Evaluating and Mitigating Malicious Data Aggregates in Named Data Networking

Kai Wang[1], Wei Bao[2], Yingjie Wang[1] and Xiangrong Tong[1]
[1] School of Computer and Control Engineering, Yantai University
Yantai 264005 - China
[e-mail: wangkai_bw@163.com, towangyingjie@hotmail.com, txr@ytu.edu.cn]
[2]School of Architecture, Yantai University
Yantai 264005 - China
[e-mail: baowei2016@icloud.com]
*Corresponding author: Kai Wang

Received July 26, 2016; revised February 7, 2017; accepted June 2, 2017; published September 30, 2017

Abstract

Named Data Networking (NDN) has emerged and become one of the most promising architectures for future Internet. However, like traditional IP-based networking paradigm, NDN may not evade some typical network threats such as malicious data aggregates (MDA), which may lead to bandwidth exhaustion, traffic congestion and router overload. This paper firstly analyzes the damage effect of MDA using realistic simulations in large-scale network topology, showing that it is not just theoretical, and then designs a fine-grained MDA mitigation mechanism (MDAM) based on the cooperation between routers via alert messages. Simulations results show that MDAM can significantly reduce the Pending Interest Table overload in involved routers, and bring in normal data-returning rate and data-retrieval delay.

Keywords: Named Data Networking (NDN), Malicious Data Aggregates (MDA), Interest Flooding Attack (IFA), Network Security

1. Introduction

With the rapid growth of modern information technologies, the working way of Internet has shifted from communications between hosts with exact locators to a global platform for content or service distributing. To keep pace with this trend, Named Data Networking (NDN) emerges and becomes one of the promising candidates for next-generation Internet technologies [1]. NDN uses named data rather than Internet Protocol (IP) addresses as the "waist" of the Internet, where service and content distribution are more important than communications, just according with the new trend of modern networking technologies [2].

NDN embeds two distinct types of packets termed as **Interest packet** and **Data packet** to support content or service retrieving based on explicit names. Moreover, to support efficient content distribution technologies such as content caching and adaptive forwarding, NDN implements three core compenonts named Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB) within each router. CS caches Data packets to satisfy future Interest packets with the same names, PIT records the information such as names and incoming interfaces of all the forwarded Interest packets, and FIB guides how to forward an Interest packet.

The basic working mechanism of NDN is as following: 1) Interest packets are used by Internet users to request for corresponding content, which is carried by Data packets. Whenever a router receives an Interest packet, the corresponding Data packet returns to answer it if the Data packet is already cached in CS. In this case, the Interest packet is satisfied by the CS within this router directly, without further forwarding. Otherwise, PIT check is performed: if the name information of this Interest packet has been recorded in PIT, the Interest packet will be discorded and only the information of its incoming interface in this router will be recorded into the existing PIT entry; else, the information of the Interest packet including name and incoming interface will be recorded as a new PIT entry. After PIT check is finished, the Interest packet will be forwarded according to the FIB. 2) Upon a Data packet, the PIT check is performed firstly in each router: if the name of the Data packet is not exist in PIT, this Data packet will be dropped directly; otherwise, the Data packet will be cached in CS, and then be forwarded from where its corresponding Interest packet comes in, which can be acquired from the corresponding PIT entry.

In NDN, Data packets return to consumers only if certain consumers have already asked for them by sending corresponding Interest packets, which can improve the resilience of NDN to counter some notable network threats such as Distributed Denial-of-Service (DDoS) attacks [3], because Data packets cannot be delivered to anywhere unscrupulously unless they have been issued by explicit Interest packets. That is, NDN is the data-driven network architecture, and security by design is among one of the natural requirements of NDN.

However, there still are some serious network threats existing in NDN. For example, Interest Flooding Attacks (IFA), which are considered as the NDN-specific DDoS attacks, can easily degrade the performance of NDN by severely exhausting the forwarding or memory resource of routers with excessive amount of spoofed Interest packets requesting for nonexistent Data packets, becoming one of the most difficult NDN security problems [4]. Current works on IFA countermeasures mainly focus on how to decrease the number of malicious Interest packets kept in the memory of each involved NDN router, but none of them attempt to counter the situation where malicious Interest packets cooperate with Data packets to congest network links [5]. For example, one of the variant types of IFA named Malicious

Data Aggregates (MDA) is such a threat. In MDA, attackers issue extensive amount of malicious Interest packets with varying and different content names to request for large amount of existent Data packets, which can severely congest the network links and significantly degrade the performance of NDN. The varying and different content names in malicious Interest packets of MDA can degrade the hit ratio of malicious Interest packets in CS of each router along the requesting path, and thus guarantee as many as possible Interest packets be forwarded as far as possible, to achieve larger damage effect on NDN. More worse, different from IFA, when MDA is launching, there only are very limited number of expired PIT entries within routers since attackers request for existent rather than nonexistent content, which causes that current state-of-the-art countermeasures designed for IFA cannot be used for detecting or mitigating MDA.

Thus, this paper focuses on MDA damage evaluation and countermeasures, and the contributions of this paper summarize as follows:

1) Whether MDA is realistic in NDN (that is, whether it is easy to implement) and its damage effect are evaluated, via extensive simulations under a realistic, large-scale network topology as well as using realistic user behavior.

2) To efficiently and timely identify and mitigate MDA, the MDA Mitigation mechanism (MDAM) is proposed. The idea of MDAM is "to detect everywhere, but to mitigate at the source" (here "everywhere" means any router in NDN while "source" means the first-hop routers via which hosts access into NDN network). MDAM detects MDA based on two detection phases that have different complexities (e.g., detecting at a granularity of per-prefix or per-prefix-per-interface) and mitigate its damage effect by blocking the incoming malicious Interest packets at the edge of NDN (e.g., the first-hop routers).

3) The performance of MDAM is evaluated using the well-known ndnSIM [7] from both routers/network and users side, and simulation results demonstrate that MDAM can quickly detect MDA and then effectively mitigate its damage effect.

The rest of this paper is organized as follows. Section 2 overviews the related works. Section 3 gives the evaluation of MDA damage. Section 4 designs the MDAM to mitigate MDA, while Section 5 evaluates the performance of MDAM. Finally, Section 6 concludes this paper.

2. Related Work

The data-driven characteristic of NDN may bring in dangerous network threats which harm NDN by issuing large amount of malicious Interest packets [6], either exhausting the memory resource of routers (IFA) or causing too many returning Data packets to congest the links (MDA).

Most of the current works focus on IFA in NDN [8]. The works in [9] analyzes the data-driven states of NDN can degrade its security level and make it vulnerable to IFA, because both content or service publications and subscriptions can bring new routing and forwarding states at the network layer. One of our previous works in [10] introduces an analytical model considering the CS size, PIT size, number of expired PIT entries, attacking rate and so on, to analyze the damage effect of IFA on NDN, and another in [11] proposes a rate-limiter based IFA countermeasure within each router, but it has a serious impact on mistakely decreasing the rate of legitimate Interest packets. Moreover, the research of [12] proposes the "Interest traceback" mechanism to de-stress the memory load of each IFA-attacked NDN router, by sending spoofed Data packets to satisfy and then delete the pending spoofed Interests recorded in PIT when attack is detected. Obviously it is not suitable

for MDA mitigation, because the constructed spoofed Data packets would aggravate the congestion on the attacking-involved network links. In addition, the work in [4] designs three IFA countermeasures with different implementation complexities and effectiveness to mitigate IFA, based on hierarchical forwarding queues at routers and varying Interest flagging mechanisms. However, the key factor of detection in these three solutions are all severely relying on the satisfication rate of Interest packets at each interface of a router, which does not fit the MDA mitigation scenario since the number of expired PIT entries is much less than in IFA, making the detection much more difficult for MDA.

All of above research regards MDA is a serious threat to NDN, just as IFA. However, they all leave it as an open problem, and the design specifics for identifying MDA remain to be filled in. The only MDA countermeasure which embeds design details can be found in [13], which is called RDAI and in fact is one of our previous work. RDAI detects MDA based on both the expired rate of the PIT entries within each router, and evaluating link load by calculating the maximum number of expected Data packets that can come in and be sent out from each interface of the router. RDAI can detect MDA, but it lacks cooperative mechanisms between routers and only detects MDA within each router alone, which cannot guarantee high detection accuracy. Moreover, it does not embed any MDA mitigation mechanisms, and thus cannot degrade the damage effect of MDA on NDN.

To the best of our knowledge, the proposed MDAM is the first complete mechanism that can simultaneously detect and mitigate MDA in NDN.

3. Evaluation for MDA Damage

3.1 Parameter Setting

An in-depth evaluation study of MDA damage using extensive ndnSIM-based simulations is presented, to show MDA is not just theoretical, by monitoring the dynamic of PIT size, rate and delay of successfully returned Data packets, in scenarios with and without MDA. The realistic and large-scale Rocketfuel's AT&T topology [14] (shown in **Fig. 1**) is used in simulations, as well as realistic user behavior model where all Interest packets follow Zipf-Mandelbrot distribution [15]. The 625 nodes from Rocketfuel's AT&T topology are extracted and classified into three categories: nodes with degree less than four are clients (296 nodes), nodes directly connected to clients are gateways (221 nodes), and remaining nodes are backbones (108 nodes). **Table 1** shows the bandwidth and delay settings for links based on their types, and **Table 2** shows the detailed settings for all simulation parameters.

Table 1. Ranges for link bandwidth and delay in simulation topology

Link type	Bandwidth	Delay
Backbone-Backbone	40Mbps - 100Mbps	5ms - 10ms
Gateway-Backbone	10Mbps - 20Mbps	5ms - 10ms
Gateway-Gateway	10Mbps - 20Mbps	5ms - 10ms
Client-Gateway	1Mbps - 3Mbps	10ms - 70ms

Table 2. Simulation parameters

Name	Value
Content items in network	10,000
Size of each content item	1024 bytes (8192 bits)
Number of clients	296
Number of gateways	221
Number of backbones	108
CS size	500 content items
PIT size	100 entries
Expired time for PIT entry	1 second
Size of each Interest packet	5 bytes
Rate of legitimate Interest packets	20 Interests per second
Rate of malicious Interest packets	400 Interests per second
Duration for legitimate Interests	0 - 60th second
Duration for malicious Interests	20th - 40th second
Number of malicious nodes	40% of clients

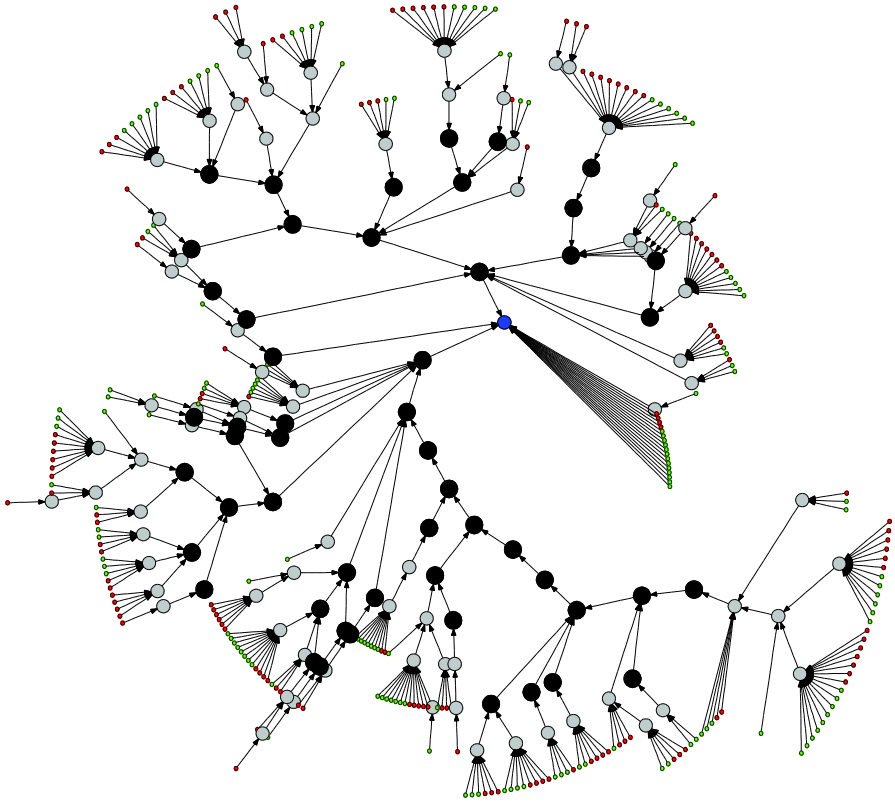

Fig. 1. Rocketfuel's AT&T topology

The content source where content items are generated and published is placed at a randomly selected gateway, which can return Data packets to satisfy Interest packets requesting for certain content. The number of content items with different popularities follows Zipf-Mandelbrot distribution, that is, content items of class k are requested with probability $\{q_k\}_{k=1, 2, \ldots, K}$, where $q_k = c/(k + q)^{\alpha}$, $c = \{ \sum_{k=1}^{K} 1/(k+q)^{\alpha} \}^{-1}$, with $\alpha = 0.7$, $q = 0.7$ and $K = 10000$,

just following the default setting for α and q in ndnSIM [7]. The percentage of malicious nodes is about 40% (according to [4]), and they are randomly picked in each simulation run.

In simulations, MDA attackers flood excessive number of malicious Interest packets to request for really existent content, but with a manner of round-robin style (randomly change the names of Interest packets every one single second), in order to bypass cached content at routers as many as possible and retrieve a large number of malicious Data packets, which can bring in not only PIT exhaustion but also link congestion.

To evaluate the damage effect of MDA on PIT of routers, we randomly select a gateway router named "gw-12906" which connects with both legitimate and malicious clients in simulation topology, and a backbone router named "bb-13131" involved in MDA, to check how the PIT size varies with and without MDA.

To evaluate the damage effect of MDA on congesting network links, we randomly select six legitimate clients ("leaf-12482", "leaf-12495", "leaf-12514", "leaf-12520", "leaf-12552", "leaf-12673"), by monitoring the rate of successfully returning Data packets and Data-retrieving delay with and without MDA.

3.2 Simulation Results of MDA

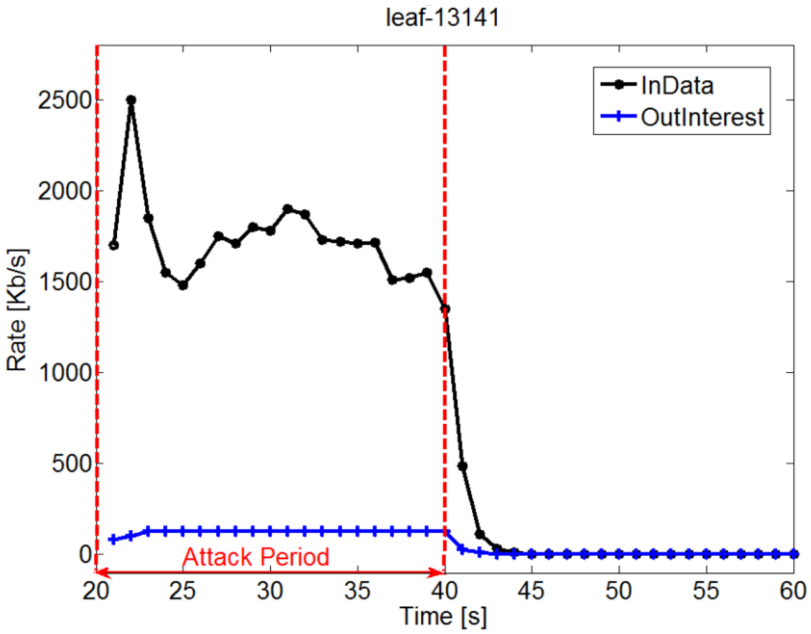

Fig. 2. Packets from and to MDA attackers

Fig. 2 shows the amount of the returned Data packets requested by malicious Interest packets from a randomly selected attacker "leaf-13141". From this figure, during the MDA attacking period between 20th and 40th second, although the sending-rate of malicious Interest packets is only about 125Kb/s, the rate of the returned malicious Data packets reaches up to about 1750Kb/s for only one attacker, which fits the characteristic of MDA (malicious Interests requesting for existent content) and shows MDA can cause severe congestion on network links since it can the traffic by enlarge the malicious traffic by several times.

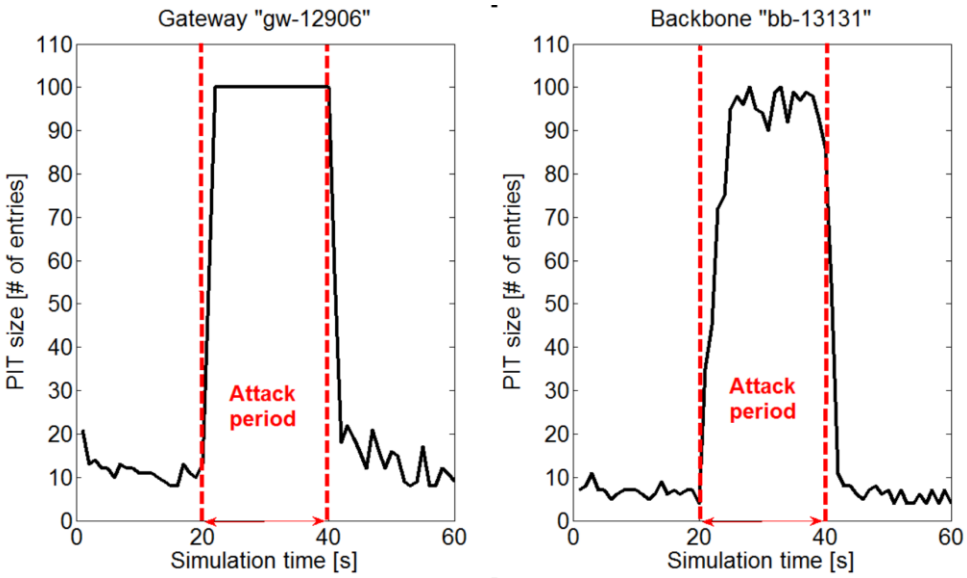

Fig. 3. PIT size for NDN router suffering MDA

Fig. 3 shows that the PIT size for the randomly selected gateway router or backbone router increases dramatically when suffering MDA, which means MDA can severely damage NDN routers by exhausting their memory resources. For example, the PIT size of the backbone router "bb-13131" increases dramatically from about 7 to 95 entries on average, almost reaching the maximum of the PIT and thus significantly consuming the resource of this router for forwarding future Interest packets. In this case, legitimate Interest packets would be dropped due to the overloaded PIT of NDN routers.

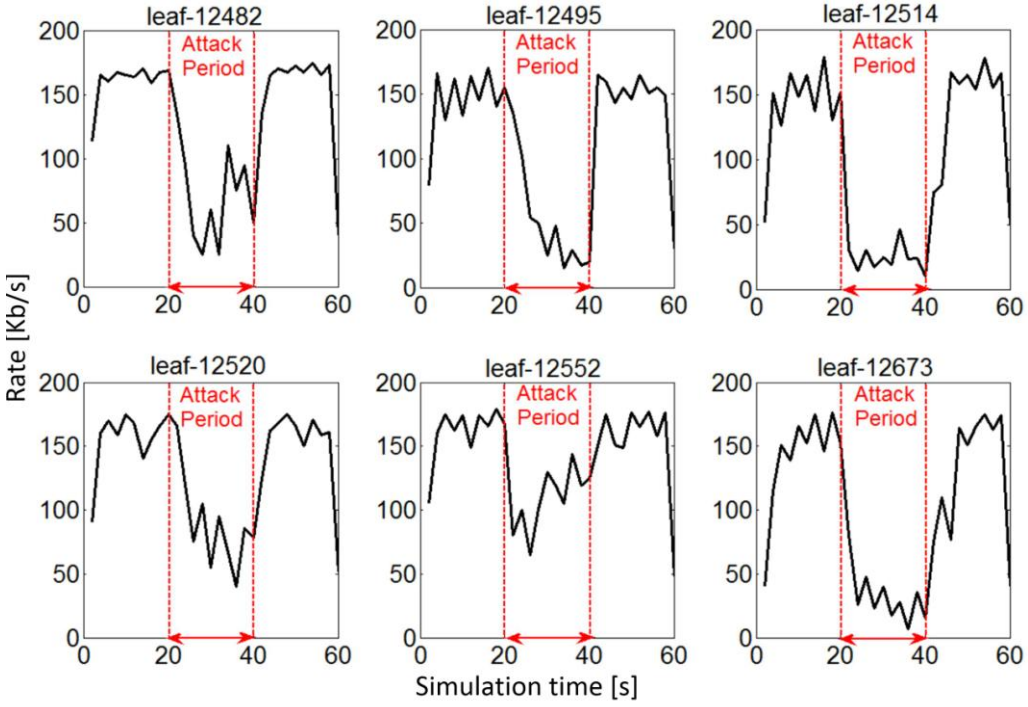

Fig. 4. Rate of returned Data packet for legitimate clients suffering MDA

Fig. 4 shows the rate of the successfully retrieved Data packets requested by each of the randomly selected legitimate users. We can observe that the amount of incoming Data packets are severely decreased during the attack period of MDA (20^{th} second ~ 40^{th} second), although the amount of Interest packets issued by them are always keeping at the same level in the simulations. Thus, the aim of MDA on degrading users' experiences of retrieving their wanted content in NDN is achieved.

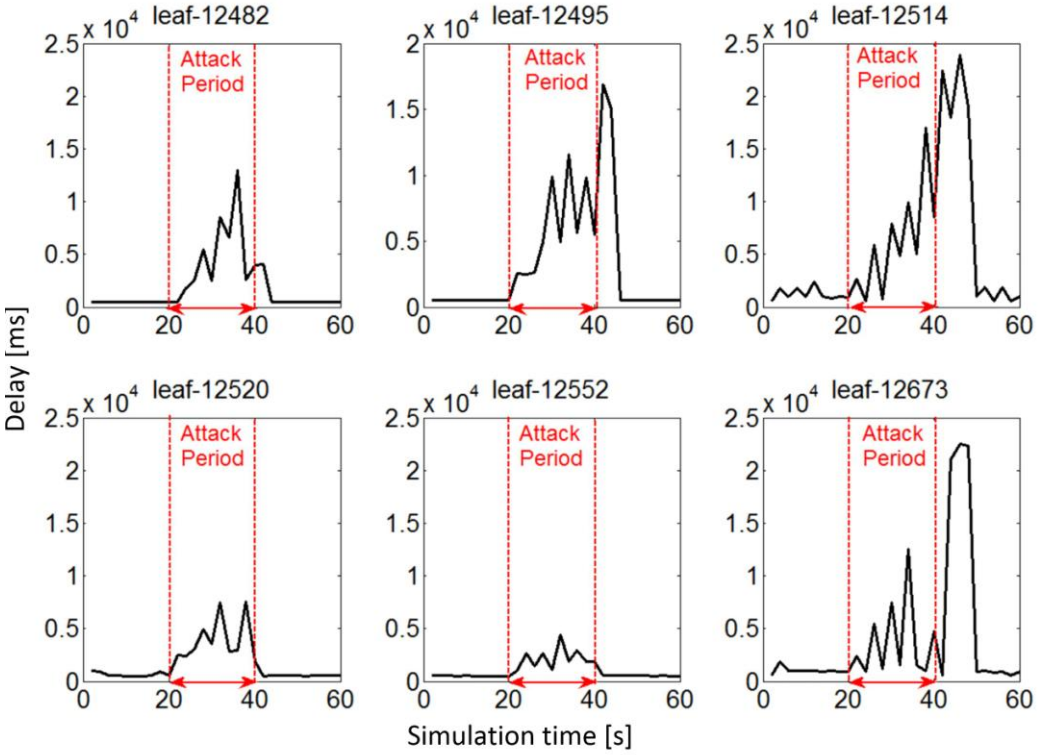

Fig. 5. Delay for legitimate clients suffering MDA

Fig. 5 shows the delay for outgoing Interest packets retrieving their corresponding Data packets for each selected node suffering MDA. For all legitimates users, the delay increases dramatically during the attack period of MDA. Moreover, the delay returns to its normal level at a slower rate than the MDA vanishes (at the finishing point of 40^{th} second, the delay remains at a larger value for 2 out of 6 selected legitimate users). Thus, MDA takes a huge damage on NDN because the users' experience would be significantly degraded due to much larger delays.

4. MDAM Design

4.1 Overview of MDAM

The NDN model, where MDA is detected and mitigated by the proposed MDAM, is as following: we model NDN as a graph of interconnected nodes (routers). Each node may have any number of clients (hosts) attached which request and receive content. Clients can only

connect to one node at the same time. Nodes can either serve requests immediately or relay them to other nodes in the network. All the routers that have connections to clients are identified as the first-hop routers for these clients.

MDAM is a set of algorithms that run on routers, and has low degree of implementation complexity. Its goal is to identify MDA as well as to mitigate its damage effect. The mechanism of MDAM is "to detect everywhere, but to mitigate at the source" (here "everywhere" means any router in NDN while "source" means each of the first-hop routers). Noting that, the routers upstream can aggregate more traffic than the first-hop routers, which makes them the better monitoring point to detect any attacks. On the other hand, if mitigating MDA at everywhere instead of only at the source, it may nourish the damage effect of MDA since some legitimate Interests requesting content with the same prefix as the malicious Interests and coming from the same interfaces where malicious Interests come in would be filtered as well. This is because it is difficult to distinguish the legitimate Interests from malicious Interests at the intermediate routers (not the first-hop routers) since each of the interfaces receives all the Interests from downstream (may include Interest packets from both attackers and legitimate users). Thus, the detection mechanism of MDAM is enabled at each router of NDN while its mitigation mechanism is only enabled at the first-hop routers.

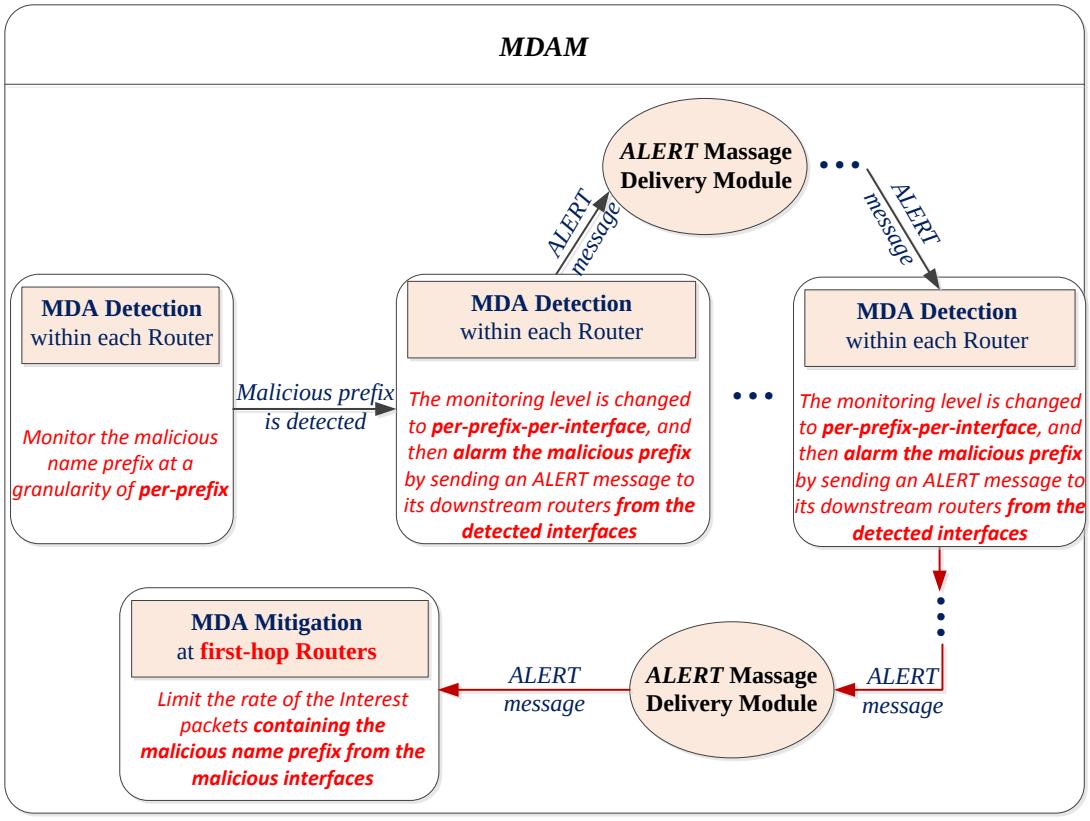

Fig. 6. MDAM framework

MDAM keeps several statistics on expired Interests for each router. In particular, for each of them it records the namespace, the incoming interfaces and the information whether its corresponding Data packet returns in time. As illustrated in **Fig. 6**, Each router monitors the

number of expired Interests pending in PIT to check the possibility of MDA at the granularity of per-prefix. Whenever MDA is detected at any router, this router will notify its downstream routers starting to monitor the number of expired Interests at a finer granularity, that is, per-prefix-per-interface, by sending an *ALERT* message that records the malicious prefix (which is being attacked) downstream from the incoming interface where malicious Interests come in and then cause expired PIT entries. In this way, the *ALERT* messages will be finally sent to the first-hop routers through which the malicious Interests come into NDN (because each of the interfaces located at the delivery path where the malicious Interests travel through should have unusual number of expired Interests because of link congestion, which is larger than its predefined threshold), where the mitigation mechanism of MDAM is enabled by imposing a filter at each of the interfaces of the first-hop routers where malicious Interest packets come in (to limit the rate of in-coming malicious Interests causing MDA).

To sum up, MDAM continuously monitors the rates of unsatisfied Interests with respect to overall pending Interests in PIT of each single router at the level of coarse granularity, in order to determine if there is MDA existing in NDN. If they exceed their predefined thresholds, MDAM then turns to monitor through which interfaces these malicious Interest packets come in (at the level of a finer granularity, per-prefix-per-interface). Dividing the detection mechanism to two phases described above can avoid exceptionally restrictive in forwarding Interests when there is no MDA existing, because MDAM only needs to monitor at the coarse granularity (per-prefix) unless MDA emerges, which achieves small consumption on each NDN router. As for the mitigation mechanism, MDAM sets a filter on each of the offending interface(s) only at the first-hop routers to limit the rate of the incoming malicious Interests. Since any and every attacker needs to connect to the first-hop routers to enable communication in NDN (has been described before), the malicious incoming interface can be determined gradually and finally by MDAM.

4.2 MDAM details

Algorithm 1 The first detection phase of MDAM

Require: MDAM-enabled router periodically monitors the number of expired PIT entries under per-prefix ($E(p)$) against its predefined threshold (P_{th});
Ensure: The malicious prefixes that should be monitored;
Input: The number of expired PIT entries under per-prefix
Output: The malicious prefixes
1: For each of the prefixes based on FIB:
2: **if** $E(p) > P_{th}$ **then**
3: The list of malicious prefixes are extracted from FIB;
4: **else**
5: continue;
6: **end if**

Algorithm 2 The second detection phase of MDAM

Require: The list of malicious prefixes has been identified at the first phase of MDAM;
Ensure: The malicious interfaces that should be monitored (for all routers) or through which the *ALERT* messages are sent out (for routers except the first-hop routers);
Input: Which interfaces the Interest packets causing unnormal number of expired PIT entries under per-prefix
Output: The forwarding interfaces where *ALERT* messages are sent out

```
1: Through which interfaces these malicious Interests come
   in are checked based on PIT:
2: if E(p)(f) > Fth then
3:    The list of the malicious interfaces corresponding to
      these malicious Interests are detected;
4: else
5:    continue;
6: end if
7: if It is one of the first-hop routers then
8:    The Interest-incoming rate of each of the detected malicious
      interfaces is decreased within decay period;
9: else
10:   ALERT messages are sent downstream from these malicious
      interfaces, carrying the malicious prefixes;
11: end if
```

MDAM detects the MDA at every NDN router, and it contains two phases (the corresponding pseudocodes for the two detection phases are shown in **Algorithm 1** and **Algorithm 2**, respectively).

First, as **Algorithm 1**, every MDAM-enabled router periodically monitors the number of expired PIT entries under **per-prefix**, denoted as $E(p)$, against its predefined threshold (P_{th}), every after an detection period (e.g., monitoring every after one second that is just the default TTL for each Interest packet in [7]). Each of the malicious prefixes is identified whenever its $E(p)$ exceeds its P_{th}. The list of the detected prefixes is extracted from FIB by MDAM in each NDN router.

Second, as **Algorithm 2**, whenever the malicious prefixes are identified, MDAM then monitors through which interfaces these malicious Interests come in according to PIT, and then checks the number of the corresponding expired PIT entries (recording these malicious Interests) at a granularity of **per-prefix-per-interface** ($E(p)(f)$) against its predefined threshold (F_{th}). In this case, a malicious interface can be identified whenever its $E(p)(f)$ exceeds F_{th}. The list of the monitored interfaces corresponding to these malicious Interests is extracted from the PIT by MDAM, because it records all the information where (through which incoming interfaces) the Interests come from. Whenever the malicious interfaces are detected, the *ALERT* messages (recording the malicious prefixes) are sent to the routers downstream from these malicious interfaces, except the first-hop routers that have no downstream routers and thus do not send out any *ALERT* messages. As shown in **Fig. 7**, the prefix of the *ALERT* message is reserved as */ALRET/MDA* in our implementation and the payload of each of these messages records the malicious prefix(s).

/ALERT/MDA	Payload (recording the malicious prefix)

Fig. 7. Alert message

Dividing the detection mechanism of MDAM into two phases instead of monitoring per-prefix-per-interface from beginning to the end can significantly decrease the overhead. For example, given the average number of prefixes extracted from FIB at each router are 20 (among which there are three malicious prefixes), and the average number of interfaces belonged to each prefix extracted from PIT is 10, the number of items that MDAM needs to monitor periodically is 20 and $max\{20, 10\times3\} = 30$ respectively at two different detection phases, while the number increases to be $20\times10 = 200$ when monitoring per-prefix-per-interface from beginning to the end rather than dividing the detection mechanism into two phases.

Whenever a router receives the *ALERT* messages, it turns to the second detection phase to monitor the malicious Interests based on the malicious prefix learnt from the *ALERT* messages at all the interfaces (which means monitoring at the granularity of per-prefix-per-interface). That is, when the attack is detected at anywhere of NDN, the involved routers along the attacking path through which malicious Interests are delivered are triggered to monitor the attack at a more refined granularity (per-prefix-per-interface). Since the $E(p)(f)$ for each involved interface of the routers along the attacking path exceeds its F_{th} during the attack period, the *ALERT* messages can be finally delivered to the first-hop routers of NDN (which connect to the attacks and legitimate users directly) through the path comprised by these involved interfaces. Nothing that when the first-hop routers receive the *ALERT* messages and have successfully determined the corresponding malicious interfaces where malicious Interests come in, through the second phase described above (to check if $E(p)(f) > F_{th}$ for every interfaces), the mitigation mechanism of MDAM is triggered: the Interest-incoming rate of each of the detected malicious interfaces is decreased because the hosts directly connect with these interfaces are identified as attackers (in the **Section 5** of this paper, we do a case study that all the Interest packets requesting the malicious prefix(es) are dropped directly at all the involved interfaces of the first-hop routers). The mitigation mechanism of MDAM is disabled if there are not any *ALERT* messages arrive within a decay period, which can be defined as several times of the detection period (e.g., 10 seconds that is five times of the detection period of every NDN router).

5. Evaluating MDAM's Effectiveness

In this section, we implement MDAM at each NDN router in **Fig. 1**. Firstly, we evaluate its performance from the network/routers side to check if the PIT size for each involved router can be decreased successfully and timely. And then, we evaluate its effect on increasing the amount of successfully returned Data packets for legitimate users, and on decreasing the delay for legitimate users retrieving content when suffering MDA.

In this part, the experimental settings are set to be the same as **Section 3.1**, except that each of the routers is implemented with MDAM. Based on the trace files of **Section 3.1**, the average number of expired PIT entries per-prefix at each router is about one entry per second, and the average number of expired PIT entries per-prefix at per-interface at each router is about 0.2 entry per second in our simulated scenarios. Based on this observation, in all simulations, we set the P_{th} to be ten times of the normal value, that is, ten entries per second at each router (P_{th}

=10). Similarly, we set the F_{th} to be two entries per second at each router (F_{th} =2). In addition, the detection period of MDAM is set to 2 seconds and the decay period is set to 10 seconds. It is worth noting that if selecting smaller but still reasonable thresholds, MDAM can achieve better performance (e.g., NDN can recover from MDA much more quickly if we set P_{th} =3 and F_{th} =0.6, which we have not presented in this paper but indeed have evaluated such scenarios in ndnSIM-based simulations, because we only focus on investigating and showing if MDAM can really mitigating the damage effect of MDA on NDN with given parameter settings, rather than analyzing how it can achieve better performance, which leaves as our future work).

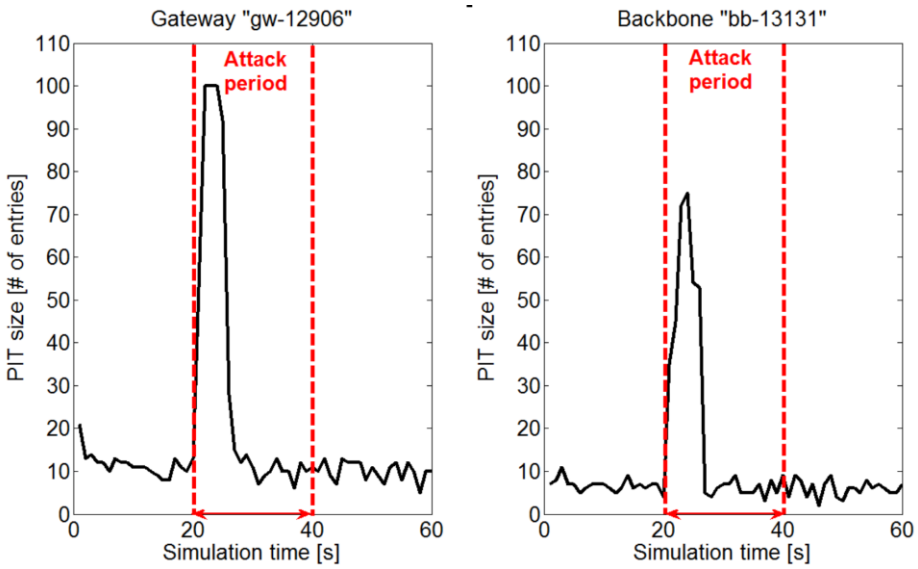

Fig. 8. PIT size for MDAM-enabled NDN router that suffers MDA

Fig. 8 shows the PIT sizes dynamic of the selected gateway router and backbone router when NDN is suffering MDA (both of the two routers are MDAM-enabled). We can observe that at the very beginning of MDA, the PIT sizes of both of these two routers increase dramatically from less than 10 entries to more than 70 entries. However, only about seven seconds after MDA launches, the PIT sizes for both routers recover to their normal levels (about 10 entries for the gateway router and 5 entries for the backbone router), which means that MDAM can successfully and timely prevent NDN routers from MDA with proper parameter settings. The involved routers that are suffering MDA can keep their PIT sizes almost at the normal level when protected by MDAM, which guarantees the legitimate Interests can get available PIT resource when they come in these routers and thus be forwarded normally (almost the same when there is no MDA occurring in NDN). That is, the damage effect of MDA on NDN routers can be effectively mitigated by MDAM. This is significant for legitimate users to successfully retrieve their wanted content (we will evaluate this in the following of this sub-section).

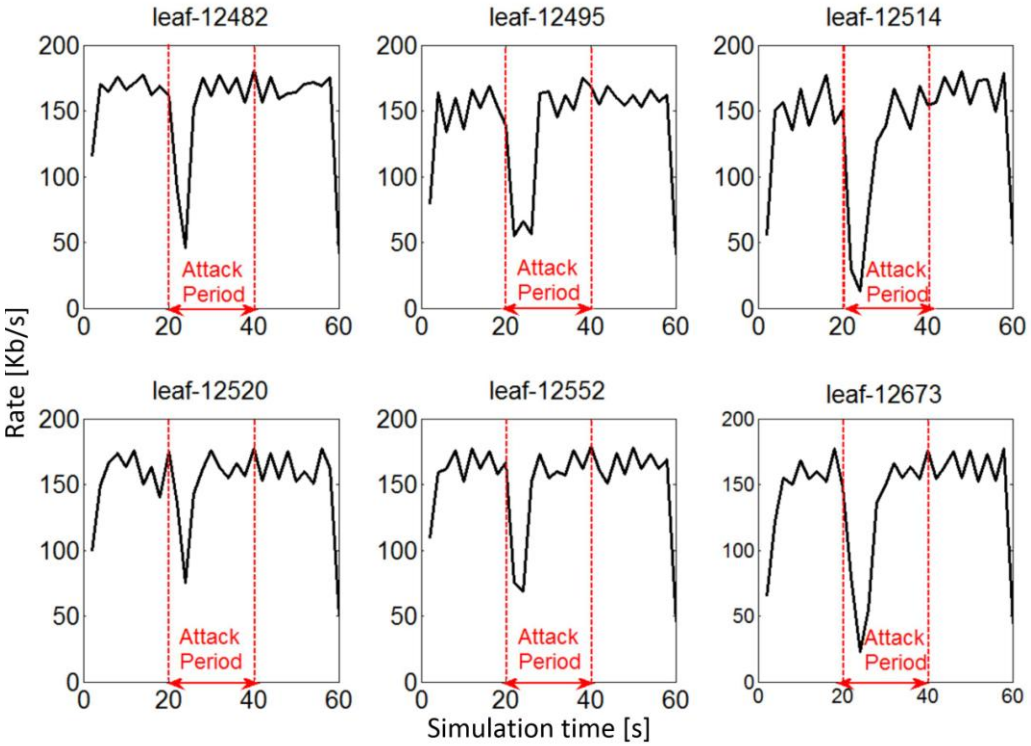

Fig. 9. Varying of returned Data packets for clients when MDAM-enabled NDN suffering MDA

Fig. 9 shows the amount of the returned Data packets for six randomly selected NDN users suffering MDA when MDAM is enabled at each router. When MDA launches at the 20*th* second, the rate of successfully returned Data packets decreases significantly from about 175*Kbits/s* to close to 0, which means the legitimate users cannot get any content when MDA launches. The reason is the memory resource of PIT of each involved NDN router that suffers MDA is almost totally exhausted by the malicious Interest packets from MDA attackers, causing almost all the legitimate Interests are dropped by the overloaded routers without retrieving any content. But only after less than 7 seconds, the rate of in-coming Data packets returns to almost the same as its normal level (175*Kbits/s* when not suffering MDA), because MDAM limits the rate of in-coming malicious Interest packets at each of the in-coming interfaces of the first-hop routers for MDA attackers. Thus, MDAM can quickly detect MDA and effectively mitigate its damage effect on blocking legitimate users to retrieve content within a relatively small time scale.

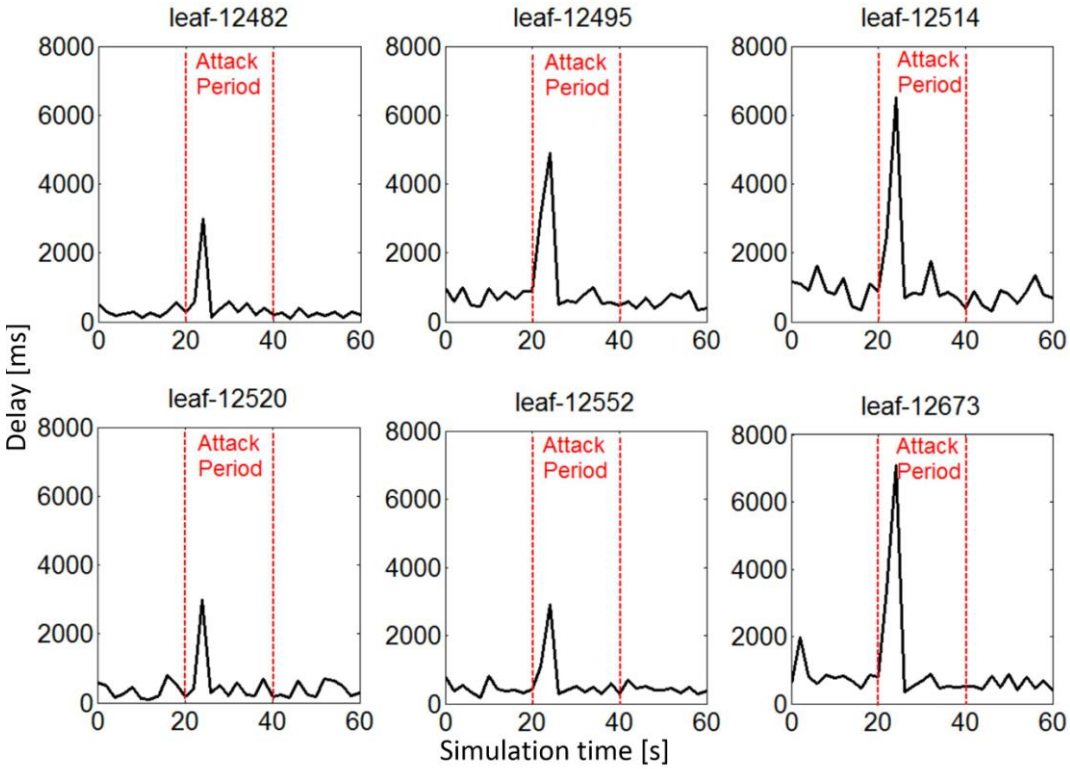

Fig. 10. Delay for legitimate users when MDAM-enabled routers suffering MDA

Fig. 10 shows the delay for each of the randomly selected legitimate users requesting for corresponding Data packets, who are suffering MDA while MDAM is enabled at each router. From this figure. When MDA launches at the 20*th* second, the delay for each of the legitimate users increases significantly (from smaller than 200*ms* to larger than 3000*ms*) within 7 seconds (before the 27*th* second). This is because the memory resource for PIT in each involved NDN router is almost totally exhausted by MDA, and thus the legitimate Interests may be dropped or badly delayed by any of the overloaded routers. In this case, legitimate users may need to continuously re-issue their Interests to retrieve the corresponding Data packets to increase the chance of legitimate Interests kept in PIT, which results in a larger delay for retrieving their wanted content. After less than 7 seconds since MDA launches, the delay for each of the legitimate users is quickly decreased by MDAM to its normal level. This is because MDAM can almost totally limit the rate of in-coming malicious Interest packets from the source (the first-hop routers), making the number of pending malicious Interests in each PIT of the involved routers decreases almost to 0. That is, MDAM can almost make the delay for legitimate users retrieving their wanted content keep at the same level with and without MIA, which can certainly guarantee the users' experience on retrieving content.

6. Conclusion

In this paper, we have presented an in-depth evaluation of MDA's damage effect on significantly degrading users' experience when retrieving content in NDN, via extensive simulations under a large-scale network topology as well as based on realistic user's behavior, showing it is not just theoretical. Furthermore, we propose the MDAM, which detects MDA

based on exploiting the state information of each NDN router and mitigates it at the first-hop routers. Simulation results show that MDAM can quickly detect MDA and can significantly mitigate its damage effect, bringing in smaller memory resource consumption for NDN routers as well as better users' experience (e.g., smaller delay for retrieving content). That is, MDAM is helpful on developing a more secure and reliable NDN.

In our future work, we will focus on how to counter MDA more efficiently by exploiting the cooperative mechanisms between the key functional modules (e.g., CS and PIT cooperation to improve the detection accuracy of MDA and IFA) within each router.

Acknowledgement

This work was supported by National Natural Science Foundation of China (NSFC) [grant number 61702439]; Shandong Provincial Natural Science Foundation China[grant number ZR2017BF018] Shandong Province Higher Educational Science and Technology Program [grant number J16LN17, J14LN24].

References

[1] V. Jacobson, D.K. Semtters, J.D. Thornton, M.F. Plass, N. H. Briggs and R. L. Braynard, "Networking named content," *Communications of the ACM*, vol. 55, no. 1, pp. 117-124, January, 2012. Article (CrossRef Link)

[2] J. Kurose, "Information-Centric Networking: The Evolution from Circuits to Packets to Content," *Computer Networks*, vol. 66, pp. 112-120, June, 2014. Article (CrossRef Link)

[3] S.T. Zargar, J. Joshi and D. Tipper, "A survey of defense mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2046-2069, March, 2013. Article (CrossRef Link)

[4] A. Afanasyev, P. Mahadevan, E. Uzun and L. Zhang, "Interest Flooding Attack and Countermeasures in Named Data Networking," in *Proc. of IFIP Networking*, pp. 217-225, May 22-24, 2013. Article (CrossRef Link)

[5] R. Tourani, T. Mick, S. Misra and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *arXiv:1603.03409v2(submitted to IEEE Communications Surveys & Tutorials)*, pp. 1-35, September, 2016. Article (CrossRef Link)

[6] E. G. Abdallah , H. S. Hassanein and M. Zulkernine, "A Survey of Security Attacks in Information-Centric Networking," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1441-1454, January 2015. Article (CrossRef Link)

[7] S. Mastorakis, A. Afanasyev, I. Moiseenko and L. Zhang, "ndnSIM 2.0: A new version of the NDN simulator for NS-3," NDN, *Technical Report NDN-0028*, pp. 1-8, January, 2015. Article (CrossRef Link)

[8] P. Gasti, G. Tsudik, E. Uzun and L. Zhang, "DoS & DDoS in Named-Data Networking," in *Proc. of 22nd International Conference on Computer Communication and Networks* (*ICCCN*), pp. 1-7, July 30 - August 2, 2013. Article (CrossRef Link)

[9] M. Wahlisch, T. C. Schmidt and M. Vahlenkamp, "Lessons from the Past: Why Data-driven States Harm Future Information-Centric Networking," in *Proc. of IFIP Networking*, pp. 253-261, May 22-24, 2013. Article (CrossRef Link)

[10] K. Wang, J. Chen, H.C. Zhou, Y.J. Qin and H.K. Zhang, "Modeling Denial-of-Service against Pending Interest Table in Named Data Networking," *International Journal of Communication Systems*, vol. 27, no. 12, pp. 4355-4368, December, 2014. Article (CrossRef Link)

[11] K. Wang, H.C. Zhou, H.B. Luo, J.F. Guan, Y.J. Qin and H.K. Zhang, "Detecting and Mitigating Interest Flooding Attacks in Content-Centric Network," *Security and Communication Networks*, vol. 7, no. 4, pp. 685-699, April, 2014. Article (CrossRef Link)

[12] H. Dai, Y. Wang, J. Fan and B. Liu, "Mitigate DDoS Attacks in NDN by Interest Traceback," in *Proc. of IEEE INFOCOM NOMEN Workshop*, pp. 381-386, April 14-19, 2013. Article (CrossRef Link)
[13] K. Wang, H.C. Zhou, J. Chen and Y.J. Qin, "RDAI: Router-based Data Aggregates Identification Mechanism for Named Data Networking," in *Proc. of the Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 116-121, July 3-5, 2013. Article (CrossRef Link)
[14] N. Spring, R. Mahajan and D. Wetherall, "Measuring ISP topologies with rocketfuel," *IEEE/ACM Transactions on Networking (TON)*, vol. 12, no. 1, pp. 2-16, February, 2004. Article (CrossRef Link)
[15] G. Carofiglio, L. Muscariello and M. Gallo, "Bandwidth and storage sharing performance in Information Centric Networking," in *Proc. of ACM SIGCOMM workshop on ICN*, pp. 26-31, August 15-19, 2011. Article (CrossRef Link)

Kai Wang (*wangkai_bw@163.com*, *wangkai.phd@outlook.com*) received his B.S. degree in Electronic Science and Technology, and Ph.D. degree in Communication and Information System, both from Beijing Jiaotong University (BJTU), respectively in July 2009 and June 2014. Now he works as a Postdoctor in the Research Institute of Information Technology (RIIT) at Tsinghua University. Before joined in Tsinghua University, he is an assistant professor in Yantai University during December 2015 to June 2017, and an Engineer in the 41st Institute of China Electronics Technology Group Corporation (CETC) during July 2014 to December 2015. His research interests include next generation Internet technology and network security.

Wei Bao (*baowei2016@icloud.com*) received her B.S. degree in Art Design from Anyang Institute of Technology in July 2010. Now she works as a research assistant in the School of Architecture at Yantai University. She holds one patent on enhancing network security in future Internet. Her research interests include next generation Internet technology and future networking architecrures.

Yingjie Wang (*towangyingjie@hotmail.com*) was born in 1986, China. She received the Ph.D. degree in Computer Science and Technology from Harbin Engineering University. She visited Georgia State University from 2013/09 to 2014/09 as a visiting scholar. Dr. Wang is currently an assistant professor in the School of Computer and Control Engineering at Yantai University. Her research interestsare trust computing, mobile social networks and Internetware. She has published 20 papers in well known journals and conferences in her research field. Inaddition, she has presided one National Natural Science Foundation of Chinaprojects, and joined three National Natural Science Foundation of China projects and one Natural Science Foundation of Heilongjiang Province project.

Xiangrong Tong (txr@ytu.edu.cn) received his Ph.D. degree in Computer Science and Technology from Beijing Jiaotong University. He is a Full Professor in Yantai University, and is the Vice-Dean of the School of Computer and Control Engineering, Yantai University. His research interests are computer science, intelligent information processing and social networks. He has published more than 30 papers in well known journals (e.g., Expert Systems with Applications) and conferences.