, targeted producer wastes considerable computational resources due to signing the content (i.e., per-packet operation). Lastly, (iii) non-existent content, where adversary requests for unique non-existent (unsatisfiable) content. These interests cannot be collapsed by routers, and are routed towards the producer(s). Such interest packets consume memory in router's PIT until they expire due to "interest life-time". Thus, a massive number of non-existent interest packets in the PIT table leads to benign interest packets being dropped in the network [1, 3, 6].

We focus on the IFA where adversary generates unsatisfiable interests. Using a valid name $prefix$, there are many ways to generate these unsatisfiable interests, e.g., (i) by enabling the name of the interest to */prefix/nonce*, where the suffix *nonce* is a random value. Such interests are propagated throughout towards the producer and are never satisfied. (ii) By swapping the `Publisher Public Key Digest` [6] field to a random value. Subsequently, no public key would match this value, therefore, will never be satisfied. (iii) Lastly, by setting the `Interest Exclude filter` to exclude all existing content starting with $/prefix$. In consequence, the interest can never be satisfied as it concurrently requests and excludes the same content.

3 Related works

Several defense mechanisms against IFA are proposed which implements detection and reaction approach, similarly, in an independent or collaborative manner (unlike securing routing protocols in IP [10]). In independent systems, the detection of attack is largely based on network traffic analysis and(or) PIT usage, while the subsequent reaction mechanisms reduce the incoming/outgoing traffic, independently on each router. For instance, Afanasayev et al. [1] proposed four

different methods to deal with IFA. The first method introduces a "simple limit" on the interfaces based on the physical capacity of the links, resulting in under-utilization of the network. The second method which is an alteration of "token fairness" algorithm, regulates the number of outgoing interests by limiting the assigned tokens to a specific outgoing interface. The drawback of this method is that it does not discriminate between benign and malicious traffic while assigning the tokens, and relatively admits a large number of malicious interests. The third method is based on the per-interface ratio between interests and their corresponding data packets for attack detection, namely "satisfaction-based". The work in [3,4,6] also adopts similar phenomena, where the mitigation is performed by reducing (or blocking) the requesting rate of detected nodes. The drawback of this method is that each router decides to forward/discard interest(s) using its local estimation of interest satisfaction ratio. Thus, the probability of benign interests being forwarded declines as the number of hops between the consumer and the producer increases [1]. The last method is a collaborative approach called as "satisfaction-based pushback. In this case, [1, 3, 4], each router sets an explicit limit value for each incoming interface, and announce this value to all downstream routers. This method has shown to be more effective than previous, but the legitimate stream is still influenced, especially when the path is long. Moreover, it creates unnecessary signalling overhead in the network.

In particular, all the countermeasures aims to limit the number of overall incoming interests (i.e., including benign and malicious), either at each interface [3], [1] or router [4]. Therefore, results in performance degradation of legitimate users and requires further enhancements in terms of traffic differentiation between benign and malicious traffic.

4 Mitigation of IFA exploiting AQM

In this paper, we take a footstep in the direction of identifying and differentiating malicious packets from the benign traffic during IFA. By exploiting the phenomena of AQM [8], we design an algorithm, i.e., CHOose to Kill malicious Interest, CHOose to keep genuine Interest for IFA (ChoKIFA) which aims to provide fairness among the benign interest packets that pass through the router. In particular, ChoKIFA utilizes the PIT state which forms adequate statistics regarding the incoming and outgoing interest packets and use it to identify and drop malicious interest packets.

4.1 System and Adversary Model

In our system model, we consider the topology illustrated in Figure 1, as used by various authors [1, 4]. Multiple benign consumers (C) issues Benign Interests (BIs) for existing content towards a producer (P) which is publishing the content under specific name prefix ($prefix$). BIs and the corresponding content packets traverse multiple routers (R) before being satisfied by P. Each router $r_i^j \ \epsilon \ |R|$ has the default settings of NDN [13], where j is the interface of i-th router.

We assume that adversary (Adv) generates massive amount Malicious Interests (MIs) which have bogus names to request non-existing content (i.e., type

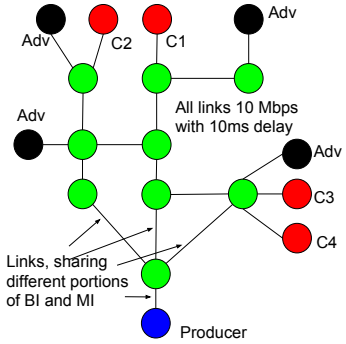

Fig. 1. Topology considered.

three, see Section 2). The aim of Adv is to saturate R's PIT, in particular, by rapid generation of large numbers of MIs [1,3]. Once the PIT is completely full, incoming BIs are being dropped. Apart from that, this has more than a few consequences. First, the sending rate of MIs is not dependent on the allocated bandwidth [6]. Secondly, MIs cannot be replied back by the $R's$ caches. Lastly, if created sophisticatedly (i.e., with a random component at the end of each name-prefix such as $prefix/Rnd$) MIs are never collapsed until the interests decay. All these effects allows Adv to efficiently fill up $R's$ PIT, which makes the attack more damaging than type one and type two IFA. In addition, without the loss of generality, we assume that Adv is capable to corrupt set of C (i.e., botnet), through which it triggers the attack [1,3]. Lastly, the percentage of bots is taken 50% with the ratio of C in the whole network [1].

4.2 ChoKIFA: CHOose to Kill Interest Flooding Attack

In this section, we present the details our proposed mitigation mechanism for IFA. In order to be effective in defending against IFA, ChoKIFA exploits traffic flow as an attribute to differentiate and penalize the MIs from BIs. Unlike IP, where traffic flow measurement relates to the accountable attributes such as source/destination address, interface number, packets/bytes counts forwarded (source to destination), backward (destination to source) counts and so on. In NDN, following content oriented communication model, traffic flow is centered around series of packets that corresponds to specific piece of data [7]. Considering this, we design the three novel attributes to compare incoming traffic flow at each router: (i) name-prefix match, (ii) interface match, and (iii) level of interest satisfaction ratio, i.e., rate between incoming interests to outgoing content, denoted as $\delta(r_i^j)$. In particular, $\delta(r_i^j) > 1$ denotes that the number of content packets received at router r_i^j is less than the number of interests forwarded from the same interface.

In order to mitigate IFA, ChoKIFA dynamically computes the actual size of the PIT, denoted as $\rho_{size}(r_i^j)$, at each instance. Further, ChoKIFA marks two thresholds on the PIT size, a minimum threshold ($\rho_{th}^{min}(r_i^j)$) and a maximum

threshold ($\rho_{th}^{max}(r_i^j)$), as well as, a threshold for interest satisfaction ratio, denoted as $\delta_{th}(r_i^j)$. For each interest arriving at r_i^j, if the actual PIT size is less than the $\rho_{th}^{min}(r_i^j)$, the interest gets stored in the router's PIT. If all the interests requested by C are satisfied by P or router's cache, then PIT size should not reach up to $\rho_{th}^{min}(r_i^j)$, frequently. In case of IFA, when the actual PIT size is greater than $\rho_{th}^{min}(r_i^j)$ and less than $\rho_{th}^{max}(r_i^j)$, each new incoming interest is compared with the randomly selected interest from PIT, named as *drop interest candidate*. If both the interests have the same traffic flow then both are dropped. This choice is motivated by the fact that all the entries in PIT are likely to be occupied by MIs (i.e., under IFA). On the other side, when the PIT size goes more than $\rho_{th}^{max}(r_i^j)$, all the new incoming interest are being dropped. This leads the PIT occupancy back to below $\rho_{th}^{max}(r_i^j)$.

The key attributes to identify the traffic flow of each new incoming interest are three subsequent conditions: (i) if it holds the same prefix as of drop interest candidate, (ii) if it is coming from the same incoming interface as of *drop interest candidate*, and (iii) if both the above conditions holds true, then router compares if the current $\delta(r_i^j)$ exceeds $\delta_{th}(r_i^j)$. In contrast, if the new incoming interest is not having the same traffic flow as of drop interest candidate then the randomly selected interest is remained stored in PIT, and the incoming interest is dropped/accepted with the probability (P_b) which depends on the average PIT size ($\rho_{avg}(r_i^j)$), as illustrated in Equation 1 [5].

$$P_b = \frac{P_{max} * (\rho_{avg}(r_i^j) - \rho_{th}^{max}(r_i^j))}{(\rho_{th}^{max}(r_i^j) - \rho_{th}^{min}(r_i^j))}, \tag{1}$$

here P_{max} denotes the maximum probability[4]. As the average PIT size varies from $\rho_{th}^{min}(r_i^j)$ to $\rho_{th}^{max}(r_i^j)$, the interest dropping probability P_b varies from 0 to P_{max}. In particular, the interest dropping probability is computed by exploiting the mechanism of packet dropping probability of Random Early Detection (RED) [5]. A detailed flow chart of ChoKIFA is given in Figure 2.

4.3 Parameters setting

The parameters, $\rho_{avg}(r_i^j)$, $\rho_{th}^{min}(r_i^j)$ and $\rho_{th}^{max}(r_i^j)$ are essential as they directly impact on the interest dropping probability. Below we illustrate few rules for parameter's setting which give effective performance for ChoKIFA under variety of traffic conditions while mitigating the attack.

Ensure adequate calculation of the average PIT size: ChoKIFA calculates the average PIT size using an exponential weighted moving average (EWMA). The use of EWMA for calculating $\rho_{avg}(r_i^j)$ makes sure that the short term increase in PIT size which may result from a burst of benign incoming interests (e.g., which are not satisfied due to network congestion/delay from the producer) do not result in the significant increase of average PIT size. Equation 2 illustrates the calculation of the $\rho_{avg}(r_i^j)$ where w_ρ is the weight factor for calculating EWMA and $\rho_{size}(r_i^j)$ is the current/actual PIT size [5].

[4] We take the value of maximum probability (P_{max}) to be one.

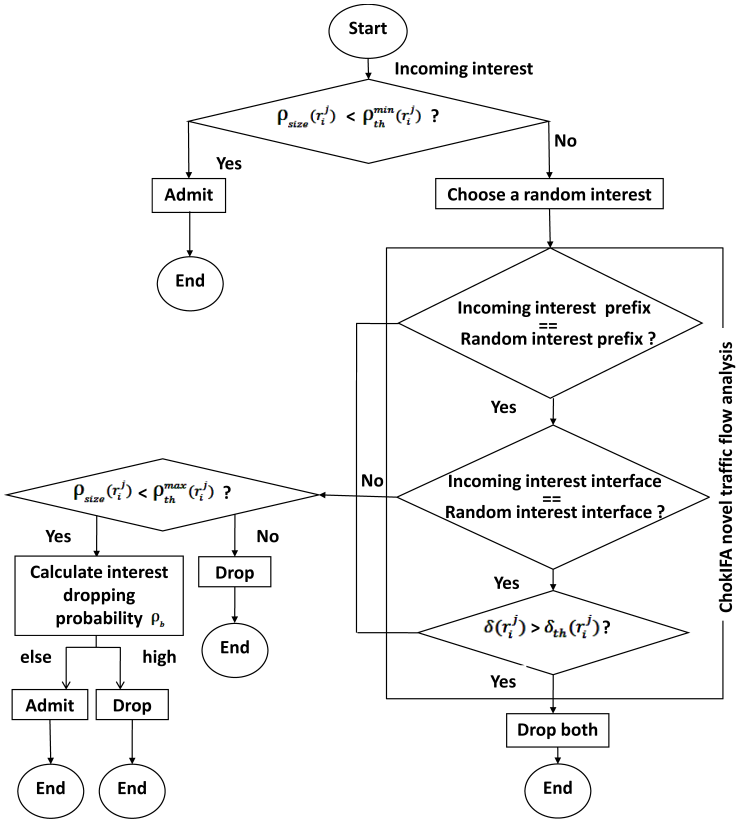

Fig. 2. ChoKIFA algorithm flowchart.

$$\rho_{avg}(r_i^j) = (1 - w_\rho) * \rho_{avg}(r_i^j) + w_\rho * \rho_{size}(r_i^j). \tag{2}$$

Note that the calculation of average PIT size can be made particularly efficient when w_ρ is set as a negative power of two[5]. If w_ρ is too large, then the averaging procedure will not filter out the temporary congestion of PIT.

Setting a minimum threshold for the PIT size: The optimal value of $\rho_{th}^{min}(r_i^j)$ depends on the desired level of $\rho_{avg}(r_i^j)$ and default network conditions. In case, the typical traffic is fairly bursty and congested, then the $\rho_{th}^{min}(r_i^j)$ should be correspondingly large to allow PIT utilization to be maintained at an acceptably high level.

Setting $\rho_{th}^{max}(r_i^j) - \rho_{th}^{min}(r_i^j)$ sufficiently large to avoid global synchronization: The optimal value of $\rho_{th}^{max}(r_i^j)$ depends in the part of maximum average delay that can be allowed to interest (e.g., round trip time for interest to retrieve

[5] In our simulations, we take w_ρ equal to 0.001.

data) and total size of PIT. A useful rule of thumb ChoKIFA implements is to set $\rho_{th}^{max}(r_i^j)$ more than thrice of $\rho_{th}^{min}(r_i^j)$ [5], since the mitigation mechanism works efficiently when max-min is larger than the typical increase in average PIT size.

5 Evaluation

We evaluate the effectiveness of our proposed approach in the presence of IFA and state of the art mitigation approaches which implements interest rate limiting based on the simple limit, interface fairness using token bucket, satisfaction ratio and with limit announcement technique [1]. To this end, we perform extensive simulations using the open-source ndnSIM [2] simulator. We evaluate the impact of IFA against ChoKIFA over three metrics which have been widely used in the related work [1, 3, 4, 9]. First, the PIT usage which indicates the available capacity of the routers to process benign traffic. Second, the percentage of BIs and MIs dropped by the network during IFA and with the proposed countermeasure. Third, we compare the efficiency our proposed countermeasure with existing mitigation approaches in terms of Interest Satisfaction Ratio (ISR) of benign users and legitimate traffic which is intended to measure the benign traffic received by users. Precisely, the lower the ISR refer, the greater amount of false positives made by the mitigation approach while distinguishing between the MIs and BIs.

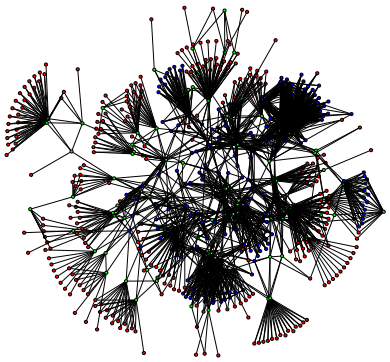

Fig. 3. Internet-like topology: 296 clients (red), 108 gateways (green), 221 backbone (blue).

Test Setup: We ran our simulations (with 100 seconds of simulation time for each experiment) on two different network topologies: a tree topology [4] (see Figure 1) and a more realistic large-scale ISP-like topology, i.e., AS-7018 [11] (see Figure 3). The selection of tree topology is because it represents one of the worst case to defend IFA [1], while the larger ISP topology reflects the performance of mitigation approach when deployed on the real Internet. The topology consist of a single P and number of consumers, including four honest

clients (C) and four adversaries (Adv) connected with multiple ICN routers. Adv requests for non-existing content (i.e., MI), which exhibits distinct suffix ($/good/rnd$) compared to valid content ($/good/data$) with frequency of 1000 interests/second. C requests the interests (BI) for valid content which are entitled to P at a rate of 30 interests/second. The total PIT size of R, i.e., 600 kilobytes, thus we set the $\rho_{th}^{max}(r_i^j)$ and $\rho_{th}^{min}(r_i^j)$ equal to 3/4 and 1/8 of total PIT capacity (i.e., 450 and 75), respectively.

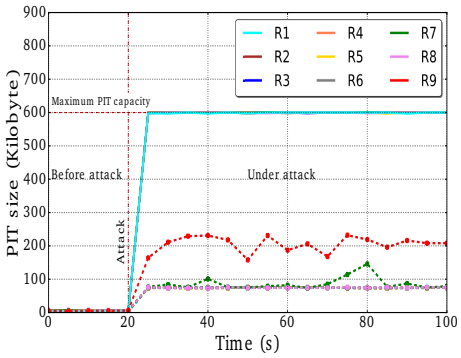

Fig. 4. PIT usage, base-line (solid lines) and ChoKIFA (dotted lines).

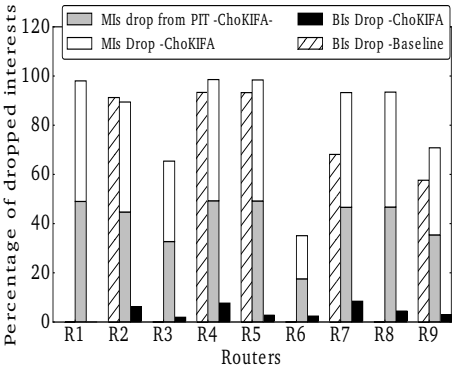

Fig. 5. BI and MI drop, base-line and ChoKIFA.

5.1 Small-scale simulation

In this section, we present the results of tree topology to evaluate the impact of attack and effectiveness of ChoKIFA. Figure 4 reports PIT usage of all the routers as a function of the simulation time under IFA for the base-line scenario (i.e., with no countermeasure) and, when the proposed countermeasure is active. In our simulations to evaluate and compare ChoKIFA under IFA, adversaries launches the attack at different time, i.e., starting from the 20th second, while the benign users starts to request for existing content from the beginning (see Figure 4). Because of the design of CHoKIFA, approach allows the IFA to fill the PIT of all the routers till 75 kilobyte before being able to start traffic flow comparison, i.e., minimum threshold of PIT. In contrast, after exceeding the minimum threshold, ChoKIFA's traffic flow comparison and interest dropping probability does not allow PITs to exceed certain level (i.e., slightly higher than 75) which depends on the dropping probability related to average PIT size. Results show (see Figure 4) that gateway node to producer attains slightly higher PIT size than the rest of routers since it receives aggregated amount of malicious traffic from the whole network.

Figure 5 reports effectiveness of ChoKIFA under IFA, in terms of legitimate (BI) and malicious traffic (MI) drop. It shows the percentage of total BIs and

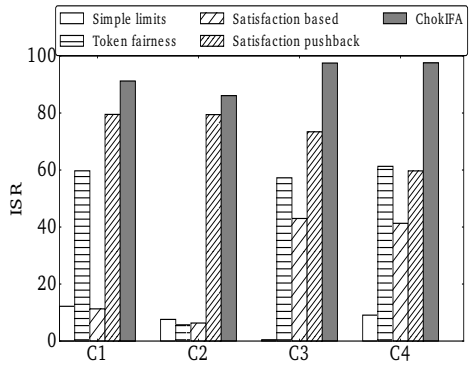

Fig. 6. Benign consumers ISR in small topology.

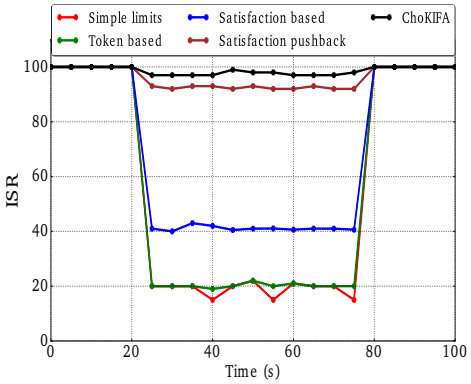

Fig. 7. Global legitimate ISR in AS-7018.

MIs dropped over total received at each router, respectively. In particular, the legitimate traffic is slightly affected (only 4% of BIs are dropped on an average) with the use of ChoKIFA, while in base-line 90% of BIs are dropped. Because the PIT is filled up with MIs, therefore, the drawn random interest from PIT is also MI with the very high probability, and in consequence ChoKIFA drops only MIs, i.e., both incoming and already stored in the PIT (see Figure 5).

Figure 6 reports the ISR of benign users which can be achieved when enabling ChoKIFA. We also compare these results with four different mitigation approaches [1]. The first three approaches are lightweight and stateless nevertheless not effective in legitimate ISR. Results show (see Figure 6) that Satisfaction-based pushback is slightly effective than previous methods but it also induces unnecessary signaling overhead by sending rate limiting announcements continuously in the whole network [1]. In particular, Figure 6 reports that ChoKIFA outperforms all four approaches in terms of all benign users ISR, remarkably. In particular, ChoKIFA is able to main 97% of all benign users ISR, moreover, induces 20 to 60% less false positives comparing to all four approaches while mitigating the attack.

5.2 Large-scale simulation

In this section, we evaluate the performance of ChoKIFA by implementing a real ISP-like topology (AS 7018) which is measured by the Rocket fuel project [11] (see Figure 3). To study the performance of ChoKIFA in ISP-like topology and under a range of conditions, we varied the percentage of adversary in the network and the frequency with which adversary is sending malicious interests.

Figure 7 confirms that rate limiting approaches [1] are not able to maintain acceptable ISR for benign users in bigger topology as well. In particular, the result shows the percentage of global ISR of all legitimate interests generated in the network, where ChoKIFA maintains almost 97% of ISR during the attack.

Note that the attack duration, in this case, is from 20 to 80 seconds. Figure 8 shows the ISR percentage of legitimate interests when we varied the percentage of attackers in the network, precisely, the values ranged from 6% attackers to over 50% attackers in the network. The results are as expected - for ChoKIFA and all four state of the art mitigation algorithms. As the number of attackers in the network increases, the lower is the ISR ratio for legitimate interests. For instance, in the case of the token bucket with per interface fairness, only 3 attackers can halve the quality of service for the remaining 13 legitimate users. While the two intelligent attack mitigation algorithms also show a decline in legitimate service quality as the percentage of attackers increases. Although ChoKIFA outperforms all mitigation algorithms and shows a very minor reduction in ISR ratio (i.e., approximately 3%) even when the attacker's percentage is raised more than 50%.

Figure 9 shows the aggregated legitimate ISR ratio when we increased malicious interest sending rate from 100 interests/second to 10000 interests/second. The result shows that ChoKIFA remains almost unaffected even with huge amount of increase in malicious interest frequency, while among all state of the art approaches only Satisfaction-based pushback shows satisfactory results.

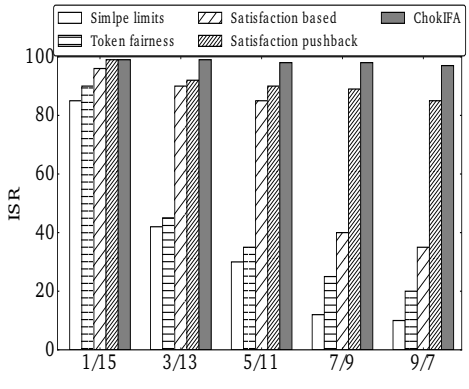

Fig. 8. Legitimate ISR with increasing adversary.

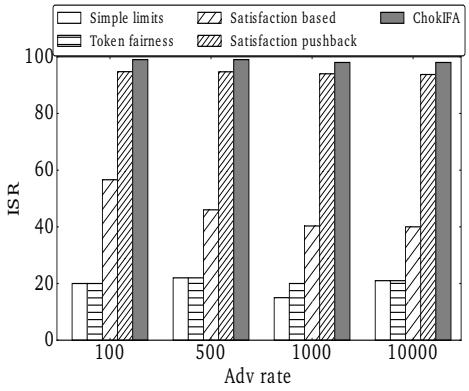

Fig. 9. Legitimate ISR with increasing malicious traffic.

6 Conclusion

In this paper, we address the interest flooding-based DDoS over NDN, which is explicitly named as IFA. More specifically, we have found that several proposed countermeasures, that adopt detection and reaction mechanisms based on interest rate limiting, are not highly effective and also damage the legitimate traffic.

In our solution, we exploited an active queue management scheme to propose an efficient detection and mitigation mechanism against IFA, which stabilizes the router PIT. The proposed approach penalizes the unresponsive flows generated by adversarial traffic by dropping malicious interests generated during

the IFA. We implemented the proposed protocol on the open-source ndnSIM simulator and compared it with the state-of-the-art. The results report that our proposed protocol effectively mitigates the adverse effects of IFA and shows significantly less false positives in comparison to the state-of-the-art IFA mitigation approaches.

References

1. Afanasyev, A., Mahadevan, P., Moiseenko, I., Uzun, E., Zhang, L.: Interest flooding attack and countermeasures in named data networking. In: IFIP Networking Conference, 2013. pp. 1–9. IEEE (2013)
2. Afanasyev, A., Moiseenko, I., Zhang, L.: ndnSIM: NDN simulator for NS-3. Technical Report NDN-0005, NDN (October 2012), http://named-data.net/techreports.html
3. Compagno, A., Conti, M., Gasti, P., Tsudik, G.: Poseidon: Mitigating interest flooding ddos attacks in named data networking. In: Local Computer Networks (LCN), 2013 IEEE 38th Conference on. pp. 630–638. IEEE (2013)
4. Dai, H., Wang, Y., Fan, J., Liu, B.: Mitigate ddos attacks in ndn by interest traceback. In: Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on. pp. 381–386. IEEE (2013)
5. Floyd, S., Jacobson, V.: Random early detection gateways for congestion avoidance. IEEE/ACM Transactions on networking **1**(4), 397–413 (1993)
6. Gasti, P., Tsudik, G., Uzun, E., Zhang, L.: Dos and ddos in named data networking. In: Computer Communications and Networks (ICCCN), 2013 22nd International Conference on. pp. 1–7. IEEE (2013)
7. Oueslati, S., Roberts, J., Sbihi, N.: Flow-aware traffic control for a content-centric network. In: 2012 Proceedings IEEE INFOCOM. pp. 2417–2425 (March 2012). https://doi.org/10.1109/INFCOM.2012.6195631
8. Pan, R., Prabhakar, B., Psounis, K.: Choke-a stateless active queue management scheme for approximating fair bandwidth allocation. In: INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. vol. 2, pp. 942–951. IEEE (2000)
9. Salah, H., Wulfheide, J., Strufe, T.: Coordination supports security: A new defence mechanism against interest flooding in ndn. In: 2015 IEEE 40th Conference on Local Computer Networks (LCN). pp. 73–81 (Oct 2015)
10. Singla, G., Kaliyar, P.: A secure routing protocol for manets against byzantine attacks. In: Computer Networks & Communications (NetCom). pp. 571–578. Springer New York, New York, NY (2013)
11. Spring, N., et al.: Measuring ISP Topologies with Rocketfuel. IEEE/ACM Trans. Netw. (2004)
12. Vassilakis, V.G., Alohali, B.A., Moscholios, I., Logothetis, M.D.: Mitigating distributed denial-of-service attacks in named data networking. In: Proceedings of the 11th Advanced International Conference on Telecommunications (AICT), Brussels, Belgium. pp. 18–23 (2015)
13. Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Crowley, P., Papadopoulos, C., Wang, L., Zhang, B., et al.: Named data networking. ACM SIGCOMM Computer Communication Review **44**(3), 66–73 (2014)
14. Zhang, L., et al.: Named data networking. ACM SIGCOMM CCR **44**(3), 66–73 (2014)