Journal of Network and Computer Applications 130 (2019) 1–13

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Efficient DDoS attacks mitigation for stateful forwarding in Internet of Things☆

Gang Liu [a], Wei Quan [a,*], Nan Cheng [b], Hongke Zhang [a], Shui Yu [c]

[a] School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China
[b] Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada
[c] School of Software, University of Technology Sydney, NSW, Australia

ARTICLE INFO

Keywords:
Internet of Things
DDoS attacks
Stateful forwarding
Network security

ABSTRACT

Stateful forwarding plane is fully considered as a novel forwarding paradigm, which is proven to be beneficial to delivery efficiency and resilient to certain types of attacks. However, this fresh attempt also introduces "varietal" Denial-of-Service attack due to complicated forwarding state operations, which may cause long-term memory exhaustion of forwarding nodes, especially for resource-limited IoT nodes. This new distributed exhaustion attack is extremely hidden and there is currently no effective defense against it. In this paper, we first establish a game model to analyze the attack benefit between attacker and defender. To further make the defender obtain more utility, it is significative to make the defender manage expired state-entries during stateful forwarding. To this end, we propose an enhanced distributed low-rate attack mitigating (eDLAM) mechanism. Particularly, eDLAM maintains a lightweight malicious request table (MRT), which is very small, to offload burden of practical forwarding state table. When a packet request is matched in MRT, it will be marked and dropped directly without any impact on forwarding state table. Based on this, eDLAM adopts an optimal threshold update method for MRT to achieve a maximum defender utility. We evaluate the eDLAM performance in terms of false negatives rate (FNR) and false positives rate (FPR). Extensive experimental results show that eDLAM can reduce FNR by 10.5% and FPR by 44% on average compared with state-of-the-art mechanisms.

1. Introduction

With emergence of Internet of Things (IoT), billions of "things" (such as vehicles) can be connected to exchange information, which can greatly improve many aspects of human lives (Parsons, 2016; Qin et al., 2016; Cheng et al., 2018). However, the issue of cybersecurity is as vital as IoT technology itself to affect its further application and development (Khan and Salah, 2018). Most of current IoT systems still adopt the host-to-host communication means, which was designed several decades ago and deposes several chronic drawbacks. The straightforward and conservative forwarding design also brings many kinds of security threats (Yu et al., 2012). According to Cisco statistics, more than one-third of organizations experienced a breach in the year 2016 (Cisco, 2017). This situation is even more abominable in IoT systems, because IoT devices are usually generally limited with resources (such as less computing capacity and power). Thus, how to effectively mitigate security attack becomes a key research issue for IoT development.

To tackle this challenge, many recent researches start to pursue novel Internet paradigms, which are expected to overcome drawbacks in the conventional Internet. For example, Farinacci et al. proposed a locator/identifier separation protocol, which aims to decouple the binding between device identity and location (Farinacci et al., 2013). Jacobson and Zhang et al. proposed a clean slate Internet paradigm, named Named Data Networking (NDN), which decouples the content/location binding by using name-based forwarding rather than IP-address based one (Van et al., 2014). Software defined networking (SDN) was proposed to separate control and forward functions, and has been well applied in many IoT scenarios (Quan et al., 2017, 2018a). More recently, Zhang et al. proposed a novel network architecture

☆ This work is supported by the National Natural Science Foundation of China (NSFC) (No. 61602030, 61702439, 61802014 and 91638204), the National Key R&D Program (No. 2017YFE0121300), and Shandong Provincial Natural Science Foundation, China (No. ZR2017BF018).

* Corresponding author.
E-mail addresses: gangliu@bjtu.edu.cn (G. Liu), weiquan@bjtu.edu.cn (W. Quan), n5cheng@uwaterloo.ca (N. Cheng), hkzhang@bjtu.edu.cn (H. Zhang), shui.yu@uts.edu.au (S. Yu).

https://doi.org/10.1016/j.jnca.2019.01.006
Received 20 June 2018; Received in revised form 22 November 2018; Accepted 7 January 2019
Available online 14 January 2019

Table 1
Some stateful forwarding paradigms.

Stateful Forwarding Paradigms	Designed to Solve the Problems:	Introduce Some Other Problems:
NDN[a]/CCN[b] DONA[c] NETINF[d]	Host-centric, insufficient IP address, low utilization of resources (Yi et al., 2013; Wählisch et al., 2013).	Traffic amplification attack (Wählisch et al., 2013; AbdAllah et al., 2015).
SDN[e]	Signaling overhead between switch and controller, and the latency shortcomings (Dargahi et al., 2017).	Overload the switch memory (AbdAllah et al., 2015).
LISP[f]	The binding between device identity and location (Farinacci et al., 2013).	Disrupt a specific targeted service (Yan et al., 2016)

[a] Named Data Networking.
[b] Content Centric Networks.
[c] Data Oriented Network Architecture.
[d] Network of Information.
[e] Software Defined Networking.
[f] Locator/ID Separation Protocol.

called smart identifier network (Zhang et al., 2016; Luo et al., 2013). This network paradigm adopts a reference model with three layers and two domains, which can solve triple bindings in conventional Internet, including resource/location binding, user/network binding and control/data binding.

As a common feature, many new Internet paradigms support *stateful forwarding* to improve data dissemination efficiency and robustness (listed in Table 1) (Yi et al., 2013; Wählisch et al., 2013; Dargahi et al., 2017). It can also provide an intrinsic support to network-level Denial-of-Service (DoS) defense (Zargar et al., 2013; Yu et al., 2011). That is because it enables intermediate nodes to record forwarding state, which allows the forwarding nodes make actions during forwarding process to mitigate attacks to endpoints. Moreover, stateful forwarding has great potential to meet other IoT requirements (Abdullahi et al., 2015; Amadeo et al., 2016; Zhang et al., 2014; Ni et al., 2018). On the one hand, stateful forwarding facilitates efficient data dissemination in dynamic environments according to opportunistic in-network caching. On the other hand, it can provide adaptability to different IoT applications. For example, IoT devices can adopt various heterogeneous communication means (*e.g.,* Zigbee (Ndih and Cherkaoui, 2016), WiFi (Pokhrel and Williamson, 2018), LiFi (Sharma et al., 2018) and Bluetooth (Harris III et al., 2016)), which can be well supported by stateful forwarding (Muralidharan et al., 2017, 2018; Mick et al., 2018; Saxena and Raychoudhury, 2017; Bizanis and Kuipers, 2016).

Unfortunately, stateful forwarding introduces new *varietal DoS attacks* to resource-limited IoT nodes. For example, since information-centric networking (ICN) (*e.g.*, NDN, DONA, NETINF) records the forwarding state in each IoT node, it leads to traffic amplification when DoS attacks occur (AbdAllah et al., 2015; Li et al., 2015). Moreover, popular flows can be cached during stateful forwarding, thus, attackers can set up lots of fake flows to overload the node memory (Yan et al., 2016; Quan et al., 2014; Saucez et al., 2016). There are several countermeasures to mitigate this new kind DoS attack (Gasti et al., 2013). However, *low-rate distributed state exhaustion attack* can be very hidden and there is currently no effective defense against it. In these attacks, attackers issue a small number of different malicious packets, which are disastrous because the sending rate is too small to be detected using the existing mechanisms. Moreover, since transit nodes record state entries locally in the process of stateful forwarding, they are vulnerable to the distributed state exhaustion attack (Zhi et al., 2018). Typically, the attacker can easily cause large-scale network attack because there are many transit nodes in IoT.

In this paper, we first establish an attacker and defender game to analyze the attacker and defender utility, and find that managing the expired state entries can make the defender achieve more utility. Therefore, we propose an enhanced distributed low-rate attack mitigating (eDLAM) mechanism to make defenders obtain maximum utility. In specific, eDLAM detects an attack event according to analyzing the expired state entries, and selects an optimal threshold for the defender to obtain maximum utility. We implement the eDLAM mechanism and evaluate its performance in terms of false negatives rate (FNR) and false positives rate (FPR). The main contributions of this paper can be summarized as follows .

1. We establish a game theory based model for analyzing *low-rate varietal DoS attacks*, and form an attacker and defender game. To make defender win the game, we believe it is necessary to manage expired state-entries in the stateful forwarding.
2. We propose an eDLAM mechanism which adopts a threshold-based detection method to manage the expired state-entries in forwarding state table, hence to make defender obtain utility. Particularly, eDLAM maintains a lightweight malicious request table (MRT) to offload burden of forwarding state table. When a packet request is matched in MRT, it will be marked without any impact on forwarding state table. Moreover, eDLAM supports an optimal threshold to get maximum utility for the defender.
3. We implement the eDLAM mechanism[1] and evaluate its performance compared to state-of-the-art mechanisms. Evaluation is carried out in both simple linear topology and actual large-scale topology according to practical scenario. Simulations results show that eDLAM can reduce FNR by 10.5% and reduce FPR by 44% on average.

The remainder of this paper is organized as follows. Section 2 introduces the model of attacks based on game theory, and demonstrates the problem formulation and motivation. Section 3 presents the eDLAM mechanism and provides the analysis for setting the optimal detection threshold. Section 4 evaluates the performance of eDLAM. Section 5 provides an overview of the related work. Finally, we summarize the paper in Section 6.

2. System model and analysis

Stateful forwarding suffers from low-rate varietal DoS attacks due to its forwarding state table, hence mitigating the attacks in one of the stateful forwarding paradigms (listed in Table 1), as well as the others. In this section, we consider *naming-related attacks* as an example (AbdAllah et al., 2015). In this type of attacks, attackers issue many malicious Interests with the same non-existent prefix to occupy memory resources, which makes the IoT nodes deny services to legitimate users. There are many countermeasures to mitigate naming-related attacks. However, these countermeasures do not consider distributed low-rate naming-related attacks. In other words, many attackers issue a small number of non-existent Interests with different prefixes.

In this section, we model the attacks as an attacker and defender game based on game theory. Specifically, the defender is the IoT node.

[1] The source codes are available via github.com (Liu et al., 2018a, b).

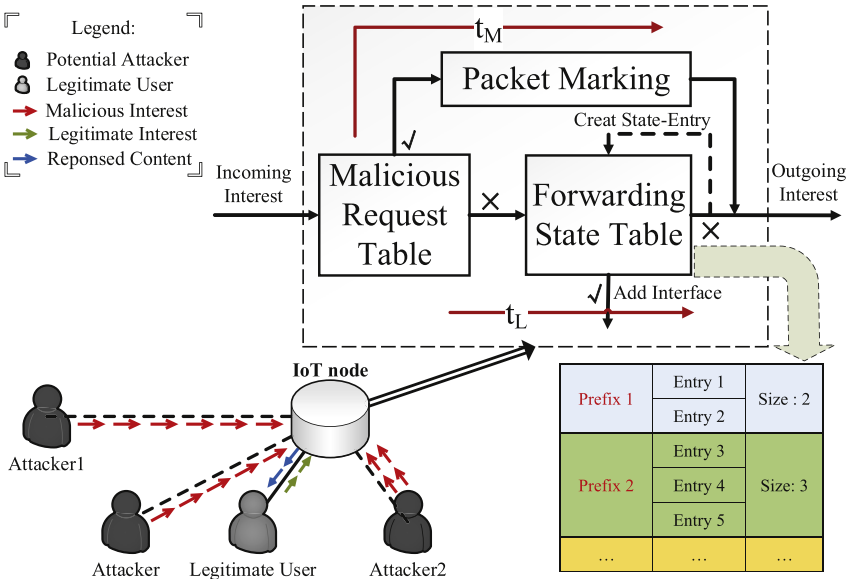


Fig. 1. Stateful forwarding process.

We utilize the model to analyze the distributed low-rate naming-related attacks, and we also theoretically demonstrate the most effective way to deal with the attacks.

2.1. Defender and attacker game model

In the existing threshold-based detection methods of *naming-related attacks*, many methods have been proposed to differentiate malicious Interests from legitimate Interests. In other words, *malicious Interests and legitimate Interests are processed differently by IoT nodes*. According to the game theory, we assume that the utility of an attacker is the time taken by the IoT node to deal with a malicious Interest, the utility of the IoT node is the time taken by the attacker to send a malicious Interest, and thus, the attacker and the IoT node form a zero-sum game.

Assumption. As shown in Fig. 1, assuming that the attacker issues r_A malicious Interests in the time period of T, and its prefix is "/dst/attacker". The detection threshold set by stateful forwarding mechanism is r_{TH}, and $r_A > r_{TH}$.

Definition. The time taken by IoT nodes to process a legitimate Interest is denoted as t_L, including the time to find the state-entry, insert it, and add the interface information to it. When a malicious Interest is identified, the time taken by the IoT nodes to process the malicious Interest as t_M, including the time taken to add the arrival interface information. The time taken by users or attackers to issue an Interest as t_S, and the experimental results are shown in Table 2. Further, t_L and t_M satisfies: $t_L > t_M$.

Model: In *naming-related attacks*, attackers issue r_A malicious Interests in the time period of T, with the prefix of "/dst/attacker". In the current round of the game, if ($r_A > r_{TH}$), then an IoT node can identify malicious Interests. The cost incurred by the IoT node is the time taken to process a malicious Interest (denoting as: t_M), whereas the cost incurred by the attacker is the time taken to send an Interest (denoting as: t_S). In that case, the utility of the IoT node can be denoted as $\Phi(r_A)$ which is a function of r_A.

$$\Phi(r_A) = r_A t_S - r_A t_M = r_A(t_S - t_M) \tag{1}$$

In the other case, if ($r_A < r_{TH}$), then the cost incurred by the IoT node is the time taken to process a legitimate Interest (denoting as: t_L), because malicious Interests are regarded as legitimate ones using the existing mechanisms. In the current round of the game, the utility of the IoT node can be denoted as $\Psi(r_A)$ which is also a function of r_A.

$$\Psi(r_A) = r_A t_S - r_A t_L = r_A(t_S - t_L) \tag{2}$$

Based on Eqs. (1) and (2), we can obtain:

$$\mu_R = \begin{cases} \Phi(r_A) & r_A > r_{TH} \\ \Psi(r_A) & r_A < r_{TH} \end{cases} \tag{3}$$

Eq. (3) demonstrates the model of the utility of the IoT node, and the following analysis is based on the model. Most of the existing attack mitigating mechanisms assume that the attackers issue the malicious Interests with the same prefix. Besides, the number of malicious Interests (denoting as: r_A) is great larger than the detection threshold. Based on the Assumption, the utility of the IoT node is:

$$\mu_{R_1} = \Phi(r_A) \tag{4}$$

2.2. Problem formulation

AssumptionWhen *distributed low-rate naming-related attacks* occur, for the sake of simplicity, we suppose there are two attackers. They respectively send r_{A_1} and r_{A_2} malicious Interests in the time period of T. However, the sum of r_{A_1} and r_{A_2} is r_A which is the same with the assumption in subsection A. Besides, each attacker issues the malicious Interests with the different prefixes "/dst/attacker1" and "/dst/attacker2" respectively. They satisfy the following condition:

$$r_{A_1} < r_{TH}, r_{A_2} < r_{TH}, r_{A_1} + r_{A_2} = r_A > r_{TH} \tag{5}$$

Inference: At this moment, the players are attacker1, attacker2, and the IoT node connected to both attacker1 and attacker2. In the existing mechanism, the detection algorithm determines whether the expiration rate of state-entries **under each prefix** (listed in Fig. 1) is greater than the threshold. Since $r_{A_1} < r_{TH}, r_{A_2} < r_{TH}$, *the attacks cannot be detected*

Table 2
Average time.

t_L	t_M	t_S
524 μs	353 μs	445 μs

using the existing mechanism. In other words, the IoT node judges the malicious Interests as legitimate Interests. The utility of the IoT node is:

$$\mu_{R_2} = \Psi(r_{A_1} + r_{A_2}) = \Psi(r_A) \tag{6}$$

Since $t_M < t_L$, we can achieve $\mu_{R_1} > \mu_{R_2}$, i.e., in the scenario of distributed low-rate naming-related attacks, the utility of the IoT node decreases with the existing mechanism.

2.3. Potential countermeasure

Assumption. Assume that we add the expiration rate of state-entries **under all the prefixes** (listed in Fig. 1) in *distributed low-rate naming-related attacks*, and subsequently, we compare this sum with the threshold to judge whether the IoT node is being attacked. Notably, $r_{A_1} + r_{A_2} = r_A > r_{TH}$, therefore, the IoT node can identify malicious Interests.

Inference: The cost incurred by the IoT node is the time taken to process a malicious Interest (denoted as t_M); whereas the cost incurred by the attackers is the time taken to send an Interest (denoted as t_S). Therefore, the utility of the IoT node is:

$$\mu_{R_3} = \Phi(r_{A_1} + r_{A_2}) = \Phi(r_A) \tag{7}$$

It is evident that $\mu_{R_3} = \mu_{R_1}$, in other words, if we use the potential mechanism to add the expiration rate under all the prefixes, even in distributed low-rate naming-related attacks, the IoT node will achieve the same utility as the existing mechanism in naming-related attacks.

2.4. Advantages of the potential mechanism

However, whether the potential mechanism can achieve more utility than the existing mechanisms is to be investigated. Based on the above analysis, we re-write the utilities of the existing and potential mechanisms when there are multiple attackers.

$$\begin{aligned} \mu_{EM} &= \Phi(r_{A_1} + r_{A_2}) \quad r_{A_1},\ r_{A_2} > r_{TH} \\ \mu_{PM} &= \Phi(r_{A_1} + r_{A_2}) \quad r_{A_1} + r_{A_2} > r_{TH} \end{aligned} \tag{8}$$

Proposition. *According to* Eq. (8), *it is evident that the value of* μ_{EM} *is equal to* μ_{PM}. *How about the probability of* $r_{A_1},\ r_{A_2} > r_{TH}$ *and* $r_{A_1} + r_{A_2} > r_{TH}$? *The answer is* $P\left(r_{A_1},\ r_{A_2} > r_{TH}\right) \neq P\left(r_{A_1} + r_{A_2} > r_{TH}\right)$.

We can obtain $\mu_{PPM} \geq \mu_{PEM}$ according to Appendix A. Thus, *if we use the potential mechanism, the IoT node probably achieves more utility*. Besides, we also do an experiment using the Matlab in which we randomly generate r_{A_1}, r_{A_2} and r_{th}. The experimental result (shown in Fig. 2) demonstrates that the possible utility of the potential mechanism is larger than the existing mechanism. That is, the potential mechanism is effective for detecting not only naming-related attacks, but also other attacks in stateful forwarding.

3. eDLAM mechanism

This section introduces the eDLAM mechanism which is based on the aforementioned potential mechanism. In order to discuss the eDLAM mechanism in detail, we implement the mechanism in NDN. Particularly, such a mechanism can also be transplanted to other stateful forwarding paradigms. We consider NDN as an example because we can perform experiments in NDN-Cxx and NDNSIM (Mastorakis et al., 2017), which we demonstrate in the following section.

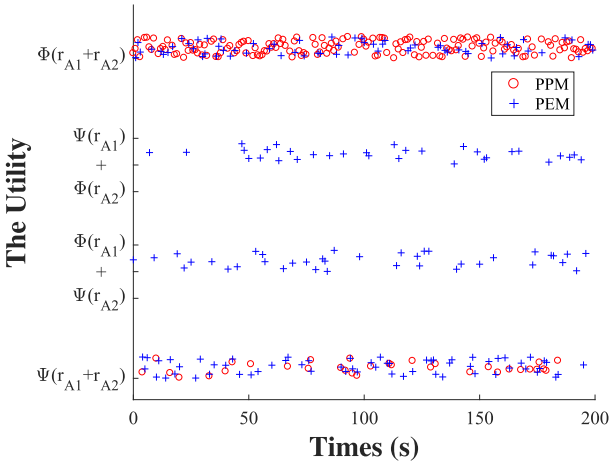


Fig. 2. The utility of the potential and existing mechanism.

3.1. Operating principle

As shown in Fig. 2, the content cache (CS), the pending interest table (PIT), and the forwarding information table (FIB) are respectively the same as those in the original NDN. CS is used to cache content. PIT records the Interest forwarding path. FIB is used to determine where to forward the Interest. Moreover, *malicious request table (MRT) is the list of malicious Interest prefixes. Packet-marking is used to add the arrival interface to the field of* "Append Name" *of the Interest packet*.

When an Interest arrives at an IoT node, the IoT node matches with the CS first. If there is a cache of the requested Data, the IoT node directly issues the Data by the incoming face that the Interest arrive. Otherwise, the IoT node will match with the MRT; if it is a success, it indicates that the Interest prefix is under attack. Note that even if the prefix is matched with the MRT, the IoT node cannot regard the Interest as a malicious Interest, because malicious Interests may have the same prefix as legitimate Interests. Therefore, it is necessary for packet-marking to add the arrival interface to the field of "*Append Name*" of the Interest packet (Yu et al., 2016). Finally, the Interest is forwarded based on FIB. If it is matched with the MRT unsuccessfully, it is a legitimate Interest, and subsequent processing is the same as the traditional NDN forwarding process.

When a Data packet arrives at an IoT node, if there is no append field, *i.e.*, the Interest prefix that the Data responds to is not in MRT, subsequent processing is the same as the traditional NDN forwarding process. However, if the Data has an append field, *i.e.*, the corresponding Interest prefix is in the MRT, the Data is forwarded based on the interface information in the field of "*Append Name*" (Wang et al., 2013).

3.2. Malicious request table (MRT)

MRT is the list of prefixes of malicious Interests. When the prefix matches with the MRT successfully, it indicates that the prefix is under attack. As shown in Fig. 3, eDLAM extends the "expired counter" field in FIB, counting the expired Interests under each prefix constantly. If the sum of all the prefix "expired counters" per second satisfies the threshold ($\sum_{k=1}^{k=n} Numk > Threshold$), we can consider that the IoT node is under attack.

If eDLAM identifies that an IoT node is being attacked, the main concern is to *distinguish the prefix of malicious Interests from the various prefixes (Prefix 1 ~ n) in FIB*. Subsequently, this malicious prefix is added to MRT. Some prefixes in the FIB are legitimate Interest prefixes,

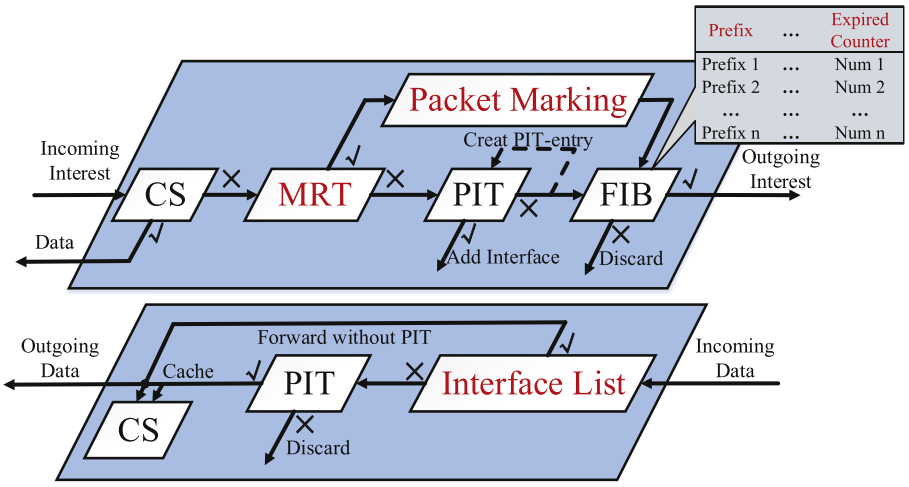


Fig. 3. eDLAM Forwarding Process.

whereas others may be malicious Interest prefixes. In eDLAM, the prefix is added to MRT with the probability given as follows:

$$P = \frac{Num\ k}{\sum_{k=1}^{k=n} Num\ k} \tag{9}$$

On the one hand, network packet loss rate is very small; therefore, it is infrequent for legitimate Interests to expire owing to packet loss. In other words, the value of "Expired Counter" is very small. On the other hand, attackers usually issue a large number of malicious Interests, and the Interests cannot be satisfied. In other words, the value of the prefix "Expired Counter" is very large. Therefore, it is reasonable to add prefixes to the MRT with the probability of P. Accordingly, *adding a legitimate Interest prefix to MRT has a very low probability, whereas adding a malicious Interest prefix has a high probability*.

3.3. Setting the optimal threshold

In this subsection, we demonstrate how to set the optimal threshold, because such a threshold can make IoT node obtain max-utility. Particularly, false total rate, which is the sum of FPR and FNR, is taken into our consideration. It is evident that we can obtain max μ_R by minimizing the false total rate.

Assumption. The eDLAM provides theoretical support for setting the optimal detection threshold. We denote n_L as the rate of legitimate Interests arriving at the IoT node per second, n_M as the rate of malicious Interests arriving at the IoT node per second, the network packet loss rate as e_r, and the detection threshold as r_{TH}. We assume that all the Interests arriving at the IoT node follow Poisson distribution. Particularly, legitimate, malicious and dropped legitimate Interests arrival process follow $Poisson(n_L t), Poisson(n_M t), Poisson(n_L e_r t)$ respectively.

Definition 1. The probability that the expired Interest is a legitimate Interest is given as $P_L = n_L e_r/(n_L e_r + n_M)$. While the probability that the expired Interest is a malicious Interest is given as $P_M = n_M/(\mathrm{n_L e_r} + \mathrm{n_M})$.

Definition 2. As described in subsection B, eDLAM adds the prefix to MRT with the probability of P. Subsequently, the probability of adding legitimate Interest prefixes to MRT is given as $P_{LM} = P(\mathbb{C}) \cdot n_L e_r/(n_L e_r + n_M)$. (where $\mathbb{C}$ denotes the event: $n_L e_r + n_M > r_{TH}$.) While the probability of adding malicious Interest prefixes to MRT is given as $P_{MM} = P(\mathbb{C}) \cdot n_M/(n_L e_r + n_M)$.

Inference: The following subsection discusses the wrong decisions made by eDLAM. We denote P_1 as FPR, which means a legitimate Interest has expired but eDLAM regards it as a malicious Interest incorrectly, in other words, eDLAM adds its prefix to MRT; thus, we obtain $P_1 = P_L \cdot P_{LM}$. Besides, we denote P_2 as FNR, which means a malicious Interest has expired but eDLAM regards it as a legitimate Interest incorrectly, in other words, eDLAM does not add its prefix to the MRT. There are two such cases. In the first case, the sum does not reach the threshold ($\sum_{k=1}^{k=n} Numk < r_{TH}$); accordingly, eDLAM does not add any prefixes to the MRT. The other case is that the sum reaches the threshold ($\sum_{k=1}^{k=n} Numk > r_{TH}$), but the malicious Interest prefix is not added to the MRT successfully. We obtain $P_2 = P_M \cdot (P(\mathbb{D}) + 1 - P_{MM})$ (where $\mathbb{D}$ denotes the event: $n_L e_r + n_M < r_{TH}$.).

Therefore, false total rate under eDLAM is given as follows:

$$P_e = P_1 + P_2 = \frac{n_L e_r}{n_L e_r + n_M} \cdot P(\mathbb{C}) + \frac{n_M}{n_L e_r + n_M} \cdot P(\mathbb{D}) \tag{10}$$

From the synthesis of Poisson process we can acknowledge that malicious and dropped legitimate Interest arrival process follow $Poisson((n_L e_r + n_M)t)$. Further, from the Poisson probability distribution shown in Fig. 4, we can denote our problem as the following equations:

$$\min\ P_e = \boldsymbol{\mathcal{A}} \cdot S_C + \boldsymbol{\mathcal{B}} \cdot S_D \tag{11}$$

subject to:

$$\begin{cases} \boldsymbol{\mathcal{A}} = n_L e_r/(n_L e_r + n_M) \\ \boldsymbol{\mathcal{B}} = n_M/(n_L e_r + n_M) \\ S_C = \sum_{k=r_{TH}}^{\infty} (n_L e_r + n_M)^k \cdot e^{-(n_L e_r + n_M)}/k! \\ S_D = \sum_{k=0}^{r_{TH}} (n_L e_r + n_M)^k \cdot e^{-(n_L e_r + n_M)}/k! \\ S_C + S_D = 1 \end{cases}$$

Solution: From the fundamental inequality we obtain,

$$P_e \geq 2\sqrt{\boldsymbol{\mathcal{A}} \cdot S_C + \boldsymbol{\mathcal{B}} \cdot S_D}$$

The equal sign holds if and only if $\boldsymbol{\mathcal{A}} \cdot S_C = \boldsymbol{\mathcal{B}} \cdot S_D$; thus,

$$\frac{\boldsymbol{\mathcal{A}}}{\boldsymbol{\mathcal{B}}} = \frac{S_D}{S_C} = \frac{n_L e_r}{n_M}$$

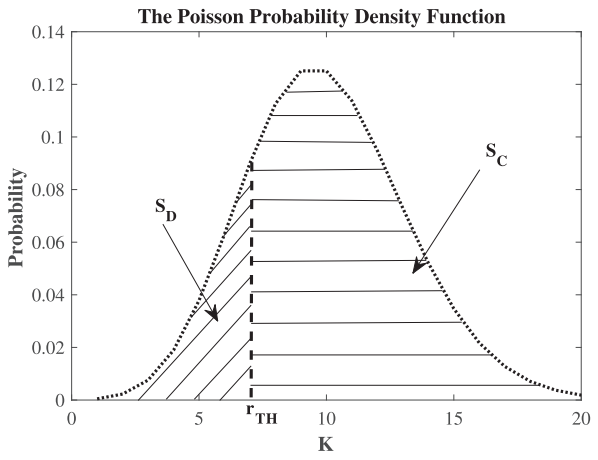


Fig. 4. Poisson probability density function.

Thus, if we select r_{TH} such that $S_D/S_C = n_L e_r/n_M$, P_e can achieve the minimum value. Finally, we obtain the following equation:

$$S_D = \frac{n_L e_r}{(n_L e_r + n_M)} \tag{12}$$

Further, we can solve the above equation by iteration, and obtain the value of r_{TH}. Subsequently, P_e can achieve the minimum value, i.e., the false total rate under eDLAM can be the lowest. It is worth mentioning that such a compute process is a little heavy to IoT nodes. Therefore, in this paper, we pre-compute the optimal threshold via other high-performance platforms and, program the fixed threshold into IoT nodes. To make eDLAM smarter, in our envisioned scenario, a smart control engine, equipped with abundant resources (*e.g.*, compute, storage and network), is integrated to collect the request rates information and compute the optimal threshold for the IoT nodes. Particularly, the engine is powered by the in-band network telemetry technology (Kim et al., 2015) to collect the request rates and other information of each IoT node. After that, the engine computes the optimal threshold and distributes it to each IoT nodes.

4. Performance evaluation

We implement eDLAM in NDN-Cxx and share the source code online (Liu et al., 2018b). In this section, we mainly evaluate the performance of eDLAM in terms of PIT-size, FNR, and FPR. The experiment is carried out under linear topology according to practical scenario. Furthermore, we simulate the performance in a realistic large-scale AT&T topology (Spring et al., 2004). NDNSIM is used to accomplish the simulation. Moreover, the experiments and simulation results are also applicable to other stateful forwarding paradigms.

4.1. Linear topology

4.1.1. Effectiveness

As shown in Fig. 5, there are seven nodes in linear topology (such a simple topology was also applied in other works (Mohaisen et al., 2015)). We modified NDN-Cxx to embed the eDLAM mechanism, and installed it in all the IoT nodes. The nodes include three content Consumers, three routers, and one content Provider. Further, the three content Consumers are legitimate user, attacker1, and attacker2. Note that the Producer can only respond to Interests with the prefix of "/dst/users/". The other experimental parameters are shown in Fig. 5.

First, we evaluate the performance of eDLAM in the case of *naming-related attacks*. We set the Interest rate at 250/s for attacker1 and attacker2 (greater than the detection threshold). Both issue malicious Interests at the 30th second till the 60th second. However, to compare performance of eDLAM with rate-limit-based (Dai et al., 2013) and disabling PIT exhaustion (DPE) (Wang et al., 2013) mechanisms, we implement a simple but reasonable rate-limit and DPE algorithm in our experiments, where the threshold is set the same as eDLAM (200/s). Fig. 6 shows the experimental results.

Fig. 6(a) shows the PIT-size of each IoT node in the absence of any defense mechanism, and Fig. 6(b) shows the PIT-size of each IoT node in DPE, rate-limit, and eDLAM mechanisms. In the figure, we can observe malicious Interests issued at the 30th second, resulting in a sharp increase in PIT-size for all the IoT nodes. Because all the Interests follow Zipf-Mandelbrot distribution (Yu et al., 2015), the PIT-size of each IoT node is approximately 900, which is smaller than expected. Particularly, the PIT-entries of some Interests already exist in PIT, and they will not be added to the PIT; only their arrival interface is added to the PIT. *DPE, rate-limit, and eDLAM mechanism can effectively detect naming-related attacks and recover from the attacks, thus mitigating PIT memory pressure.*

In order to evaluate the scene envisioned by *distributed low-rate naming-related attacks* (the Interest rate under each prefix is lower than the detection threshold), we set the Interest rate to 150/s and 100/s

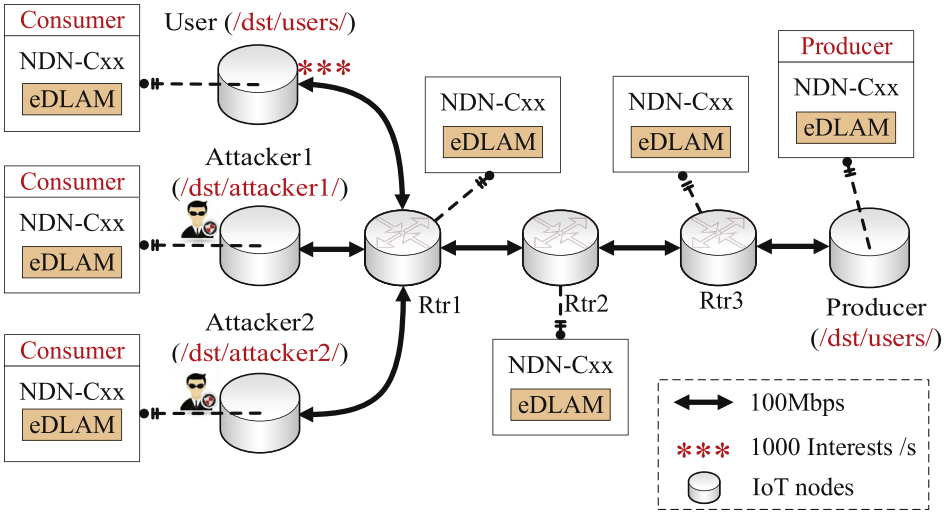
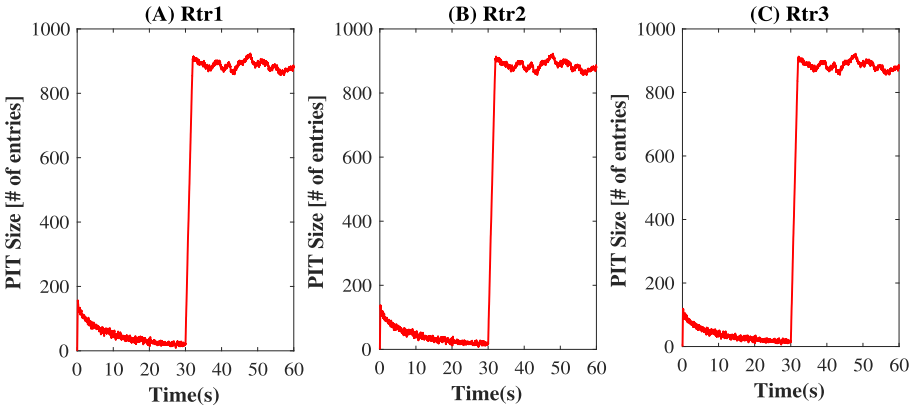
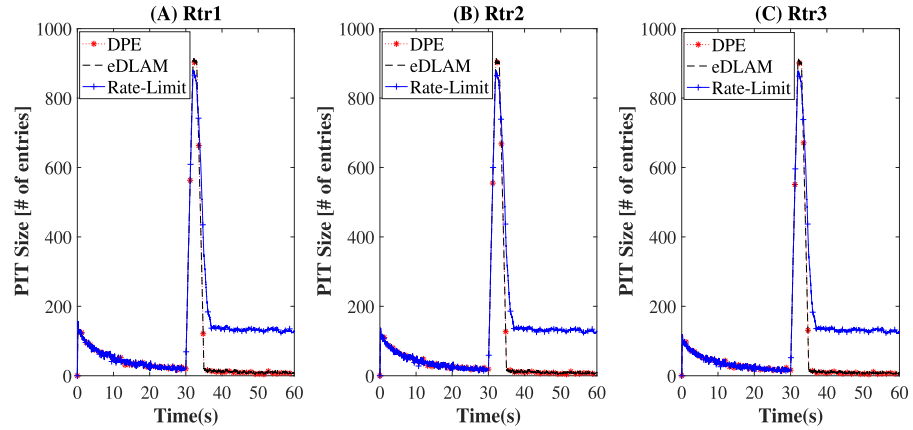


Fig. 5. Linear topology.



(a) Routers Without Any Defence Mechanisms



(b) Various Mechanisms (Attacker's Rate: 250/s)

Fig. 6. PIT Size under naming-related attacks.

for the attackers. As evident from Fig. 7, when the attacks occur, DPE mechanism cannot detect the attacks effectively, making the PIT-size very large. However, eDLAM can still detect effectively, thus avoiding PIT memory pressure becoming too large. Since the rate-limit mechanism detects attacks according to the PIT-size, but not the expired PIT-size, the mechanism can also detect attacks successfully. However, the final PIT-size is larger than eDLAM, and is usually half of the threshold. Particularly, when there are too many legitimate PIT-entries owing to packet loss rate, the rate-limit mechanism will unfortunately result in mistakes, and the following subsection will describe them in detail. *The eDLAM is effective to detect distributed low-rate naming-related attacks whereas the other mechanisms are ineffective at dealing with the attacks*.

4.1.2. Accuracy

In order to compare the performance of eDLAM, DPE, and rate-limit more intuitively, we evaluate the three mechanisms in terms of FPR (denoted as p_1) and FNR (denoted as p_2). Such two parameters are relevant to the utility of IoT node, and it can be denoted as follows (Based on Eq. (3)).

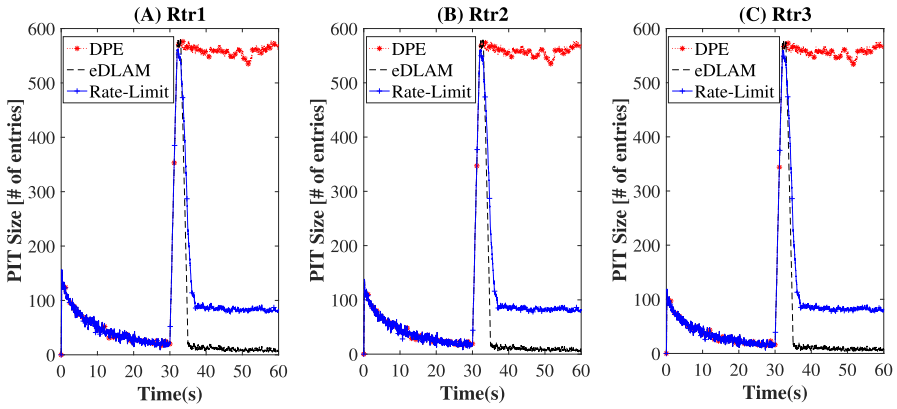
$$\mu_R = \sum(1-p_1)\Psi(r_A) + (1-p_2)\Phi(r_A) \tag{13}$$

On the one hand, the lower p_1 is, the greater μ_R is. On the other hand, the lower p_2 is, the greater μ_R is. It is evident that FPR and FNR are relevant to the utility of IoT node, therefore, we evaluate the three mechanisms in terms of the two parameters.

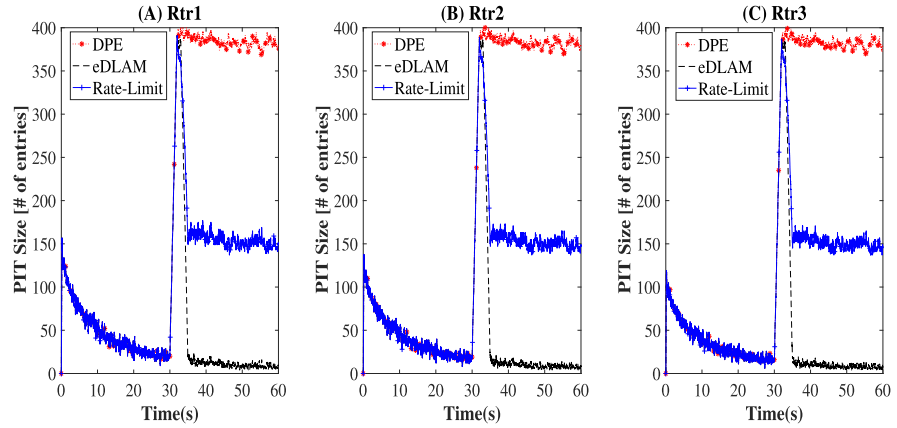
Most of the experimental parameters are the same as those in Fig. 5. Further, the malicious Interest rate is randomly selected between 50 per second and 350 per second, updated every 5 s, and the experimental time is set to 500 s. The experimental results are shown in Figs. 8–10. Note that 'e' refers to the packet loss rate.

From Fig. 8, we can observe that, at the beginning of the experiment (before approximately 100 s), in case of eDLAM and other mechanisms, the data line fluctuates significantly owing to fewer experimental samples at the beginning. When the time exceeds 300 s, the experimental results tend to become stable. The three solid lines represent the performance of DPE for three different packet loss rates. These lines are coincident because DPE detects the attacks according to the expired PIT-entry number under each prefix. Therefore, owing to packet loss, legitimate Interests may be unsatisfied. However, this does not affect the judgment. The three dotted lines represent the performance of eDLAM for three different packet loss rates, and these lines are not coincident because eDLAM detects the attacks according to the expired PIT-entry numbers under all the prefixes. Therefore, when legitimate Interests are unsatisfied owing to packet loss, it confuses the IoT nodes when judging attacks. As evident from the figure, *compared with the DPE mechanism, eDLAM mechanism enables the FNR to decrease from approximately 52% to 22%*.

Further, the three dashed lines represent the performance of rate-limit mechanism for three different packet loss rates. These lines are different from each other, and the FNR is approximately 9% less than that of eDLAM because the attacks are detected according to PIT-size, but not the expired PIT-size. Particularly, at approximately the 430th second, eDLAM misjudges more attackers as the packet loss rate increases, whereas rate-limit demonstrates the inverse. As the packet loss rate increases, rate-limit can detect attacks easier by performing



(a) Various Mechanisms (Attacker's Rate: 150/s)



(b) Various Mechanisms (Attacker's Rate: 100/s)

Fig. 7. PIT Size under distributed low-rate naming-related attacks.

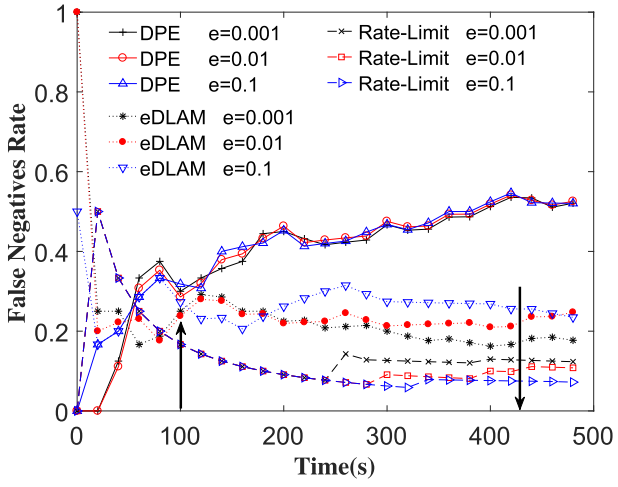


Fig. 8. False negatives rate.

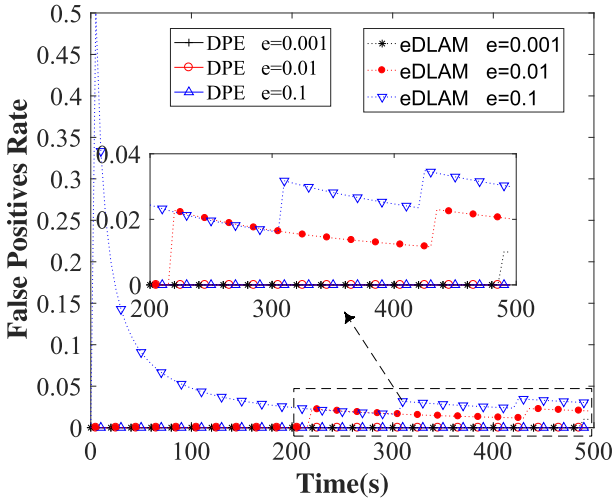


Fig. 9. False positives rate.

an extreme action: all the unsatisfied *Interests* are considered malicious, which introduces an undesirable side-effect described in the following subsection.

We can also observe that the data line fluctuates in Figs. 9 and 10 at the beginning of the experiment (before approximately 100 s), owing to fewer experimental samples at the beginning. DPE detects the attacks according to the expired PIT-entry number under each prefix, and the number of legitimate expired PIT-entries is small owing to the content storage of the IoT nodes. Therefore, there are no false positives in DPE from e = 0.001 to e = 0.1. As evident from Figs. 9 and 10, when the packet loss rate increases, the dotted lines also rise, i.e., *the FPR of eDLAM increases by 3.5%*. However, in Fig. 10, the three solid lines rise

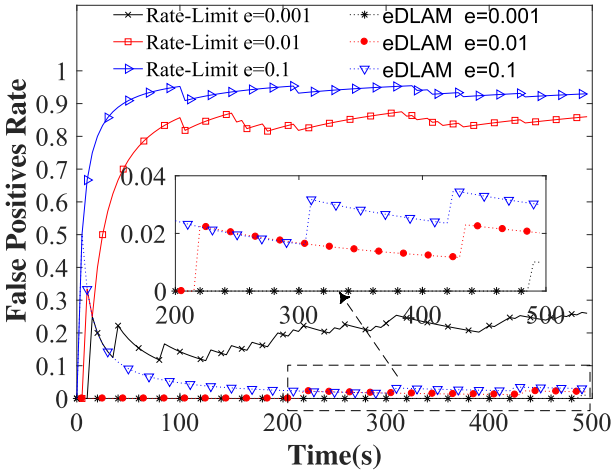


Fig. 10. False positives rate.

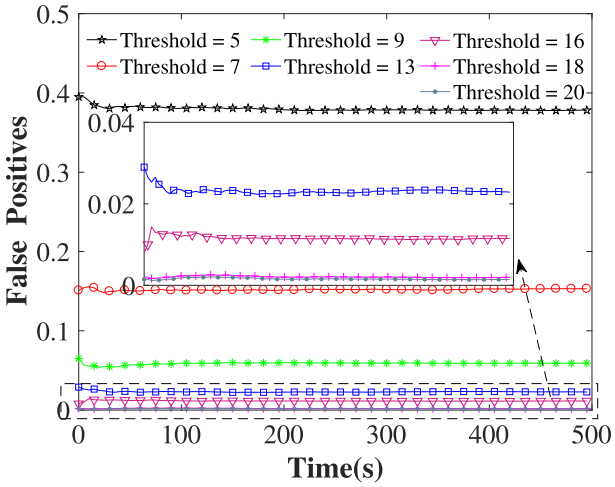


Fig. 12. False Positives Rate under different threshold.

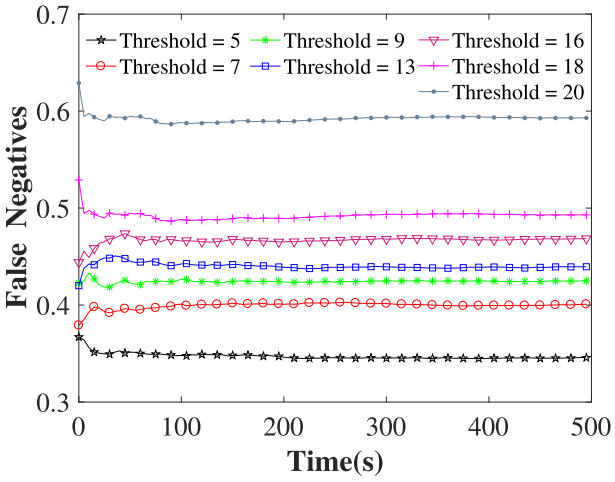


Fig. 11. False Negatives Rate under different threshold.

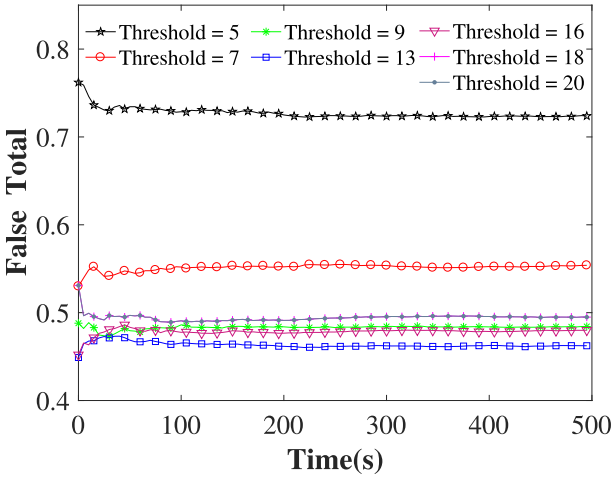


Fig. 13. False Total Rate under different threshold.

sharply because the rate-limit mechanism performs an extreme action and considers all the unsatisfied Interests as malicious. In other words, when a legitimate Interest is unsatisfied, rate-limit misjudges it as an attacker. It is an unreasonable method, and the FPR increases to approximately 95% when the packet loss rate is 0.1. In summary, compared with DPE and rate-limit mechanisms, the FNR of eDLAM can reduce by 10.5% on average, and the FPR can reduce by 44% on average. *The eDLAM is a reasonable and effective way to detect attacks accurately*.

4.1.3. Optimal threshold

We also evaluate the optimal threshold via experiments. Note that in these experiments, the rates are known in advance and the threshold is optimally set because we assume there is a powerful control engine. The engine collects the rates and other information via the in-band network telemetry technology, distinguishes the potential attackers through analyzing the rate feature, computes the optimal threshold and distributes it to IoT nodes. Currently, the malicious Interest rate is randomly selected between 0/s and 20/s (mean value is 10/s), and the legitimate Interest rate is selected as 5/s. Particularly, in order to ensure that the expired legitimate PIT-entry number is constant, we set the packet loss rate at 100% between "Rtr2" and "Rtr3". In other words, there are five expired legitimate PIT-entries constantly. The experimental results under "Rtr1" are shown in Figs. 11–13.

We calculate the optimal threshold first. From Section 3, we have $n_L e_r = 5$, $n_M = 10$, and thus, from Eq. (12) we obtain $S_D = 1/3$. Subsequently, we must determine r_{TH} such that $S_D = 1/3$. We solve it by iteration, using a numerical computing environment (MATLAB). Finally, we achieve $r_{TH} = 13$ in MATLAB.

From Fig. 11, we select the threshold from 5 to 20. When the threshold rises, the line also rises, i.e., the FNR increases. This is because $P(r_A + r_L > r_{TH})$ decreases when the threshold rises; i.e., many malicious Interests have expired but the IoT nodes may not be aware of it. In Fig. 12, when the threshold rises, the lines fall, i.e., the FPR decreases because, when legitimate Interests expire, it is difficult to satisfy the threshold if it is too large. When the threshold is reached, the malicious Interest prefix is added to the MRT with a larger probability, whereas the legitimate Interest prefix is added with a smaller probability i.e., the FPR decreases. From Figs. 11 and 12, we cannot determine the optimal threshold; thus, we add the FNR and FPR, and the result is shown in Fig. 13. From the figure, we can observe that, when the threshold is set at 13, the sum of the FNR and FPR is the minimum, which is the same as the result obtained in the above calculation.

4.2. AT&T topology

In order to further investigate the performance of eDLAM, we simulate the performance under AT&T topology. AT&T topology is an actual,

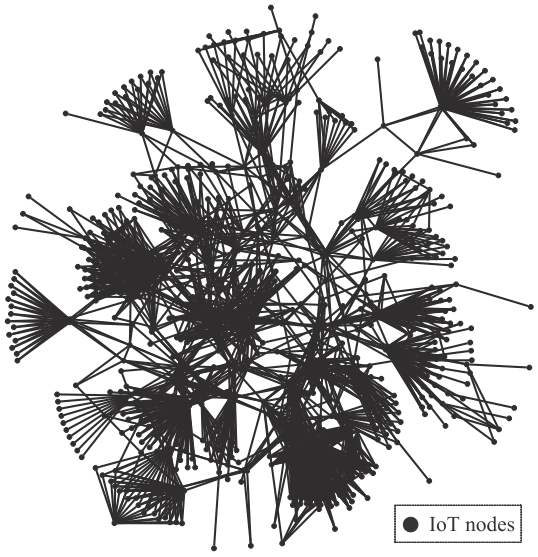


Fig. 14. AT&T topology.

Table 3
Simulation parameters in AT&T topology.

Parameters		Value
CS size		1000
Size of each content item		1 Kbytes
Forwarding strategy		Best Route
Rate of legitimate users		15/s
Duration for legitimate Interests		0–30 s
Detection Threshold		200/s
Backbone-Backbone	Delay	5 ms ~10 ms
	Bandwidth	40 Mbps ~100 Mbps
Gateway-Backbone	Delay	5 ms ~10 ms
	Bandwidth	10 Mbps ~20 Mbps
Gateway-Gateway	Delay	5 ms ~10 ms
	Bandwidth	10 Mbps ~20 Mbps
Client-Gateway	Delay	10 ms ~70 ms
	Bandwidth	1 Mbps ~3 Mbps

large-scale topology, and Fig. 14 shows the topology used in our simulation. There are 625 IoT nodes in the topology based on different degrees. We separate the IoT nodes into three categories: clients, gateways, and backbones. Among them, the nodes with a degree less than four are called the client (a total of 296 such nodes, expressed as "leaf-n"), the nodes directly connected to the client are classified as the gateway (a total of 221 such nodes, expressed as "gw-n"), and the remaining nodes are called backbone nodes (a total of 108 such nodes, expressed as "bb-n").

We randomly select 50 IoT nodes as attackers, and the remaining 246 IoT nodes are used as legitimate users in the simulations i.e., the number of malicious nodes is approximately 20%. All the legitimate Interests have the prefix of "/dst/users/", whereas all the malicious nodes are divided into two groups randomly. In which one group issues the malicious Interests with the prefix of "/dst/attacker1/" and the other issues malicious Interests with the prefix of "/dst/attacker2/". Moreover, we select the node "gw-12931" as the observation node, because it is connected to two types of attackers and a legitimate user in the simulation. We also randomly select a gateway node as a content Provider ("gw-1263" in the simulation), and the other simulation parameters are set as shown in Table 3.

Similar to the experiments in linear topology, we simulate *naming-related attacks* first. Accordingly, we set the malicious Interest rate at 250/s for all the attackers (greater than the detection threshold). The simulation results are shown in Fig. 15. At the beginning of the simulation, the PIT-size of "gw-12931" is very small, because the IoT node is connected to only one user, which issues 15 legitimate Interests per second. We can also observe from the figure that the attacks are launched at the 20th second, and DPE, rate-limit, and eDLAM can effectively detect and recover from the attacks, thus avoiding the IoT node being continuously under attack.

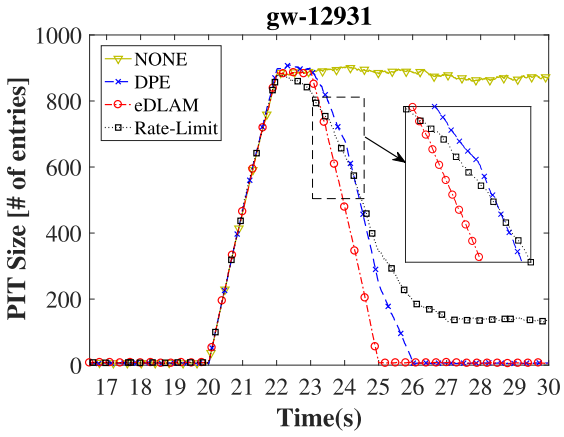


Fig. 15. PIT Size under naming-related attacks.

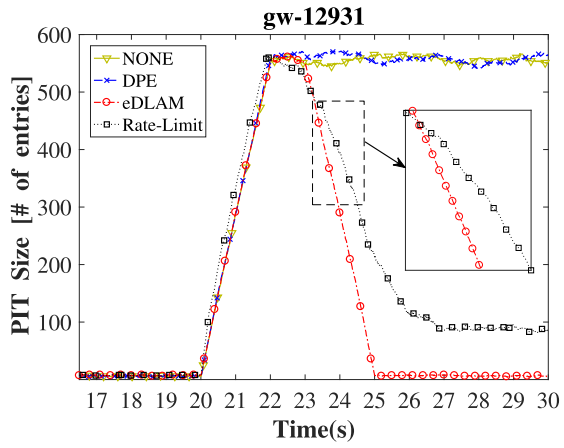


Fig. 16. PIT Size under distributed low-rate naming-related attacks.

Moreover, in order to simulate *distributed low-rate naming-related attacks*, we set the Interest rate to 150 per second for all the attackers, and the simulation results are shown in Fig. 16. When the attacks are launched, DPE is ineffective for detecting the attacks, and the attackers use too many PIT memory resources. However, eDLAM can significantly detect and recover from these attacks, thus avoiding PIT memory pressure becoming too large. Although rate-limit can also detect and recover from the attacks, the PIT-size is still large at approximately 100 PIT-entries owing to its own extreme action, which we described in subsection (1). Particularly, from Figs. 15 and 16, we can observe that *eDLAM decreases more sharply than DPE and rate-limit,* i.e., eDLAM has less latency in detecting and recovering from the attacks. It is important for some IoT nodes to be aware of attacks quickly, particularly the IoT nodes closed to the Producer.

5. Related works

Early works on naming-related attacks mostly focus on the typical characteristics. The authors in (Gasti et al., 2013) discussed the principle of naming-related attacks in detail, and classified the attacks into three categories. In particular, Interests can be used to request: (i) existing,

(ii) dynamically generated, or (iii) non-existent Data. NDN routers provide a built-in mitigation for type (i) owing to their caches. The attack in type (ii) aims at exhausting the resources of origin Data providers by serving malicious Interests. However, once the malicious Interest obtains a response, the impact of this type of attack is significantly diminished. In type (iii), excessive number of spoofed Interest requests does not exist Data, this type of attack has the most significant impact. However, the authors in (Gasti et al., 2013) did not provide an effective countermeasure to mitigate naming-related attacks.

Recent works on naming-related attacks mostly focus on mitigating the attacks, thus avoiding long-term occupation of memory resources. Wang et al. proposed a mechanism based on threshold detection to mitigate the attacks in (Wang et al., 2014). The works in (Afanasyev et al., 2013) extended the function of PIT, and designed three mechanisms to ease the attacks: token bucket with per interface fairness, satisfaction-based Interest acceptance, and satisfaction-based push-back. Although these countermeasures can mitigate the attacks, it is difficult to implement them. The authors in (Dai et al., 2013) proposed a mechanism for tracking Interests to deal with the attacks, by generating a spoof Data to respond to malicious Interests, but the mechanism is still based on the interface rate to detect the attacks. In (Wang et al., 2013), Wang et al. proposed a mechanism called DPE to avoid the consumption of PIT memory resources by the attacks. This mechanism counts the number of expired PIT entries under each prefix. If a certain threshold is reached, it is judged that the prefix of this PIT entry is under attack. Recently, Wang et al. further proposed the a simple, direct, lightweight yet efficient IFA countermeasure method (InterestFence) to achieve accurate detection meanwhile efficient attack-traffic filtering without harming any legitimate Interests (Wang et al., 2018a). Irrespective of whether the attacks are detected by the interface rate or the expired entries reach a threshold, these mechanisms *do not consider distributed low-rate naming-related attacks*. In other words, *when the attacks occur, all the countermeasures mentioned above will be invalid*. Therefore, we designed the eDLAM mechanism, such that all the attacks can be effectively detected irrespective of whether they are naming-related attacks with a large-rate or a distributed low-rate.

Owing to various proposed countermeasures, currently, most of researches focus on the novelty to detect naming-related attacks accurately and mitigate them effectively. In (Salah et al., 2015), Salah et al. proposed a cooperation mechanism of resistance to attacks, and the authors identified the problem of distributed low-rate flooding attack first. Accordingly, the authors designed three components called DC, NR, and MR to coordinate the completion of the detection of attacks. Although the authors in (Salah et al., 2015) were aware of the possibility of distributed low-rate naming-related attacks, it is difficult to implement their mechanism and the accuracy remains to be verified. Our previous work (Liu et al., 2018a) considered to balance the detecting accuracy and delay, and proposed an mTBAD solution to minimize the detecting delay while guaranteeing the accuracy.

Moreover, the low-rate distributed state exhaustion attacks (such as naming-related attacks) not only existing in ICN, but also disturbing other stateful forwarding paradigms. We take SDN for example because it is widely adopted in various aspects (Quan et al., 2018b; Wang et al., 2018b). Particularly, Arashloo et al. proposed the stateful network-side abstractions for packet processing in SDN (Arashloo et al., 2016). Such a stateful SDN mechanism enables the switch keep the state information of the flows and perform packet level state transition, which is the same as recording packet arriving interfaces in ICN routers. Thus, an attacker may take advantage of the potentially large in-memory space that each switch requires in order to store flow state information, to exhaust the memory of the switch (Dargahi et al., 2017). In general, eDLAM is proposed to detect and mitigate the low-rate distributed state exhaustion attacks not only in ICN but also other stateful forwarding paradigms.

6. Summary and future work

In this paper, we establish an attacker and defender game through analyzing low-rate varietal DoS attacks based on game theory, and find that managing all the expired state-entries can make the defender obtain more utility. Therefore, we propose the eDLAM mechanism to mitigate the attacks and obtain max-utility. The eDLAM manages all expired state-entries. Particularly, eDLAM maintains a lightweight MRT to offload burden of forwarding state table. When a packet request is matched in MRT, it will be marked and forwarded without the help of forwarding state table. Moreover, eDLAM supports an optimal threshold to get maximum utility for the defender. We evaluated the performance of eDLAM in linear topology and actual large-scale topology according to practical scenario. Simulation results show that eDLAM can reduce by 10.5% and 44% on average in terms of FNR and FPR reduces respectively, compared to state-of-the-art measures.

In the future work, we will pay efforts to achieve less latency in attack awareness of IoT nodes. Since eDLAM detects an attack based on expired state-entry numbers, thus, less distance to producer indicates that larger size of forwarding state table is required. In this view, we will integrate traceback-like mechanism into eDLAM to further improve detection efficiency.

Acknowledgment

The authors would like to thank the anonymous reviewers to improve this paper.

Appendix A

Proof of the Proposition

Definition 1. We denote $\left(r_{A_1}, r_{A_2} > r_{TH}\right)$ as event $\mathbb{A}$. We note that the possible utility of the existing mechanism is:

$$\mu_{PEM} = \mu_{EM} \cdot P(\mathbb{A}) \tag{14}$$

We denote $\left(r_{A_1} + r_{A_2} > r_{TH}\right)$ as event $\mathbb{B}$. We note that the possible utility of the potential mechanism is:

$$\mu_{PPM} = \mu_{PM} \cdot P(\mathbb{B}) \tag{15}$$

Since $\mu_{EM} = \mu_{PM}$, if we compare the results of $P(\mathbb{A})$ and $P(\mathbb{B})$, then as well as and μ_{PEM} and μ_{PPM}.
We note that event $\mathbb{A}$ and event $\mathbb{B}$ satisfy the relationship: $\mathbb{A} \subset \mathbb{B}$. Hence,

$$\mathbb{B} = \mathbb{A} \cup (\mathbb{B} - \mathbb{A}) \ \ and \ \ \mathbb{A}(\mathbb{B} - \mathbb{A}) = \emptyset \tag{16}$$

Therefore,

$$P(\mathbb{B}) = P(\mathbb{A} \cup (\mathbb{B} - \mathbb{A})) = P(\mathbb{A}) + P(\mathbb{B} - \mathbb{A}) \tag{17}$$

In other words, $P(\mathbb{B}) - P(\mathbb{A}) = P(\mathbb{B} - \mathbb{A})$. From the non-negative nature of probability, we can obtain $P(\mathbb{B} - \mathbb{A}) \geq 0$. Hence, $P(\mathbb{B}) - P(\mathbb{A}) = P(\mathbb{B} - \mathbb{A}) \geq 0$. Thus,

$$P(\mathbb{B}) \geq P(\mathbb{A}) \tag{18}$$

Since $\mu_{EM} = \mu_{PM}$, we obtain $\mu_{PM} \cdot P(\mathbb{B}) \geq \mu_{EM} \cdot P(\mathbb{A})$. Finally,

$$\mu_{PPM} \geq \mu_{PEM} \tag{19}$$

References

AbdAllah, E.G., Hassanein, H.S., Zulkernine, M., 2015. A survey of security attacks in information-centric networking. IEEE Commun. Surv. Tutorials 17 (3), 1441–1454.

Abdullahi, I., Arif, S., Hassan, S., 2015. Survey on caching approaches in information centric networking. J. Netw. Comput. Appl. 56, 48–59.

Afanasyev, A., Mahadevan, P., Moiseenko, I., Uzun, E., Zhang, L., 2013. Interest flooding attack and countermeasures in named data networking. In: IFIP Networking Conference, 2013. IEEE, pp. 1–9.

Amadeo, M., Campolo, C., Quevedo, J., Corujo, D., Molinaro, A., Iera, A., Aguiar, R.L., Vasilakos, A.V., Mar. 2016. Information-centric networking for the internet of things: challenges and opportunities. IEEE Netw. 30 (2), 92–100.

Arashloo, M.T., Koral, Y., Greenberg, M., Rexford, J., Walker, D., 2016. Snap: stateful network-wide abstractions for packet processing. ACM SIGCOMM 29–43.

Bizanis, N., Kuipers, F.A., 2016. Sdn and virtualization solutions for the internet of things: a survey. IEEE Access 4, 5591–5606.

Cheng, N., Lyu, F., Chen, J., Xu, W., Zhou, H., Zhang, S., Shen, X., 2018. Big data driven vehicular networks. IEEE Netw. 32 (6), 160–167.

Cisco, 2017. Cisco Annual Cybersecurity Report. Tech. Rep. Available: https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecuri\ignorespacesty-report-2017.html.

Dai, H., et al., 2013. Mitigate ddos attacks in ndn by interest traceback. In: INFOCOM Workshops, pp. 381–386.

Dargahi, T., et al., 2017. A survey on the security of stateful sdn data planes. IEEE Commun. Surv. Tutorials 19 (3), 1701–1725.

Farinacci, D., Lewis, D., Meyer, D., Fuller, V., 2013. The Locator/id Separation Protocol (Lisp). IETF RFC 6830.

Gasti, P., Tsudik, G., Uzun, E., Zhang, L., 2013. Dos and Ddos in Named Data Networking. *ICCCN*, pp. 1–7.

Harris III, A.F.., Khanna, V., Tuncay, G., Want, R., Kravets, R., Dec. 2016. Bluetooth low energy in dense iot environments. IEEE Commun. Mag. 54 (12), 30–36.

Khan, M.A., Salah, K., 2018. Iot security: review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 82, 395–411.

Kim, C., Sivaraman, A., Katta, N., Bas, A., Dixit, A., Wobker, L.J., 2015. In-band Network Telemetry via Programmable Dataplanes. *ACM SIGCOMM*.

Li, Q., et al., 2015. Live: lightweight integrity verification and content access control for named data networking. IEEE Trans. Inf. Forensics Secur. 10 (2), 308–320.

Liu, G., Quan, W., Cheng, N., Wang, K., Zhang, H., 2018a. Accuracy or delay? a game in detecting interest flooding attacks. Internet Technol. Lett. 1 (2), e31.

Liu, G., et al., 2018b. The Edlam Mechanism Source Code. https://github.com/KB00100100/paper/tree/master/eDLAM.

Luo, H., et al., 2013. Preventing ddos attacks by identifier/locator separation. IEEE Netw. 27 (6), 60–65.

Mastorakis, S., Afanasyev, A., Zhang, L., Jul. 2017. On the evolution of ndnSIM: an open-source simulator for NDN experimentation. ACM Comput. Commun. Rev. 47 (3), 19–33.

Mick, T., Tourani, R., Misra, S., Apr. 2018. Laser: lightweight authentication and secured routing for ndn iot in smart cities. IEEE Internet Things J. 5 (2), 755–764.

Mohaisen, A., et al., Nov. 2015. Timing attacks on access privacy in information centric networks and countermeasures. IEEE Trans. Dependable Secure Comput. 12 (6), 675–687.

Muralidharan, S., Sahu, B.J.R., Saxena, N., Roy, A., Jun. 2017. Ppt: a push pull traffic algorithm to improve qos provisioning in iot-ndn environment. IEEE Commun. Lett. 21 (6), 1417–1420.

Muralidharan, S., Roy, A., Saxena, N., Feb. 2018. Mdp-based model for interest scheduling in iot-ndn environment. IEEE Commun. Lett. 22 (2), 232–235.

Ndih, E.D.N., Cherkaoui, S., 2016. On enhancing technology coexistence in the iot era: Zigbee and 802.11 case. IEEE Access 4, 1835–1844.

Ni, J., Lin, X., Shen, X.S., Mar. 2018. Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot. IEEE J. Sel. Area. Commun. 36 (3), 644–657.

Parsons, G., Jul. 2016. The internet of things [edit note]. IEEE Commun. Mag. 54 (7), 2–3.

Pokhrel, S.R., Williamson, C., 2018. Modeling compound tcp over wifi for iot. IEEE/ACM Trans. Netw. (99), 1–15 vol. PP.

Qin, Y., Sheng, Q.Z., Falkner, N.J., Dustdar, S., Wang, H., Vasilakos, A.V., 2016. When things matter: a survey on data-centric internet of things. J. Netw. Comput. Appl. 64, 137–153.

Quan, W., Xu, C., Guan, J., Zhang, H., Grieco, L., January 2014. Scalable name lookup with adaptive prefix bloom filter for named data networking. IEEE Commun. Lett. 18 (1), 102–105.

Quan, W., Liu, Y., Zhang, H., Yu, S., 2017. Enhancing crowd collaborations for software defined vehicular networks. IEEE Commun. Mag. 55 (8), 80–86.

Quan, W., Wang, K., Liu, Y., Cheng, N., Zhang, H., Shen, X.S., 2018a. Software-defined collaborative offloading for heterogeneous vehicular networks. Wireless Commun. Mobile Comput. 2018, 1–9.

Quan, W., Cheng, N., Qin, M., Zhang, H., Chan, H.A., Shen, X., 2018b. Adaptive transmission control for software defined vehicular networks. IEEE Wireless Commun. Lett. 1–1 (Early Access).

Salah, H., et al., 2015. Coordination supports security: a new defence mechanism against interest flooding in ndn. In: Local Computer Networks (LCN), 2015 IEEE 40th Conference on, pp. 73–81.

Saucez, D., Iannone, L., Bonaventure, O., 2016. Locator/id Separation Protocol (Lisp) Threat Analysis. IETF RFC 7835.

Saxena, D., Raychoudhury, V., 2017. Design and verification of an ndn-based safety-critical application: a case study with smart healthcare. IEEE Trans. Syst., Man, Cybern. Syst. (99), 1–15 vol. PP.

Sharma, P.K., Jeong, Y.S., Park, J.H., 2018. Eh-hl: effective communication model by integrated eh-wsn and hybrid lifi/wifi for iot. IEEE Internet Things J. (99) vol. PP, pp. 1–1.

Spring, N., et al., 2004. Measuring isp topologies with rocket fuel. IEEE/ACM Trans. Netw. 12 (1), 2–16.

Van, J., et al., 2014. Named data networking. Comput. Commun. Rev. 44 (3), 66–73.

Wählisch, M., et al., 2013. "Backscatter from the data plane–threats to stability and security in information-centric network infrastructure. Comput. Network. 57 (16), 3192–3206.

Wang, K., Dong, J., Quan, W., Yu, S., 2018. Interestfence: a simple but efficient way to counter interest flooding attacks. J. Netw. Comput. Appl. 1–8.

Wang, K., Yin, H., Quan, W., Min, G., September 2018. Enabling collaborative edge computing for software defined vehicular networks. IEEE Netw. 32 (5), 112–117.

Wang, K., et al., 2013. Decoupling malicious interests from pending interest table to mitigate interest flooding attacks. In: Globecom Workshops. IEEE, pp. 963–968.

Wang, K., et al., 2014. Modeling denial-of-service against pending interest table in named data networking. Int. J. Commun. Syst. 27 (12), 4355–4368.

Yan, Q., Yu, F.R., Gong, Q., Li, J., 2016. Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: a survey, some research issues, and challenges. IEEE Commun. Surv. Tutorials 18 (1), 602–622.

Yi, C., et al., 2013. A case for stateful forwarding plane. Comput. Commun. 36 (7), 779–791.

Yu, S., Zhou, W., Doss, R., Jia, W., March 2011. Traceback of ddos attacks using entropy variations. IEEE Trans. Parallel Distr. Syst. 22 (3), 412–425.

Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y., Tang, F., June 2012. Discriminating ddos attacks from flash crowds using flow correlation coefficient. IEEE Trans. Parallel Distr. Syst. 23 (6), 1073–1080.

Yu, S., Gu, G., Barnawi, A., Guo, S., Stojmenovic, I., Jan. 2015. Malware propagation in large-scale networks. IEEE Trans. Knowl. Data Eng. 27 (1), 170–179.

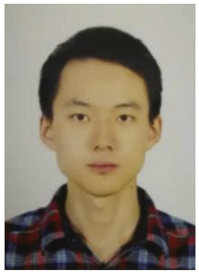
Yu, S., Zhou, W., Guo, S., Guo, M., May. 2016. A feasible ip traceback framework through dynamic deterministic packet marking. IEEE Trans. Comput. 65 (5), 1418–1427.

Zargar, S.T., et al., 2013. A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks. IEEE Commun. Surv. Tutorials 15 (4), 2046–2069.

Zhang, K., Liang, X., Lu, R., Shen, X., Oct. 2014. Sybil attacks and their defenses in the internet of things. IEEE Internet Things J. 1 (5), 372–383.

Zhang, H., et al., 2016. Smart identifier network: a collaborative architecture for the future internet. IEEE Netw. 30 (3), 46–51.

Zhi, T., Luo, H., Liu, Y., March 2018. A gini impurity-based interest flooding attack defence mechanism in ndn. IEEE Commun. Lett. 22 (3), 538–541.

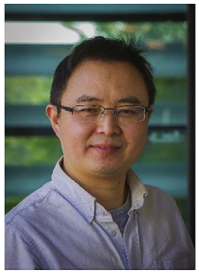


Gang Liu was born in Wuhu City, Anhui, China, in March 1993. He is currently working toward the Ph.D. degree at National Engineering Lab for Next Generation Internet Technologies (NGIT), Beijing Jiaotong University (BJTU), Beijing, China. He is a Student Member of IEEE, ACM. His current research interests include Information Centric Networking (ICN), Software Defined Networking (SDN), and Network Function Virtualisation (NFV).

Wei Quan (M′14) received his Ph.D degree in Communication and Information System from Beijing University of Posts and Telecommunications (BUPT), Beijing, China in 2014. During 2014–2016, During 2014–2016, he is a Postdoctoral Fellow at National Engineering Lab for Next Generation Internet Technologies (NGIT), Beijing Jiaotong University (BJTU), Beijing, China. He currently is an Associate Professor at School of Electronic and Information Engineering, BJTU. He has published more than 20 papers in prestigious international journals and conferences including IEEE Wireless Communications Magazine, IEEE Network Magazine, IEEE Communications Letters, IFIP Networking, IEEE WCNC etc. and serves as technical reviewers for some important international journals and conferences. His research interests include key technologies for network analytics, innovative Internet, space-air-ground networking, and vehicular communications. He is a Member of IEEE, ACM, and a Senior Member of CAAI (Chinese Association of Artificial Intelligence).

Nan Cheng (S′12,M′16) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, and B.E. degree and the M.S. degree from the Department of Electronics and Information Engineering, Tongji University. He is currently working as a joint Postdoctoral fellow with the Department of Electrical and Computer Engineering, University of Toronto and the Department of Electrical and Computer Engineering, University of Waterloo. His research interests include performance analysis, MAC, opportunistic communication for vehicular networks, unmanned aerial vehicles, and cellular traffic offloading.

Hongke Zhang (M′13-SM′16) was born in Datong, Shanxi, China, in September 1957. He received his M.S. and Ph.D. degrees in electrical and communication systems from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1988 and 1992, respectively. From 1992 to 1994, he was a post-doctor at Beijing Jiaotong University (BJTU), Beijing, China. He is currently a professor at the School of Electronic and Information Engineering, Beijing Jiaotong University (BJTU), China and the director of a National Engineering Lab on Next Generation Internet Technologies, China. His research has resulted in many papers, books, patents, systems and equipment in the areas of communications and computer networks. He is the author of more than 10 books and the holder of more than 70 patents. He is the Chief Scientist of a National Basic Research Program of China (973 Program) and has also served on the editorial board of several international journals.



Shui Yu (M04-SM12) is currently a full Professor of School of Software, University of Technology Sydney, Australia. Dr Yu's research interest includes Security and Privacy, Networking, Big Data, and Mathematical Modelling. He has published two monographs and edited two books, more than 200 technical papers, including top journals and top conferences, such as IEEE TPDS, TC, TIFS, TMC, TKDE, TETC, ToN, and INFOCOM. Dr Yu initiated the research field of networking for big data in 2013. His h-index is 32. Dr Yu actively serves his research communities in various roles. He is currently serving the editorial boards of IEEE Communications Surveys and Tutorials, IEEE Communications Magazine, IEEE Internet of Things Journal, IEEE Communications Letters, IEEE Access, and IEEE Transactions on Computational Social Systems. He has served more than 70 international conferences as a member of organizing committee, such as publication chair for IEEE Globecom 2015, IEEE INFOCOM 2016 and 2017, TPC chair for IEEE BigDataService 2015, and general chair for ACSW 2017. He is a Senior Member of IEEE, a member of AAAS and ACM, the Vice Chair of Technical Committee on Big Data of IEEE Communication Society, and a Distinguished Lecturer of IEEE Communication Society.