IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received January 28, 2020, accepted February 11, 2020, date of publication February 24, 2020, date of current version March 3, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2976141

A Reputation Value-Based Early Detection Mechanism Against the Consumer-Provider Collusive Attack in Information-Centric IoT

TING ZHI[1], **YING LIU**[1], **AND JUN WU**[2]
[1]School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
[2]School of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: Ying Liu (yliu@bjtu.edu.cn)

This work was supported by the National Key Research and Development Program of China under Grant 2018YFA0701604.

ABSTRACT As the Internet of Things (IoT) has connected large number of devices to the Internet, it is urgently needed to guarantee the low latency, security, scalable content distribution of the IoT network. The benefits of Information-Centric Networking (ICN) in terms of fast and efficient data delivery and improved reliability have raised ICN as a highly promising networking model for IoT environments. However, with the widely spread of the viruses and the explosion of kinds of network devices, the attackers can easily control the devices to form a botnet such as the Mirai. Once the devices are under control, the attackers can launch a consumer-provider collusive attack in the Information-Centric IoT context. In this attack, the malicious clients issue Interest packets that can only be satisfied by the malicious content provider, and the malicious provider replies to the clients just before exceeding the Pending Interest Table entry's expiration time, to occupy the limited resources. In this paper, we expound the model of the consumer-provider collusive attack and analyze the negative effect of the attack. Then we propose a Reputation Value based Early Detection (RVED) mechanism to relieve the impact of the collusive attack. The method aims to adjust the packet dropping rates of different interfaces based on their reputation value, thus to protect the legitimate packets from being dropped as possible. We implement the consumer-provider collusive model and evaluate our defend mechanism in the simulator, and simulation results verify the feasibility and effectiveness against the collusive attack of the RVED mechanism.

INDEX TERMS Information-centric networking, Internet of Things, collusive attack, reputation value, early detection.

I. INTRODUCTION

With the explosive development of the information technology, Internet of Things (IoT) [1] has attracted extensive attention. IoT aims to connect kinds of devices to the Internet so that these devices can connect to networks at any time, any place, and any path. Common used IoT application scenarios include smart city [2], connected building [3], connected industry [4], connected car [5], connected health [6] and smart energy [7] and so on. According to the prediction from GSMA Intelligence, the globally total number of IoT connections will reach 25.2 billion in 2025, up from 6.3 billion in 2017 [8]. These connections will be widely used in areas of public services and facilities, traffic, manufacturing industry, healthcare, agriculture and financial industry, which will bring great changes and convenience to human life. However, as billions of IoT devices are connected to the Internet, the production, processing and transmission of large amounts of generated data will bring great challenges to the traditional network architecture. In addition, with the development and implementation of 5G network [9], large scale mobile devices are brought into networks, which also brings great and urgent challenges to the Internet Service Providers (ISPs) and users.

Traditional network architecture holds the host-to-host design principle, and all hosts in the network use IP addresses to represent their location information. This host-centric network architecture has exposed many serious problems to be solved in scalability, manageability, mobility and security. As a promising approach to accomplish the shortcomings

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

of current IP address based networking, Information-Centric Networking (ICN) [10], [11] is proposed. ICN architecture is based on naming the contents to avoid the shortage of address spaces, which acquires the requested contents by content names, caches the returned contents at intermediate nodes to provide efficient and reliable data delivery. To ensure the widespread adoption of IoT applications [12], low latency, security, mobility, and scalable content distribution support are required. The characteristics of ICN, such as efficient data delivery and promoted reliability have proposed that ICN can be used as a highly promising networking model for IoT environments [13]. So far, there have many researches around ICN-based IoT caching [14], [15], ICN-based IoT naming [16], [17], ICN-based IoT security [18]–[20] and ICN-based IoT mobility [21], [22] schemes. To solve the problem of the actual deployment of the Information-Centric IoT, there also exists some researches discussing the techniques that can act as a bridge between IP and ICN networks. For instance, Shannigrahi *et al.* [23] propose a protocol named IPoC that can enable a transition to ICN in mobile networks by encapsulating and forwarding IP traffic over an ICN core. IPoC allows existing applications to keep using IP until they are ready to transition into native use of ICN. And the authors point out that IPoC can benefit 5G mobile networks through simplifying handover operations and introducing intelligent multi-path strategies.

Since the architecture of Information-Centric IoT has been gradually coming true, the cybersecurity issues under this environment should be paid more indispensable attention. While large scale cyberattacks have become commonplace, little has been relatively accomplished for their network protection. A recently emerged example is the Mirai [24] botnet. The Mirai botnet is composed primarily of IoT devices, and took the Internet by storm in late 2016 with massive Distributed Denial-of-Service (DDoS) [25] attacks. Notably one in October 2016 against service provider Dyn that took down hundreds of websites-including Twitter, Etsy, Github, Vox, Spotify, Airbnb, Netflix and Reddit-for several hours. Researchers latter pointed out that the attack sources are mainly the IoT devices infected by the Mirai virus. As viruses such as Mirai have spawned many variants to infect the networks, IoT devices based botnets will be commonly used by attackers to launch DDoS attacks. Besides, with the public release of Mirai's source code, competing Mirai botnet variants have come into operation. Although Arshad *et al.* [13] has introduced that security and privacy in IoTs can be promoted through using ICN named contents, the cybersecurity of the Information-Centric IoT still needs necessary guarantees. Specifically, when the IoT devices are controlled by the attackers, they could be used to launch a consumer-provider collusive attack in the environment of Information-Centric IoT. Since the Interest packets are recorded in the pending interest table (PIT) of the intermediate routers, the attackers can send numerous Interest packets to occupy the PIT to exhaust the memory resources of key routers. In the consumer-provider collusive attack, malicious consumers send requests to malicious content providers, and the malicious content providers reply to the consumers only when the expiration of the requests is about to be exceeded. Under the circumstances, the network resources are occupied and wasted by the long-lived malicious requests, leading to that the legitimate requests cannot be satisfied properly or timely.

In this paper, to mitigate the consumer-provider collusive attack which can be launched easily by infected IoT devices, we propose a Reputation Value based Early Detection (RVED) mechanism to alleviate the effects of the attack and to protect the legitimate clients from being influenced. The main contributions are as follows:

- We present a detail implementation model of the consumer-provider collusive attack, by which the attackers can successfully obtain the expiration time of the PIT entries and then can launch the attack.
- We propose to compute the average PIT utilization rate and drop Interest packets when the value of the utilization rate exceeds the predefined threshold, to relieve the congestion of the network that brought by the collusive attack.
- We put forward to set different thresholds for different faces according to their reputation values and adaptively adjust the packet dropping rate of different faces, to avoid discarding of the legitimate Interest packets as possible.
- We conduct simulations to verify the proposed RVED mechanism. Simulation results indicate that the negative impact of the consumer-provider collusive attack can be eliminated significantly.

The rest of the paper is organized as follows. Section II introduces related work of the Information-Centric IoT and the content-provider collusive attack in ICN. Section III models the collusive attack. Section IV describes the defend mechanism RVED. Section V conducts the evaluation and analyzes the results. Section VI finally concludes the paper.

II. RELATED WORK

A. INFORMATION-CENTRIC IOT

As a promising network architecture, ICN has been deeply explored and implemented. With the advantages of content name-based routing, in-network caching, security property of self-certifying contents, ICN has been used in many network application domains, such as IoT, video streaming and download, web applications [26]. IoT can benefit from the in-network caching property of ICN. Kwak *et al.* [14] propose hybrid content caching algorithms for joint content caching control in the hierarchical cellular network architecture to reduce the average end-to-end latency. Meddeb *et al.* [15] propose a novel cache coherence mechanism to check the validity of cache contents and give a caching strategy in the M2M environment, which can help ensure validity of requested content while maintain system performances. In the Information-Centric IoT context, not only the contents and services but also the IoT devices can be named with the naming mechanisms of ICN, which can achieve conveniently name-based routing and devices management. Hong [16] point out that it is important in ICN for IoT because billions of data objects will be connected to IoT networks, and the authors also discuss challenges of the name resolution services for ICN toward IoT. Arshad *et al.* [17] propose a hybrid naming scheme that names contents using hierarchical and flat components to provide both scalability and security. As ICN uses various signature-based methods to provide data verification, the authenticity and reliability of the data transmitted in the Information-Centric IoT can be well guaranteed. For example, Li *et al.* [18] propose a scheme called DPD-ICIoT to enable secure and flexible access control for IoT data. The system evaluations the DPD-ICIoT can effectively reduce the bandwidth cost of attribute retrieval when compared to existing server-based scheme. Sicari *et al.* [19] analyze the current security functionalities in the context of Information-Centric IoT and point out that the service discovery, naming service and content delivery solutions should be integrated with security schemes to prevent any violation attempt. Mick *et al.* [20] propose and evaluate a novel framework for lightweight authentication and hierarchical routing in the Named Data Networking (NDN)-based IoT networks. And the framework is verified to be efficient for emerging large-scale IoT environments such as smart cities. Besides the research aspects of caching, naming and security in Information-Centric IoT, the mobility solutions are also widely discussed. Ullah *et al.* [21] point out that edge computing enables to deploy services on the edge of work and provides local computing and storage, while ICN supports decentralized caching and multicast natively. Therefore, a combination of ICN and edge computing is a promising way to solve the issue of latency and mobility for autonomous driving. An and Kim [22] propose an ICN-based light-weighted content delivery method in IoT, and evaluation results show that this method can achieve the mobility support without additional control packets. As mentioned above, the numerous research outputs have continuously verified the feasibility and practicability of the Information-Centric IoT solutions.

B. THE CONTENT-PROVIDER COLLUSIVE ATTACK

There are lots of researches focusing on the consumer-provider collusive attack in ICN. Salah and Strufe [27] propose to detect and mitigate the collusive attack based on aggregated and timely knowledge of local and global forwarding states. However, this method needs to introduce a center controller which may aggravate the burden of the NDN and the controller is also vulnerable. Signorello *et al.* [28] propose a more complete attack model in NDN and prove that the state-of-the-art countermeasures fail to detect and mitigate the attack properly. And the authors leave the attack defending solutions as a future work. Xin *et al.* [29] put forward to extract the signals in attack using wavelet analysis technique to recognize the attack traffic. However, this work does not specify how the attackers obtain the PIT expiration time exactly. Nasserala and Moraesy [30] point out that the purpose of the collusive attack is to increase the retrieval time of legitimate contents by decreasing the cache hit ratio of the legitimate requests in the intermediate routers, but the countermeasures are not given. The authors then promote a producer-consumer collusion attack countermeasure called Cache nFace [31], which divides the cache store of a router into sub caches for different interfaces. This method ensures that at least one sub cache works properly even when under an attack. However, it cannot fundamentally eliminate the attack. Umeda *et al.* [32] propose that the edge routers can detect the attackers by calculating the user reputation values and rate limit the non-existent malicious content name prefixes to defend against the attack. However, the router needs to know the whole network topology to confirm whether it is an edge router. Shinohara *et al.* [33] control the PIT entries through limiting the Interest information coming from the interfaces which have low reputation value and high PIT occupation rate, but the authors do not give a countermeasure against the collusive attack. Abu *et al.* [34] put forward to send an explicit congestion notification to the requester when the utilization of the PIT exceeds a certain threshold. However, this method does not distinct the usage of the malicious PIT entries and the legitimate ones. Nakatsuka *et al.* [35] propose an approach called FROG which uses the packet hop count value to distinguish the malicious users on the client-edge routers, but the situation when the attackers control both consumers and providers has not been discussed. Liu *et al.* [36] propose a lightweight bloom filter based attack mitigating mechanism in the context of Information-Centric IoT. However, this method is lack of discussion about the situation where the malicious Interest can be satisfied by the controlled malicious content provider. Moreover, in our previous work, we have proposed a gini impurity-based approach [37] and an improved entropy-svm based attack detection mechanism [38] to resist the non-cooperative Interest flooding attack in ICN, we are now moving forward to address the consumer-provider collusive attack.

III. MODEL OF THE CONSUMER-PROVIDER COLLUSIVE ATTACK

As presented by Salah and Strufe [27] and Signorello *et al.* [28], attackers can attack the network by a botnet of collusive consumers and providers. More precisely, malicious clients issue a large number of unique requests that can be satisfied only by the malicious server, resulting in one PIT entry per Interest packet in each router on the path. Then, the malicious server answers with Data packets just before the corresponding PIT entries expire, which delays the delivery of the corresponding Data packets at maximum. However, these previous work have not explained how attackers can obtain the entries expiration information. Therefore, in this section, we describe a consumer-provider collusive attack model in detail, analyze how the attackers obtain the PIT expiration time and demonstrate the procedure and impact of

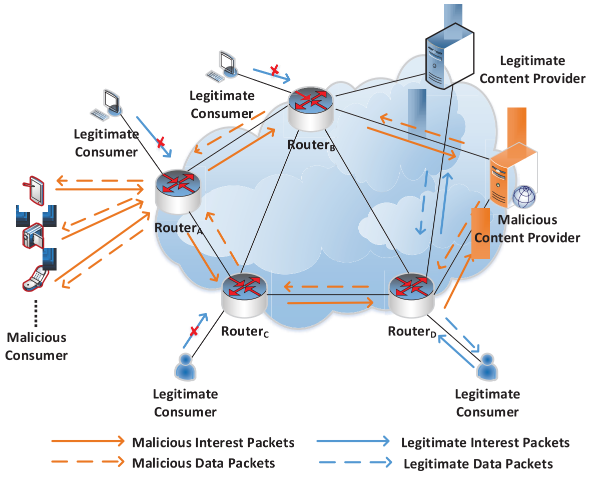


FIGURE 1. Example of the consumer-provider collusive attack scenario.

the attack. Figure 1 shows an example of the consumer-provider collusive attack in Information-Centric IoT.

Firstly, in the attack preparation phase, attackers control numbers of computers or devices through infecting viruses such as the Miria, and let the controlled clients send out Interest packets towards to the malicious content provider to obtain the PIT expiration time. Then, in the attack execution phase, the malicious clients issue massively malicious Interest packets that can only be satisfied by the malicious content provider, leading to one PIT entry for each request. The malicious content provider holds the requests and then replies the Interest packets almost near the expiration of corresponding PIT entries. As a result, the PIT entries of the malicious requests will occupy the PIT space for a long time and they will be released only when the expiring time is almost exceeded, leading to the legitimate Interests being discarded and the performance of the network decreasing. Besides, through requesting massively malicious Interest packets and receiving corresponding Data packets, the Content Store (CS) of the intermediate routers will also be occupied by the caches of the malicious contents. Since the CS will update and replace the caching contents when the cache space is full, the caches of the legitimate contents may be replaced by the malicious contents, causing the cache hit ratio of the legitimate Interests decreasing and the legitimate contents retrieval delay increasing.

To keep the PIT being occupied as long as possible, the attackers need to know the expiration time of the PIT entries. After obtaining the expiration time, the attackers can make the malicious content provider reply the malicious Interest packets when the PIT entries are near to be expired. Here we discuss how to infer the PIT expiration time from the view of attackers. As shown in Figure 2, the attacker first specifies an initial time interval Δt_1 as the supposed PIT expiration time. When the malicious content provider receives $Interest_1$ sent by the malicious client at time $t_{Interest_1}$, it holds the request for a while and reply it with $Data_1$ just before time $t_{Interest_1} + \Delta t_1$. If the malicious client receives the $Data_1$, it indicates that Δt_1 is less than the actual PIT expiration time of the network $t_{expired}$. Once the malicious client receives Δt_1, it will send $Interest_2$ immediately. At the same time, the malicious content provider will increase Δt_1 by $1s$, which is denoted as Δt_2. If the malicious client receives $Data_2$, it continues to send out $Interest_3$, and malicious content provider increase $Data_2$ by $1s$, denoted as Δt_3. After several rounds of the above steps, the malicious client sends out$Interest_n$ and the malicious content provider replies with $Data_n$ at time $t_{Interest_n} + \Delta t_n$. If the malicious client cannot receive $Data_{n+1}$ in the next iteration period, resulting in the malicious content provider cannot receive the next Interest packet, the provider deduces that t_{n+1} has exceeded the actual PIT expiration time. Consequently, t_n is regarded as the estimated PIT expiration time, and it will be used as the reply delay of the malicious content provider when the attack begins. In the first iteration phase, if the malicious client does not receive $Data_1$, it indicates that t_1 is larger than the actual PIT expiration time of the network. In this case, the provider reduces the time interval by half until the malicious client starts receiving the data packet, and then repeats the steps shown in Figure 2 to find out the PIT expiration time. The PIT expiration time analyzing algorithm is given in Algorithm 1.

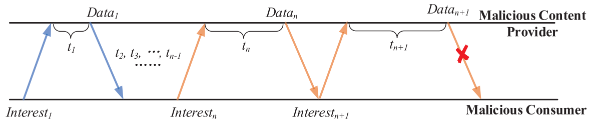


FIGURE 2. PIT expiration time analyzing model.

In general, the consumer-provider collusive attack has these features: 1) As the malicious Interest packets and malicious Data packets are similar to the legitimate ones, and they are forwarded by NDN nodes in normal ways, it is hard to detect the attack when only use traditional statistics information of Interest packets based methods. 2) Since the attackers want to occupy more PIT spaces on the paths between the malicious clients and the malicious content provider, the malicious clients will generate requests for different contents each time, to ensure that the malicious Interest packets can reach the malicious content provider and the malicious information is stored in every intermediate routers. 3) With the explosive developments of the IoT devices, the spawned viruses such as the Mirai are also increasing dramatically. In this context, attackers can easily vary botnets and change target scopes and links, so that the persistency of the collusive attack can be guaranteed.

IV. DEFEND MECHANISM

When the consumer-provider collusive attack starts, the PIT will be occupied by the long lived malicious entries, leading to the legitimate packets being discarded by the intermediate routers. In this situation, congestion occurs in the network and the legitimate clients cannot acquire the contents they need. In this section, we construct a consumer-provider

Algorithm 1 The PIT Expiration Time Analyzing Algorithm

```
Input:
  Initial time interval: $\Delta t_i$.
Output:
  The PIT expiration time: $t_{expired}$.
for each time period do
    malicious client sends $Interest_i$ at time $t_{Interest_i}$;
    malicious content provider replies with $Data_i$ at time $t_{Interest_i} + \Delta t_i$;
    if the malicious client receives $Data_i$ then
        the malicious client sends $Interest_{i+1}$;
        $\Delta t_{i+1} = \Delta t_i + 1$;
        if the malicious client cannot receive $Data_{i+1}$ then
            $\Delta t_{i+1}$ exceeds the actual expiration time;
            $t_{expired} = \Delta t_i$;
        end if
    end if
    return $t_{expired}$;
    if the malicious client does not receive $Data_i$ then
        $\Delta t_{i+1} = \Delta t_i / 2$;
    end if
end for
```

collusive attack defend mechanism through implementing a congestion control strategy based on the PIT information.

A. THE REPUTATION VALUE-BASED EARLY DETECTION (RVED) MECHANISM

We propose a Reputation Value-based Early Detection (RVED) mechanism to mitigate the network congestion caused by the consumer-provider collusive attack.

1) PROCEDURE OF THE RVED MECHANISM

Among the previous mentioned researches, Abu *et al.* [34] have put forward a random early detection-like (RED-like) method to control the PIT occupancy. However, this method aims to infer the congestion and notify the clients to reduce their Interest sending rate, and it does not distinguish between malicious and legitimate Interest packets. In this paper, we intend to control congestion of the PIT brought by the malicious Interest requests, and minimize the negative impact on legitimate requests at the same time.

The basic idea of the RVED mechanism is to detect and alleviate congestion by computing the average PIT utilization rate and drop Interest packets when the average PIT utilization rate exceeds the predefined threshold. The average PIT utilization rate $\tilde{\Gamma}_t$ can be calculated using the exponential weighted moving average (EWMA) [39] approach, as below.

$$\tilde{\Gamma}_t = \frac{\alpha \tilde{\Gamma}_{t-1} + (1-\alpha)\tau_t}{1-\alpha^t}, \tag{1}$$

where α represents the rate of weighted decline and ranges from 0 to 1. $\tilde{\Gamma}_{t-1}$ is the average PIT utilization rate at the last time $t-1$, and τ_t denotes the instantaneous PIT utilization rate value at time t. $1-\alpha^t$ represents the parameter of the bias correction aiming to reduce the error of the exponential weighted average in the early period. With the increase of t, the value of the $1-\alpha^t$ approaches 1, and the weighted average in the late period is not affected. The EWMA approach well reflects the change trend of time series. The smaller the coefficient α, the lower the weight of the past measured value, while the larger the coefficient, the higher the weight of the past value. In this paper, the value of α is set to be large so that the average PIT utilization rate changes slowly, to avoid dealing with an instantaneous and sudden request.

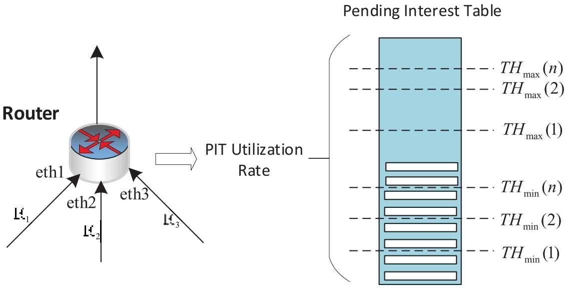


FIGURE 3. An example of the different thresholds of the PIT.

Generally, there are two kinds of thresholds for the PIT utilization rate - the minimum threshold $TH_{\min}$ and the maximum threshold $TH_{\max}$. When the PIT utilization rate is lower than $TH_{\min}$, there is no need to do any rate control operation. Packets are discarded with certain probability when the PIT utilization rate is between $TH_{\min}$ and $TH_{\max}$. And when the rate exceeds $TH_{\max}$, all of the packets will be dropped. However, this simple approach fails to distinguish the malicious PIT entries and the legitimate ones, so that it will deal with all kinds of Interest packets when the consumer-provider collusive attack begins. In order to overcome this deficiency, we propose to use different thresholds for different router interfaces according to the reputation value of the interfaces. Specifically, the PIT utilization rate of the entry coming from the interface with high reputation has higher threshold, while the entry from interface with the low reputation has lower threshold. In this way, when congestion occurs by the consumer-provider collusive attack, the Interest packets from the low reputation-interface will be limited first. Since the malicious packets will decrease the reputation of the interface, the malicious Interest information then will be blocked from getting into the PIT first, which can helpfully reduce the impact on normal Interest packets. As shown in Figure 3, the interfaces with different reputation values have different thresholds of the PIT utilization rate. Assume $\mathbb{R}_i$ $(i = 1, 2, \cdots, n)$ and $\mathbb{R}_1 < \mathbb{R}_2 < \cdots < \mathbb{R}_n$, the related minimum and maximum thresholds of interface i are $TH_{\min}(i)$ and $TH_{\max}(i)$, respectively. Then it can be obtained that $TH_{\min}(1) < TH_{\min}(2) < \cdots < TH_{\min}(n)$ and $TH_{\max}(1) < TH_{\max}(2) < \cdots < TH_{\max}(n)$.

When $\tilde{\Gamma}_t$ is lower than $TH_{\min}(i)$, the router can work normally and there is no need to do congestion control operations. When $\tilde{\Gamma}_t$ is higher than $TH_{\max}(i)$, the router will drop all the Interest packets coming from interface i. Besides, when $\tilde{\Gamma}_t$ is between $TH_{\min}(i)$ and $TH_{\max}(i)$, the Interest packets from i will be dropped with probability $p(i)$. Generally, the packet dropping probability $p(i)$ can be described as below:

$$p(i)=\begin{cases}0, & 0\leqslant\tilde{\Gamma}_t<TH_{\min}(i)\\ P_{\max}(i)\\ \times\dfrac{\tilde{\Gamma}_t-TH_{\min}(i)}{TH_{\max}(i)-TH_{\min}(i)}, & TH_{\min}(i)\leqslant\tilde{\Gamma}_t<TH_{\max}(i)\\ 1, & \tilde{\Gamma}_t\geqslant TH_{\max}(i).\end{cases}\tag{2}$$

where $P_{\max}(i)$ is the maximum dropping probability of interface i. $P_{\max}(i)$, $TH_{\min}(i)$ and $TH_{\max}(i)$ are related to the reputation value of interface i.

It is apparent that the packet dropping probability increases when the PIT utilization rate raises. In other words, when a large space of the PIT is occupied by the entries from certain interface, the newly arrived Interest packets from this interface will be dropped with high probability. Furthermore, when the collusive attack is finished, the PIT space will no longer be occupied by the malicious entries. So that the packet dropping strategy of the interfaces will not be triggered, and the packets' transmission process will be handled as normal on the routers.

2) COMPUTATION OF THE REPUTATION VALUE

In the related work mentioned above, there are some researches of attack defend methods based on the reputation value of the interface. In work [32], [33], the reputation value is defined by a proportion of the number of the returned Data packets to the number of Interest packets forwarded for each interface, which can also be called the Interest satisfaction rate. The authors point out that the attacker will send massive Interest packets and cannot get Data packets back, leading to the attacked interface having a low Interest satisfaction rate. However, under the situation of the consumer-provider collusive attack, since the attackers act like normal clients and the malicious Interest packets will be satisfied by the malicious content provider, the Interest satisfaction rate cannot truly represent the reputation value of the interface. Therefore, we propose an optimized reputation value computation approach. We take into consideration the average Round Trip Time (RTT) of the Interest packets of interface i, because the attackers try to maintain the PIT entries as long as possible and this will lead to a high data retrieval time. Then, the reputation value of the interface i denoted by $\mathbb{R}_i$ is calculated as below.

$$\mathbb{R}_i=\beta\cdot\frac{N_{DATA,i}}{N_{INTEREST,i}}+(1-\beta)\cdot\frac{\bar{\gamma}_{RTT,i}}{\sum\bar{\gamma}_{RTT,i}},\tag{3}$$

where β is the weighting parameter, $N_{DATA,i}$ represents the incoming Data packets to interface i, $N_{INTEREST,i}$ is the outgoing Interest packets from interface i, $\bar{\gamma}_{RTT,i}$ denotes the average RTT of the Interest packets of interface i, and $\sum\bar{\gamma}_{RTT,i}$ represents the total RTT of the Interest packets of all interfaces on the router.

3) ADAPTIVE MAXIMUM PACKET DROPPING PROBABILITY

When the reputation value of the interface is low, the corresponding maximum packet dropping probability should be a relatively large value. In other words, the attacked interface should drop the malicious Interest packets with a high probability. In this paper, we define the maximum packet dropping probability of interface i as below.

$$P_{\max}(i)=P_{\max}\times\frac{\sum_i^n\mathbb{R}_i}{\mathbb{R}_i},\tag{4}$$

where $P_{\max}$ is the initially settled maximum dropping probability and $\sum_i^n\mathbb{R}_i$ is the sum of the reputation value of all the n interfaces.

4) THRESHOLDS OF THE PIT UTILIZATION RATE

In the RVED mechanism, the interface which has a lower reputation value should drop packets first when there occurs network congestion by the consumer-provider attack. Therefore, the PIT utilization rate of the low reputation-interface will reach its threshold before the high reputation-interface. In this way, it can be ensured that the attacked interface is limited the earliest and the legitimate packets are protected. The thresholds of the PIT utilization rate of interface i can be calculated as below.

$$TH_{\min}(i)=TH_{\min}\times\frac{n\mathbb{R}_i}{\sum_i^n\mathbb{R}_i},\tag{5}$$

$$TH_{\max}(i)=TH_{\max}\times\frac{n\mathbb{R}_i}{\sum_i^n\mathbb{R}_i},\tag{6}$$

where $TH_{\min}$ and $TH_{\max}$ are the initially settled thresholds of the PIT utilization rate, and $\sum_i^n\mathbb{R}_i$ is the sum of the reputation value of all the n interfaces. Moreover, it is worth noting that the maximum packet dropping probability and the thresholds of the PIT utilization rate are updated with a certain interval.

5) OPTIMAL PACKET DROPPING PROBABILITY

As described earlier, when the average PIT utilization rate of the interface i is between the minimum and maximum threshold, the Data packets replying to interface i will be marked with probability in formula (2). To make it more intuitively, we demonstrate an example of the packet dropping probability in Figure 4.

It can be observed that the probability distribution of the packet dropping follows a piecewise function. The curve is linear when the PIT utilization rate is between the minimum and maximum threshold, causing that the gradient of the packet dropping probability is the same whatever the PIT utilization rate is. However, in the attack mitigation process, when the PIT utilization rate closes to the minimum threshold, the congestion is less likely to occur and the PIT space should be efficiently used. Otherwise, when the PIT utilization rate closes to the maximum threshold, congestion

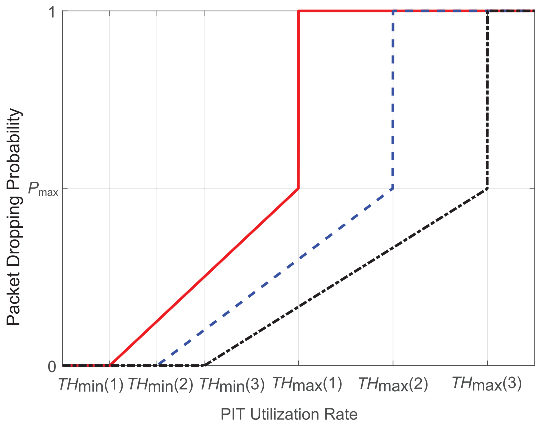


FIGURE 4. An example of the general packet dropping probability.

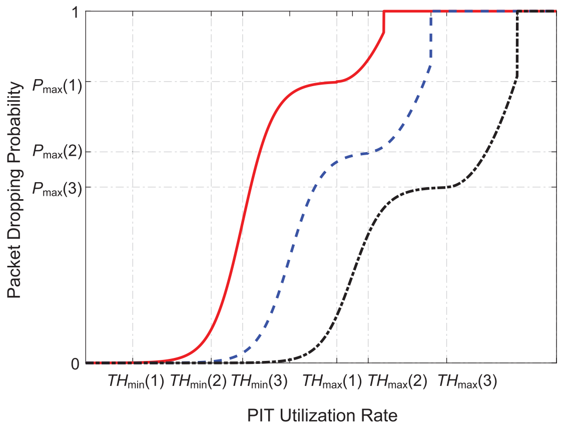


FIGURE 5. The optimal packet dropping probability.

caused by the attack occurs and the packet dropping probability needs to be sensitive to the change of PIT utilization rate. Thus, the linear variation of the packet dropping probability does not correspond to the practical necessity of the attack mitigation. Moreover, the general packet dropping probability increases suddenly to the highest value when the PIT utilization rate is larger than the maximum threshold, which is likely to cause oscillations in the network. Therefore, we put forward to use more adaptive and smoother functions to achieve the packet dropping probability, and we introduce an additional threshold $2 \cdot TH_{\max}(i)$ as a transition.

The optimal packet dropping probability is formulized as below.

$$p(i) = \begin{cases} 0, & 0 \leqslant \tilde{\Gamma}_t < TH_{\min}(i) \\ \frac{1}{2}P_{\max}(i) \times \frac{1}{1+e^{-\left[\tilde{\Gamma}_t - \frac{1}{2}(TH_{\min}(i)+TH_{\max}(i))\right]}}, & TH_{\min}(i) \leqslant \tilde{\Gamma}_t < TH_{\max}(i) \\ P_{\max}(i) \times \frac{\left(\tilde{\Gamma}_t - TH_{\max}(i)\right)^2}{TH^2{}_{\max}(i)} + \frac{1}{2}P_{\max}(i), & TH_{\max}(i) \leqslant \tilde{\Gamma}_t < 2 \cdot TH_{\max}(i) \\ 1, & \tilde{\Gamma}_t \geqslant 2 \cdot TH_{\max}(i). \end{cases} \tag{7}$$

When $\tilde{\Gamma}_t$ is less than $TH_{\min}(i)$, the packet will not be dropped. When $\tilde{\Gamma}_t$ is between $TH_{\min}(i)$ and $TH_{\max}(i)$, the packet dropping probability $p(i)$ follows a *sigmoid* function distribution. When $\tilde{\Gamma}_t$ is between $TH_{\max}(i)$ and $2 \cdot TH_{\max}(i)$, $p(i)$ follows a quadratic function distribution. And when $\tilde{\Gamma}_t$ is larger than $2 \cdot TH_{\max}(i)$, $p(i)$ increases to 1.

The example of the optimal packet dropping probability is demonstrated in Figure 5. As the figure shows, the variation of packet dropping probability becomes smoother, which can effectively improve the stability of the network control. The proposed RVED mechanism is given in Algorithm 2.

B. COMPLEXITY ANALYSIS

In this paper, we propose a reputation value-based early detection mechanism defending against the consumer-provider collusive attack in Information-Centric IoT context. There is no additional overhead cost of extra packets. In the RVED mechanism, the parameters RTT, reputation value of each interface, minimum and maximum thresholds of the PIT utilization rate and the maximum packet dropping probability are updated every $\hat{t}$ time interval, and updating these variables is an $O(1)$ operation. In each time interval, the current average PIT utilization rate and the packet dropping probability are needed to be computed for the n interfaces, which is an $O(n)$ operation. Since aggregating an Interest or creating a PIT entry is a normal process in the information centric based network, there will be no more additional cost by using the RVED mechanism.

V. EVALUATION

This section aims to verify the effectiveness of the proposed mechanism. We describe the evaluation method in section V-A, the impact of the attack in section V-B and the simulation results of the RVED mechanism in section V-C.

A. METHOD

We conduct the experiments based on the open-source ndnSIM [40], which implements NDN protocol stack for NS-3 network simulator. We observe and analyze the Interest traffic and Data traffic produced by the NDN simulator [41], and compare the network performance with RVED and without RVED when the collusive attack happens. We use a 25 nodes topology as shown in Figure 6. The point to point data rate between Router 7 and Router {1-6} is 100Mbps and the others' rate is 10Mbps. The channel delay is 10ms. We select Client {1, 2, 4, 5, 7} as the malicious clients, while Content Provider {3, 5, 6, 8, 9} as the malicious content provider. The legitimate clients issue 500 Interest packets/s and the malicious clients send 1000 Interest packets/s

Algorithm 2 The RVED Algorithm

```
Input:
  Initially maximum dropping probability: $P_{\max}$;
  Initially thresholds of the PIT utilization rate: $TH_{\min}, TH_{\max}$;
  Time interval: $\hat{t}$;
  Weight parameters: $\beta, \alpha$.
Output:
  Packet dropping rate of each interface $p(i)$.
for each time interval $\hat{t}$ do
    count incoming Data packets to $i$: $N_{DATA,i}$;
    count incoming Interest packets from $i$: $N_{INTEREST,i}$;
    calculate the average RTT of interface $i$: $\bar{\gamma}_{RTT,i}$;
    calculate the reputation value of each interface $i$: $\mathbb{R}_i$, $\mathbb{R}_i = \beta \cdot \frac{N_{in,i}}{N_{out,i}} + (1-\beta) \cdot \frac{\bar{\gamma}_{RTT,i}}{\sum \bar{\gamma}_{RTT,i}}$;
    calculate thresholds of the PIT utilization rate of each interface: $TH_{\min}(i)$ and $TH_{\max}(i)$, $TH_{\min}(i) = TH_{\min} \times \frac{n\mathbb{R}_i}{\sum_i^n \mathbb{R}_i}$; $TH_{\max}(i) = TH_{\max} \times \frac{n\mathbb{R}_i}{\sum_i^n \mathbb{R}_i}$;
    calculate the adaptive maximum packet dropping probability of each interface: $P_{\max}(i)$, $P_{\max}(i) = P_{\max} \times \frac{\sum_i^n \mathbb{R}_i}{\mathbb{R}_i}$;
    calculate the PIT utilization rate at time $t$: $\tilde{\Gamma}_t$;
    for each interface $i$ do
        if $0 \leqslant \tilde{\Gamma}_t < TH_{\min}(i)$ then
            the packet dropping probability $p(i) = 0$;
            accept incoming Interest packets as normal;
        else if $TH_{\min}(i) \leqslant \tilde{\Gamma}_t < TH_{\max}(i)$ then
            calculate the packet dropping probability $p(i)$, $p(i) = \frac{1}{2}P_{\max}(i) \times \frac{1}{1+e^{-\left[\tilde{\Gamma}_t - \frac{1}{2}(TH_{\min}(i)+TH_{\max}(i))\right]}}$;
            drop the incoming Interest packets from interface $i$ with probability $p(i)$;
        else if $TH_{\max}(i) \leqslant \tilde{\Gamma}_t < 2 \cdot TH_{\max}(i)$ then
            calculate the packet dropping probability $p(i)$, $p(i) = P_{\max}(i) \times \frac{\left(\tilde{\Gamma}_t - TH_{\max}(i)\right)^2}{TH^2{}_{\max(i)}} + \frac{1}{2}P_{\max}(i)$;
            drop the incoming Interest packets from interface $i$ with probability $p(i)$;
        else if $\tilde{\Gamma}_t \geqslant 2 \cdot TH_{\max}(i)$ then
            the packet dropping probability $p(i) = 1$;
            drop the incoming Interest packets;
        end if
    end for
end for
return packet dropping probability $p(i)$.
```

with uniform distribution. The payload size of each Data packets is 512 bytes. The PIT size is set as 100 entries, the PIT timeout period is 2s, the simulation time is 80s, the consumer-provider collusive attack starts from 20s to 40s, and the information statistics time interval is 0.5s. $P_{\max}$ is 0.3. Referring to [42], [43], $TH_{\min}$ is set as 0.33. As [44] and [45] suggest that a useful rule-of-thumb in a queue management scheme is to set the maximum threshold to at least twice minimum threshold, we set $TH_{\max}$ as 0.45, so that the maximum threshold in RVED - $2 \cdot TH_{\max}$ satisfies the rule in [44], [45]. The time interval $\hat{t}$ is 0.5s, β is 0.25, α is 0.875. The malicious clients request for existent prefixes {“/dst3”, “/dst5”, “/dst6”, “/dst8”, “/dst9”} which can be provided by the malicious content providers.

B. IMPACTS OF THE CONSUMER-PROVIDER COLLUSIVE ATTACK

This section describes the negative influence brought by the consumer-provider collusive attack. Figure7 shows that the average normal PIT utilization rate of Client 3, Router 1 and Router 7 is 0.42, 0.31 and 0.83, respectively. Then, the PIT utilization rates of these nodes immediately increase to 1 when the attack begins, which results in the legitimate Interest packets being dropped. Figure 8 shows the variation of the Interest packets on different nodes under the collusive attack. When the attack begins, the satisfaction rate of the Interest packets sharply decreases and remains in a low position until the attack ends. Simultaneously, the drop rate and time out rate of the Interest packets increases with the injection of the malicious packets.

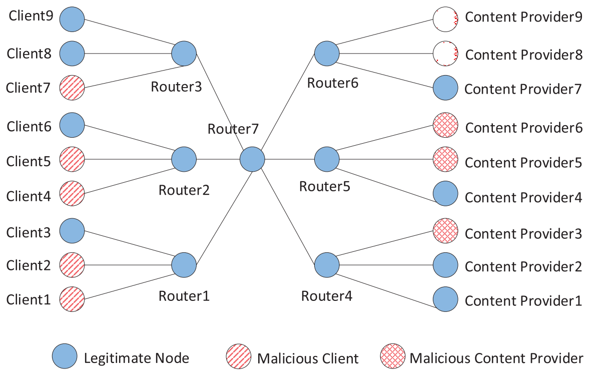


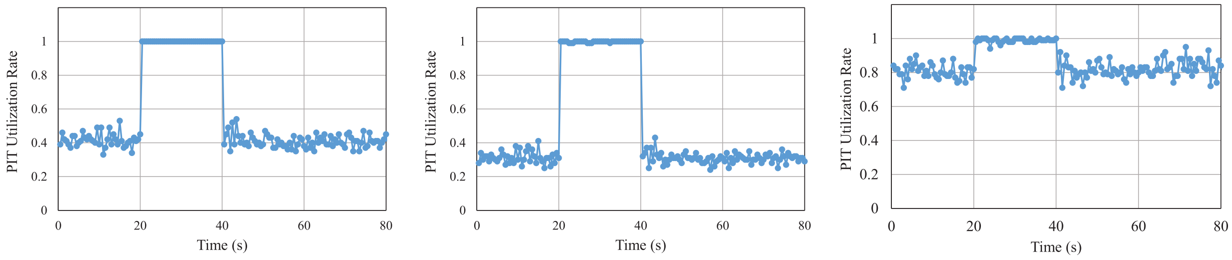
FIGURE 6. **Topology of the evaluation.**

In addition, we demonstrate the full delay of the data retrieval on the legitimate consumers. The full delay represents the time between sending the first Interest packet requesting a content and receiving the requested Data packet. As Figure 9 shows, the normal average value of the full delay is about 0.081s. When the collusive attack is launched, the full delay of the legitimate Consumer 3, Consumer 6, Consumer 8 and Consumer 9 increases to 23.8587s, 27.6414s, 22.6590s and 22.6926s, respectively. The results apparently indicate that the consumer-provider collusive attack brings negative influence on the performance of the entire network and makes the network in an instable status.

C. EFFECTIVENESS OF THE RVED METHOD

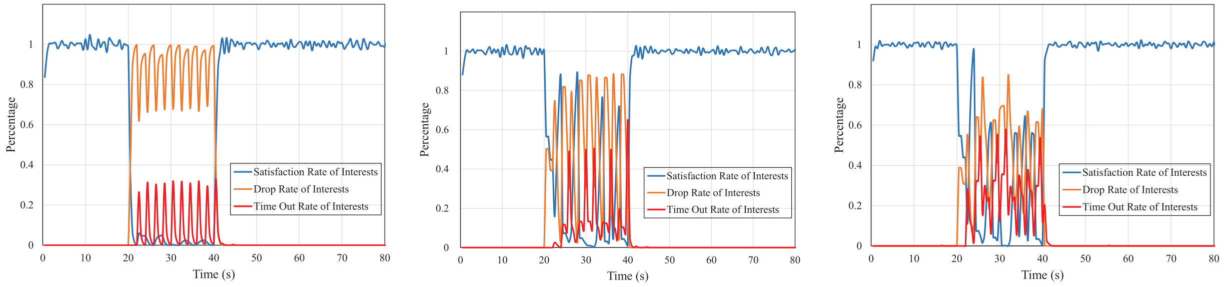
To evaluate the effectiveness of the RVED mechanism, we first implement simulations under different attack rates. We let each malicious client send 500, 1000, 2000 Interest packets per second, respectively. Figure 10 shows that the PIT utilization rate of Router1 increases to 1 when the attack starts and then quickly back to the normal level when using the proposed RVED method.

Then we compare what happens with RVED and without RVED. Figure 11 provides the Cumulative Distribution Function (CDF) curves of the Interest packets under different attack rates of the interface on Router1 which connected to Client 3. When each malicious client issues 500 malicious Interest packets per second, Figure 11(a) shows that the satisfaction rate of the Interests without RVED is less than 0.4 in 25% of total simulation time, while the satisfaction rate with RVED is less than 0.8 in only 8% of total time. The drop rate of Interests without RVED increases from 0 to 0.9 in 23% of time, and the drop rate with RVED is only effected in 4% of time. Besides, the time out rate of Interests without RVED varies from 0 to 0.85 in 22% of time while the rate with RVED just varies in 3% of time. When the attack rate is 1000 packets/s, we can observe from Figure 11(b) that the satisfaction rate without RVED is less than 0.55 in 20% of time, while that with RVED is less than 0.55 in 5% of time. The drop rate of Interests without RVED is affected in 25% of time, while the rate with RVED acts abnormally in 4.5% of time. And the time out rate without and with RVED are affected in 22% and 3% respectively. When the attack rate is 2000 packets/s, Figure 11(c) shows that the satisfaction rate without and with RVED are fluctuated in 25% and 6% of time. The drop rate without and with RVED are mainly



(a) Client 3 (b) Router 1 (c) Router 7

FIGURE 7. **The PIT utilization rate of the nodes.**



(a) Router 7 (b) Router 10 (c) Router 11

FIGURE 8. **The variation of the Interests on the nodes under the collusive attack.**

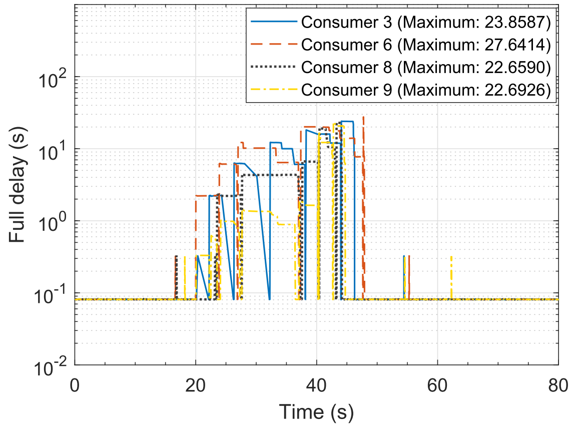


FIGURE 9. The full delay to obtain the data on the consumers.

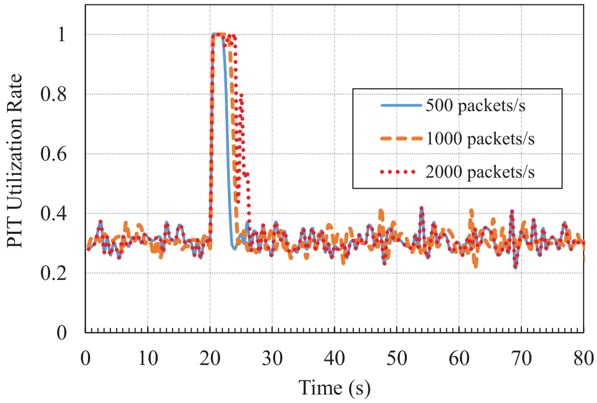
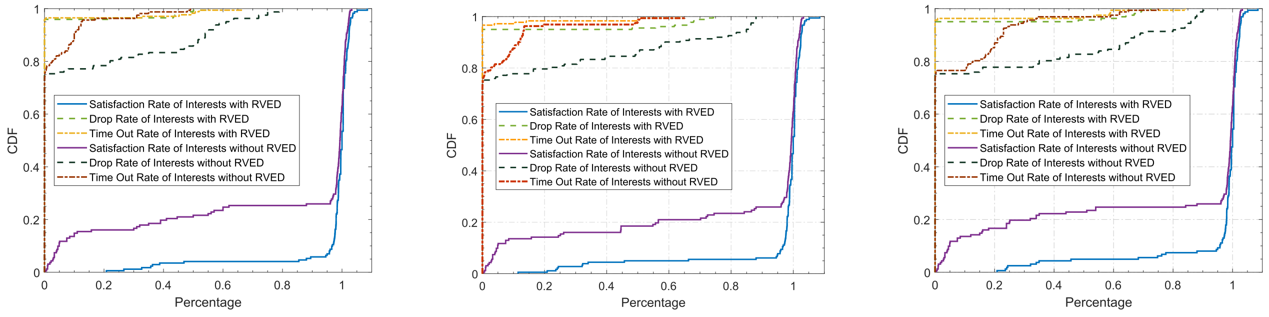


FIGURE 10. The PIT utilization rate with RVED of Router 1.

influenced in 24% and 5% of time. Besides, the time out rate of the Interests without RVED is influenced in 23.5% of time while that with RVED varies in 3% of time. The statistical results indicate that the RVED mechanism can decrease the negative impacts brought by the collusive attack and make the network stay in a more stable state.

Furthermore, we demonstrate the CDF of the full delay of Data retrieval in Figure 12. When the payload size of each Data packet is 256 bytes, the full delay without RVED is larger than 8s in 14% of total time, and the delay with RVED is larger than 4s in 2.5% of time. When the payload size of each Data is 512 bytes, the full delay without RVED is larger than 13s in 10% of time and the delay with RVED is exceeds 4s in just 2.4% of the total time. Additionally, when each Data packet carries 1024 bytes payload, the full delay without RVED is larger than 15s in 9% of time, while the delay with RVED is larger than 2.2s in only 2.5% of the total time. This implies that the RVED can effectively reduce the Data packet retrieval time when the consumer-provider collusive attack occurs. Besides, it is worth mentioning that when we consider the legitimate heavy load traffic appears at the same time as the attack traffic in the network. Although in this case, the routers still need to consider the average delay when calculating the reputation values. The considered average delay represents the delay between last Interest sent and Data packet received, rather than the full delay between first Interest sent and Data packet received, which includes the retransmission delay. As a normal traffic, the heavy traffic's average delay is much smaller than that of the attack traffic because the attackers are always trying to keep the delay nearing to the PIT expiration time. As a result, although the legitimate heavy load may be easy to be confused with the attack traffic in terms of traffic statistics, it can still be recognized from the statistics against the PIT, the average delay and the reputation values.

Finally, we compare the proposed RVED mechanism with the previous IFBN method [33] and RED-like method [34]. We simulate different attack rate scenarios and analyze the effectiveness on mitigating the consumer-provider collusive attack of these methods. Figure 13 demonstrates the changes of the PIT utilization rate on Router 1 when the attack happens from 20s to 80s with each malicious client sends 500 packets and 1000 packets per second. As shown in this figure, both the RED-like and the proposed RVED methods can slow down the impact of the attack. However, since the RED-like method limits all kinds of the incoming packets without distinguish the suspicious interfaces, the legitimate Interest packets are dropped with the same possibility of the malicious packets, result in the PIT utilization rate being lower than the normal level after the rate limiting.



(a) each malicious client sends 500 packets/s. (b) each malicious client sends 1000 packets/s. (c) each malicious client sends 2000 packets/s.

FIGURE 11. CDF of the Interest packets under different attack rates.

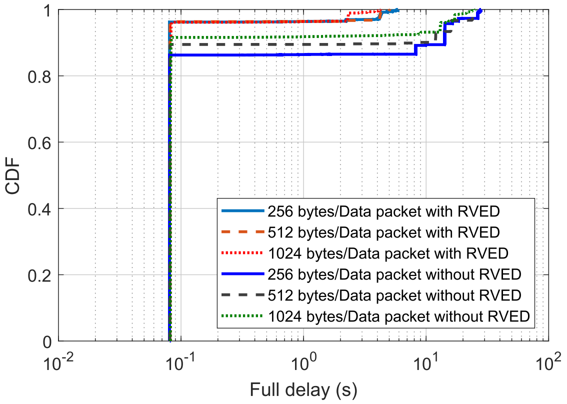


FIGURE 12. CDF of the full delay of Data packet retrieval.

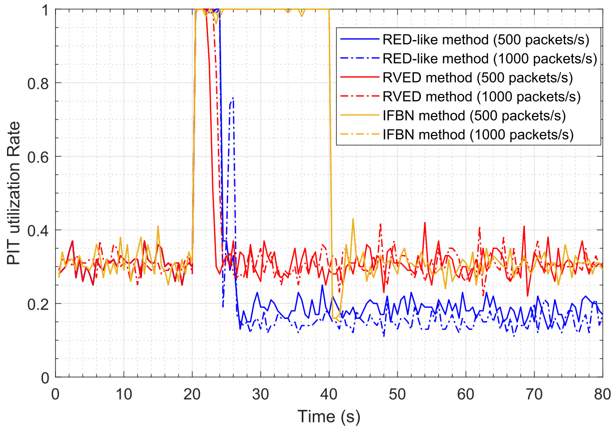


FIGURE 13. Comparisons with the previous methods on PIT utilization rate under different attack rates.

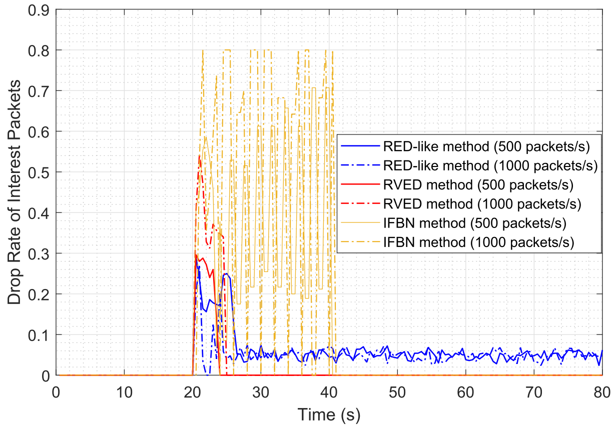


FIGURE 14. Comparisons with the previous method on packet drop rate under different attack rates.

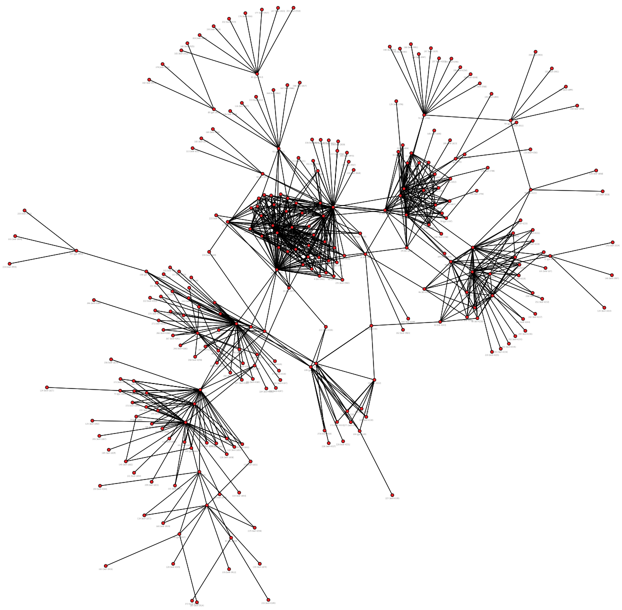


FIGURE 15. The Rocketfuel network topology.

TABLE 1. Link bandwidth and delay in the Telstra topology.

Link type	Bandwidth (Mbps)	Delay (ms)
Backbone node - backbone node	41 ∼ 91	5 ∼ 10
Backbone node - gateway node	10 ∼ 20	5 ∼ 10
Gateway node - leaf node	1 ∼ 3	12 ∼ 66

Figure 14 demonstrates the drop rate of Interest packets of the face on Router 1 that connected to legitimate Consumer 3. When the collusive attack starts, the PIT of the router is occupied by massive malicious entries, and then leads to the legitimate Interest packets being dropped. When using the IFBN method, the packets drop rate is quite high and the network exposes an instable state. This is because that the satisfaction rate of the interface that is not attacked directly will also be affected by the collusive attack. It will decrease to a low value as the interface being attacked directly. Therefore, the IFBN method does not satisfy its cache control condition, so that the negative effect of the consumer-provider collusive attack is not eliminated. Besides, as the figure shows, both of the RED-like method and the RVED method can reduce the packets drop rate. After a processing time, the legitimate packets are still being dropped when using the RED-like method, while the legitimate packets of the RVED method are prevented from being dropped. This indicates that the proposed RVED method can help protect the legitimate Interest packets effectively.

D. PERFORMANCE OF RVED UNDER A LARGE-SCALE TOPOLOGY

To better illustrate the effectiveness of the proposed RVED method, we conduct simulations under a larger topology, which can be more consistent with an actual IoT devices' deployment. As Figure 15 shows, we use a Telstra network topology (AS1221) of the Rocketfuel [46]. The topology consists of 65 backbone nodes, 45 gateway nodes and 169 leaf nodes. The basic link configurations are listed in Table 1. We randomly select 48 leaf nodes as legitimate consumers and the rest 121 leaf nodes as malicious consumers. Besides,

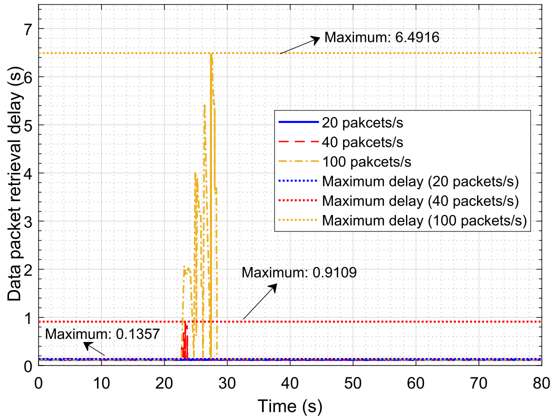


FIGURE 16. Data packet retrieval delay of the legitimate consumer under different attack rates.

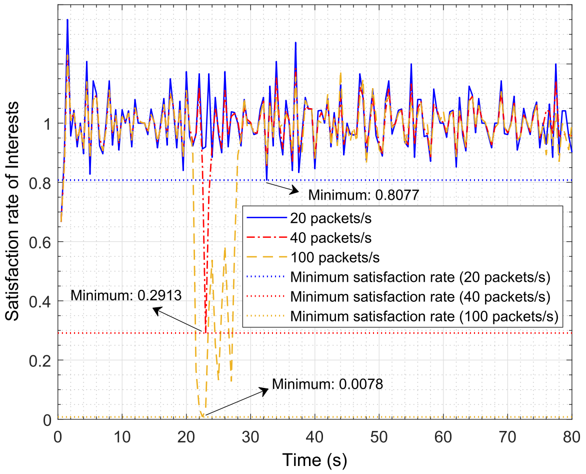


FIGURE 17. Satisfaction rate of the legitimate consumer under different attack rates.

we select three backbone nodes as the legitimate content providers and another three backbone nodes as the malicious content provider. We repeat the simulation for 10 times. Referring to [47], we set the packet sending rate of the legitimate consumer as 50 packets/s, while the rate of the malicious consumer as 20, 40 and 100 packets/s, respectively. As stated in Section V-A, the simulation time is 80s and the collusive attack starts from 20s to 40s. To evaluate the effect of the collusive attack and the RVED defending method, we observe the performance of the legitimate consumers.

Figure 16 shows the Data packet retrieval delay of the legitimate consumer under different attack rates. When each attacker sends 20 malicious Interest packets per second, the attack is not effective, and the maximum packet retrieval delay is 0.1357s. When the attack rate increases to 40 packets/s, the attack shows negative effects on the network. The content retrieval delay of the legitimate consumer increases to 0.9109s but it soon returns to a normal state. Moreover, when the malicious Interest packets are sent with a rate of 100 packets/s, the impact of the attack on the network is increased incredibly. The maximum delay to obtain a required Data packet reaches to 6.4916s, which is several times greater than the value when the attack is invalid. The figure also shows that, with the proposed RVED method, the performance of the network is recovered gradually and finally back to a normal level.

In addition, we evaluate the satisfaction rate of Interests on the legitimate consumer. As shown in Figure 17, when each malicious consumer sends 20 packets per second, the legitimate consumer is not affected and the satisfaction rate of Interests is relatively stable. When the attack rate is 40 packet per second, the satisfaction rate is decreased apparently, where the minimum value is 0.2913. Besides, the minimum satisfaction rate is 0.0078 when each malicious consumer sends 100 packets per second, which strongly indicates that with the increase of the attack strength, the network performance gets worse. Nevertheless, it can be observed that the satisfaction rate of Interests returns to a normal state soon when adopting the proposed RVED method. Based on the results and analysis, it is proved that the RVED method can effectively alleviate the negative impact brought by the consumer-provider collusive attack.

VI. CONCLUSION

In this paper, we have proposed a Reputation Value based Early Detection (RVED) mechanism to mitigate the negative impacts on the network, which caused by the consumer-provider collusive attack in the context of Information-centric IoT. Specifically, we have expounded a model of the consumer-provider collusive attack. We have proposed to detect and alleviate the congestion by computing the average PIT utilization rate and drop Interest packets when the average PIT utilization rate exceeds the predefined threshold. We have put forward to set different thresholds for different faces according to their reputation values and to adaptively adjust the packet dropping rate. We have conducted simulations to verify the effectiveness of the proposed RVED mechanism and compared it with the previously existing method. The simulation results have shown that the RVED could effectively reduce the negative impacts on the legitimate Interest packets, and could protect legitimate packets from being probabilistically dropped to a great extent. As a future work, we plan to apply the proposed mechanism into more realistic topologies and construct an actual system to validate our mechanism.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[2] M. Mohammadi, A. Al-Fuqaha, M. Guizani, and J.-S. Oh, "Semisupervised deep reinforcement learning in support of IoT and smart city services," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 624–635, Apr. 2018.

[3] A. Pandharipande, M. Zhao, E. Frimout, and P. Thijssen, "IoT lighting: Towards a connected building eco-system," in *Proc. IEEE 4th World Forum Internet Things (WF-IoT)*, Singapore, Feb. 2018, pp. 664–669.

[4] Y. Seungjun and J. Hyojung, "Issues and implementation strategies of the IoT (Internet of Things) industry," in *Proc. 10th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Fukuoka, Japan, Jul. 2016, pp. 503–508.

[5] V. Petrov, A. Samuylov, V. Begishev, D. Moltchanov, S. Andreev, K. Samouylov, and Y. Koucheryavy, "Vehicle-based relay assistance for opportunistic crowdsensing over narrowband IoT (NB-IoT)," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3710–3723, Oct. 2018.

[6] S. Sharma, K. Chen, and A. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 42–51, Mar. 2018.

[7] M. H. Yaghmaee and H. Hejazi, "Design and implementation of an Internet of Things based smart energy metering," in *Proc. IEEE Int. Conf. Smart Energy Grid Eng. (SEGE)*, Oshawa, ON, Canada, Aug. 2018, pp. 191–194.

[8] *The GSMA Guide to the Internet of Things*. Accessed: Jun. 25, 2018. [Online]. Available: https://www.gsma.com/iot/wp-content/uploads/2018/09/4048-GSMA-IOT-Guide2018-WEB.pdf

[9] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, and H. Dai, "A survey on low latency towards 5G: RAN, core network and caching solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3098–3130, 2018.

[10] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, "A survey of information-centric networking research," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1024–1049, 2014.

[11] J. Wu, M. Dong, K. Ota, J. Li, W. Yang, and M. Wang, "Fog-computing-enabled cognitive network function virtualization for an information-centric future Internet," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 48–54, Jul. 2019.

[12] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-AI enabled IoT: A consortium blockchain-based efficient and incentive approach," *IEEE Trans Ind. Informat.*, vol. 15, no. 12, pp. 6367–6378, Dec. 2019.

[13] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, "Recent advances in information-centric networking-based Internet of Things (ICN-IoT)," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2128–2158, Apr. 2019.

[14] J. Kwak, Y. Kim, L. B. Le, and S. Chong, "Hybrid content caching in 5G wireless networks: Cloud versus edge caching," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 3030–3045, May 2018.

[15] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, and K. Drira, "Cache coherence in Machine-to-Machine information centric networks," in *Proc. IEEE 40th Conf. Local Comput. Netw. (LCN)*, Clearwater, FL, USA, Oct. 2015, pp. 430–433.

[16] J. Hong, "Challenges of name resolution service for information centric networking toward IoT," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Jeju-do, South Korea, Oct. 2016, pp. 1085–1087.

[17] S. Arshad, B. Shahzaad, M. A. Azam, J. Loo, S. H. Ahmed, and S. Aslam, "Hierarchical and flat-based hybrid naming scheme in content-centric networks of things," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1070–1080, Apr. 2018.

[18] R. Li, H. Asaeda, and J. Li, "A distributed publisher-driven secure data sharing scheme for information-centric IoT," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 791–803, Jun. 2017.

[19] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "A secure ICN-IoT architecture," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Paris, France, May 2017, pp. 259–264.

[20] T. Mick, R. Tourani, and S. Misra, "LASeR: Lightweight authentication and secured routing for NDN IoT in smart cities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 755–764, Apr. 2018.

[21] R. Ullah, S. H. Ahmed, and B.-S. Kim, "Information-centric networking with edge computing for IoT: Research challenges and future directions," *IEEE Access*, vol. 6, pp. 73465–73488, Dec. 2018.

[22] D. An and D. Kim, "ICN-based light-weighted mobility support in IoT," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Hangzhou, China, Jul. 2018, pp. 1–2.

[23] S. Shannigrahi, C. Fan, and G. White, "Bridging the ICN deployment gap with IPoC: An IP-over-ICN protocol for 5G networks," in *Proc. Workshop Netw. for Emerg. Appl. Technol. (NEAT)*. New York, NY, USA: ACM, 2018, pp. 1–7.

[24] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *Proc. 26th USENIX Secur. Symp. USENIX Secur.*, Vancouver, BC, Canada, Aug. 2017, pp. 1093–1110.

[25] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS attacks: Trends and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2242–2270, 4th Quart., 2015.

[26] D. Kutscher, S. Eum, K. Pentikousis, I. Psaras, D. Corujo, D. Saucez, T. C. Schmidt, and M. Waehlisch, *Information-Centric Networking (ICN) Research Challenges*, document RFC 7927, Jul. 2016.

[27] H. Salah and T. Strufe, "Evaluating and mitigating a collusive version of the interest flooding attack in NDN," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Messina, Italy, Jun. 2016, pp. 938–945.

[28] S. Signorello, S. Marchal, J. Francois, O. Festor, and R. State, "Advanced interest flooding attacks in named-data networking," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Oct. 2017, pp. 1–10.

[29] Y. Xin, Y. Li, W. Wang, W. Li, and X. Chen, "Detection of collusive interest flooding attacks in named data networking using wavelet analysis," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Baltimore, MD, USA, Oct. 2017, pp. 557–562.

[30] A. Nasserala and I. M. Moraesy, "Analyzing the producer-consumer collusion attack in content-centric networks," in *Proc. 13th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, , Jan. 2016, pp. 849–852.

[31] A. Nasserala, I. V. Bastos, and I. Monteiro Moraes, "Cache nFace: A simple countermeasure for the producer-consumer collusion attack in named data networking," *Ann. Telecommun.*, vol. 74, nos. 3–4, pp. 125–137, Oct. 2018.

[32] S. Umeda, T. Kamimoto, Y. Ohata, and H. Shigeno, "Interest flow control method based on user reputation and content name prefixes in named data networking," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, Aug. 2015, pp. 710–717.

[33] R. Shinohara, T. Kamimoto, K. Sato, and H. Shigeno, "Cache control method mitigating packet concentration of router caused by interest flooding attack," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Tianjin, China, Aug. 2016, pp. 324–331.

[34] A. J. Abu, B. Bensaou, and A. M. Abdelmoniem, "Inferring and controlling congestion in CCN via the pending interest table occupancy," in *Proc. IEEE 41st Conf. Local Comput. Netw. (LCN)*, Dubai, United Arab Emirates, Nov. 2016, pp. 433–441.

[35] Y. Nakatsuka, J. L. Wijekoon, and H. Nishi, "FROG: A packet hop count based DDoS countermeasure in NDN," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Natal, Brazil, Jun. 2018, pp. 492–497.

[36] G. Liu, W. Quan, N. Cheng, B. Feng, H. Zhang, and X. S. Shen, "BLAM: Lightweight Bloom-filter based DDoS mitigation for information-centric IoT," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 1–7.

[37] T. Zhi, H. Luo, and Y. Liu, "A Gini impurity-based interest flooding attack defence mechanism in NDN," *IEEE Commun. Lett.*, vol. 22, no. 3, pp. 538–541, Mar. 2018.

[38] T. Zhi, Y. Liu, and Z. Yan, "An entropy-SVM based interest flooding attack detection method in ICN," in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Chicago, IL, USA, Aug. 2018, pp. 1–5.

[39] J. M. Lucas and M. S. Saccucci, "Exponentially weighted moving average control schemes: Properties and enhancements," *Technometrics*, vol. 32, no. 1, pp. 1–12, Feb. 1990.

[40] A. Afanasyev, I. Moiseenko, and L. Zhang, "ndnSIM: NDN simulator for NS-3," NDN, Shanghai, China, Tech. Rep. NDN-0005, Oct. 2012.

[41] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the evolution of ndnSIM: An open-source simulator for NDN experimentation," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 47, no. 3, pp. 19–33, Sep. 2017.

[42] R. Stankiewicz and A. Jajszczyk, "Analytical models for multi-RED queues serving as droppers in DiffServ networks," in *Proc. IEEE IEEE Global Telecommun. Conf. (GLOBECOM)*, Washington, DC, USA, Nov. 2007, pp. 2667–2671.

[43] R. Pan, B. Prabhakar, and K. Psounis, "CHOKe—A stateless active queue management scheme for approximating fair bandwidth allocation," in *Proc. IEEE Conf. Comput. Commun., 19th Annu. Joint Conf. IEEE Comput. Commun. Societies (INFOCOM)*, Mar. 2000, pp. 942–951.

[44] B. Zheng and M. Atiquzzaman, "DSRED: An active queue management scheme for next generation networks," in *Proc. 25th Annu. IEEE Conf. Local Comput. Networks. LCN*, Washington, DC, USA, Nov. 2000, pp. 242–251.

[45] S. Floyd, R. Gummadi, and S. Shenker, "Adaptive RED: An algorithm for increasing the robustness of RED's active queue management," in *Proc. ICIR*, Aug. 2001, pp. 1–12. [Online]. Available: http://www.icir.org/floyd/red.html

[46] N. Spring, R. Mahajan, and D. Wetherall, "Measuring ISP topologies with rocketfuel," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 4, p. 133, Oct. 2002.

[47] F. Malandra, L. O. Chiquette, L.-P. Lafontaine-Bédard, and B. Sansò, "Traffic characterization and LTE performance analysis for M2M communications in smart cities," *Pervas. Mobile Comput.*, vol. 48, pp. 59–68, Aug. 2018.

TING ZHI received the B.S. degree from Beijing Jiaotong University, in 2014, where she is currently pursuing the Ph.D. degree with the School of Electronic and Information Engineering. Her research interests are network security and information centric networking.

YING LIU received the M.S. and Ph.D. degrees from Beijing Jiaotong University, in 2003 and 2012, respectively. Since 2012, she has been an Associate Professor with the National Engineering Laboratory for Next Generation Internet Technology, School of Electronic and Information Engineering, Beijing Jiaotong University. Her current research interests include network architecture, network security, protocols optimization, wireless communications, and cloud computing.

JUN WU received the Ph.D. degree in information and telecommunication studies from Waseda University, Japan, in 2011. He is currently an Associate Professor with the School of Cyber Security, Shanghai Jiao Tong University, China, where he is also the Vice Director of the National Engineering Laboratory for Information Content Analysis Technology. His research interests include advanced computing, communications and security techniques of software-defined networks, information-centric networks smart grids, and the Internet of Things.