IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 23, 2020, accepted July 5, 2020, date of publication July 13, 2020, date of current version July 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3008723

The Detection Method of Collusive Interest Flooding Attacks Based on Prediction Error in NDN

LIANG LIU, WENZHI FENG, ZHIJUN WU, MENG YUE, AND RUDAN ZHANG
School of Electronics and Information and Automation, Civil Aviation University of China, Tianjin 300300, China

Corresponding author: Liang Liu (liul@cauc.edu.cn)

This work was supported in part by the Joint Funds of National Natural Science Foundation of China and Civil Aviation Administration of China under Grant U1933108, and in part by the Fundamental Research Funds for the Central Universities of China under Grant 3122019051.

ABSTRACT Named Data Networking (NDN) is one of the main research projects of the information center network (ICN), and its efficient forwarding mechanism attaches the attention of researchers. Like other networks, NDN also faces the threat of cyber attacks. With the assistance of the colluding server, the Collusive Interest Flooding Attacks (CIFA) can use the defects of the NDN's internal forwarding mechanism to send malicious interest packets in the form of pulses. It affects the normal requests of legitimate users and reduces the quality of NDN network services in this way. By analyzing the characteristics of network traffic and CIFA model, a new CIFA detecting method based on the prediction error between particle filter and one-step prediction algorithm is proposed. This scheme samples the network traffic and judges whether the network is under attack by comparing the normalized error value of the one-step prediction and the estimate of the particle filter. Experimental analysis shows that the detection scheme in this paper has higher detection rate than the existing detection schemes.

INDEX TERMS Named data networking, collusive interest flood attacks, prediction error, one-step prediction, particle filter.

I. INTRODUCTION

The core architecture of TCP/IP networks remains relatively stable. But the security, mobility and distribution aspects of the network are increasingly demanded by a variety of applications. In order to solve the contradiction between the growing application and the traditional network architecture, the concept of future network is proposed [1]. Among them, the most striking is the NDN, which retains the narrow-waist model in the TCP/IP architecture and guarantees that each routing node can transmit information efficiently with a variety of flexible routing strategies [2], [3].

The NDN network is designed with safety first. NDN can defend against various types of attacks in TCP/IP networks through the mutual cooperation among Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB), including the most common denial-of-service attacks in today's network, such as exhaustion of bandwidth resource, reflection attack and flooding attack [1]. Effective defense against these types of attacks can greatly enhance the security of NDN, making it highly anticipated in the development stage. However, the Interest Flooding Attack (IFA) has been found in the NDN network. This kind of attack sends a large number of false interest packets that exceed the accepted limit of the routing node, so that the PIT entries generated by them can overload the PIT space, causing the victimized routing node to discard the legitimate interest packets that are subsequently passed in. It is a type of DDoS attack against NDN network [4], [5]. The attackers can use IFA to overload the entire infrastructure, destroy all close-range users and even cause the NDN internal service to be paralyzed, which is very serious for the NDN architecture.

The IFA attacks are divided into three categories:(1) request static content;(2) request dynamic content;(3) request nonexistent content [6]. At present, researchers have focused on mitigating the (3) type of attack, mainly because it can more easily damage the NDN network environment by requesting content that does not exist in the network, resulting in a

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

decline in network service quality. At present, this type of attack has been well mitigated. However, a new DDoS attack named CIFA has emerged in recent years. With the help of the colluding server, the attacker can send a type (1) or (2) to initiate DDoS attack and the attack effectiveness is similar to type (3). The colluding server can send the data packets before the corresponding PIT entry expires, so that the colluding interest packet is satisfied by the server like other legitimate interest packets. This ensures that the PIT entries generated by the colluding interest packets remain in the PIT of the affected routing node for as long as possible without being detected. Therefore, the PIT occupancy of the victim router will remain high without producing expired PIT entries. If the PIT of routing node on the path is overloaded, all subsequent incoming interest packets will be discarded, resulting in legitimate users' interest packets not being satisfied by the normal server. CIFA can attack the PIT space intermittently with less resources, keep the PIT in the overload state. It greatly reduces the service quality of NDN network and make the NDN network lose its advantages in transmission performance [7].

Based on the study of NDN traffic characteristics, we analyze the CIFA model and proposes a new detecting method for CIFA based on the prediction error between particle filter and one-step prediction algorithm is proposed. When CIFA attack occurs, malicious traffic will destroy the stability of network traffic. This detection scheme does not need to acquire a large number of attack features for a long time. It can feel the traffic changes caused by CIFA sensitively and has good real-time performance. Meanwhile, the detection mechanism is an independent detection module, which does not affect the forwarding mechanism and transmission status. Compared with the existing detection scheme, the scheme has higher detection rate and lower false alarm rate.

The remaining of the paper is organized as follows: Section 2 discusses the related works about research progress of detection approaches on IFA, CIFA and Low-rate DDoS (LDoS) attacks; Section 3 mainly introduces the proposed approach based on prediction error; Section 4 shows the experimental results and comparative analysis can prove the effectiveness of the proposed approach; Section 5 summarizes this paper and describes our future work.

II. RELATED WORK

CIFA is a new type of IFA against NDN network, which can collude with the server to request the real content to exhaust the space of PIT on the victim router. The CIFA can periodically send malicious interest packets at a low average rate which can be hidden in background traffic, resulting in the existing detection schemes basically not detecting abnormal changes caused by CIFA attacks on the network. Therefore, the CIFA attack should attract more attention from relevant researchers. In terms of anomaly detection, most of the existing research programs are aimed at traditional IFA and have good detection and defense effects. For CIFA, researchers mainly focus on the analysis of attack effectiveness and feature extraction. Because the attack principles of CIFA attacks are different from IFA, the detection scheme of IFA is not suitable for detecting CIFA. There is still a lack of effective detection schemes for CIFA attacks. The traditional detection scheme for IFA can only be used as reference objects for experiments. As studying the state of the art, we also provide an overview and analysis of IFA attack detection methods, which can provide reference for research of CIFA.

Alexander *et al.* proposed a traffic control method for NDN network. There are three different defense schemes in [8]. The core idea of these three defense strategies is to reduce the malicious impact of IFA on the network by limiting the rate of incoming interest packets at the interface. The implementation scheme adopts the improved Token Bucket algorithm on the interface of routing nodes to control the number of forwarding interest packets.

Albert's team proposed a defense scheme called Poseidon [6], whose main defense method is to monitor the satisfaction of interest packets and the PIT occupancy of routing nodes. When the detected feature is abnormal during the continuous monitoring cycle, the router informs the neighboring node of the malicious interface. This method uses collaboration between routing nodes to mitigate the malicious impact of IFA on the network. But if the neighboring nodes are hijacked, it will bring more serious threats.

Kun *et al.* proposed a detection scheme based on Markov state transfer [9]. In this scheme, the space vector is defined according to the amount of change in PIT occupancy rate. The network status is judged with a quantized value. Finally, by calculating the Euclidean distance to distinguish between legitimate interest packets and malicious interest packets. This detection method can guarantee a high detection rate. However, it takes too much network resources to detect all interest packets for a large amount of network traffic in the NDN network.

Hou *et al.* [10] proposed IFA countermeasure based on Theil. This countermeasure can divide interest packets into different groups and identify attacks based on the distribution of names. Zhi *et al.* [11]. proposed a detection defense mechanism against IFA based on Gini coefficients. When attack occurs, the Gini impurity of name in the network environment is affected by a large number of malicious interest packets and exceeds the normal range. However, [10], [11] need to process information of thousands of megabytes of traffic in NDN network. This greatly reduces the real-time capability of the detection scheme. At the same time, the detection effect of this kind of monitoring scheme against CIFA attack is poor.

Considering that CIFA attack mechanism is closer to the LDoS attack in the TCP / IP network, so we also conducted comparative analysis. In TCP/IP network architecture, most of the detection methods for LDoS attack are based on network traffic characteristics, including time-domain characteristics, frequency-domain characteristics and so on. The time domain method mainly extracts the time domain characteristics of normal traffic and abnormal traffic to judge whether

TABLE 1. Comparison of attack detection schemes in different network environments.

Detection algorithm	Detection characteristics	Network environment	Type of attack detected	Detection rate	False alarm rate	Real-time performance	Difficulty of deployment	Deployment location
Paper[6]	Satisfaction of interest packets and the occupancy of PIT	NDN	IFA	High	Low	Middle	High	All routing nodes in the network
Paper[7]	Network throughput	NDN	CIFA	High	High	High	High	All routing nodes in the network
Paper[8]	Satisfaction of interest packets	NDN	IFA	High	Low	High	High	All routing nodes in the network
Paper[11]	The name of the interest packets	NDN	IFA	High	Low	High	High	All routing nodes in the network
Paper[12]	The mixture of features	TCP/IP	LDOS	Low	Low	High	Middle	Victimized routing node
Paper[15]	Spectrum Features	TCP/IP	LDOS	High	Low	Middle	Low	Victimized routing node
Paper[14]	Network throughput	TCP/IP	LDOS	Middle	Middle	High	High	All routing nodes in the network
Detection scheme in this paper	Network throughput	NDN	CIFA	High	Low	High	Low	Modular deployment

there is LDoS attack in the network. Kwok *et al.* [12] proposed a detection method HAWK. By observing the number of high-speed pulses in the sampling time, if it exceeds the set threshold, it is judged that there is an attack in the network. Xiang *et al.* [13] generalized entropy and information distance were calculated to distinguish normal traffic and LDoS attack traffic, so as to judge whether attacks occurred in the network. Yuhei *et al.* [14] proposed a method to detect DoS attacks by using the router's function of fast matching. It is proved that the duration of burst attack traffic can be used as distinguishing feature between normal traffic and LDoS attack traffic.

The frequency-domain feature based method is mainly combined with signal processing technology. Through frequency domain transformation of the time series to deal with the acquired characteristics of the frequency domain, so as to achieve the detection and filtering of the LDoS attack traffic. Paul *et al.* [15] analyzed the spectrum characteristics of LDoS attack traffic based on fisher's statistical test and siegel's statistical test, showing that the siegel's statistical test can identify low-rate denial of service attacks more effectively when there are multiple complex LDoS attack pulses.

The method based on correlation detection is mainly aimed at a series of network characteristics after the network is attacked by LDoS. Wei *et al.* [16] detected DDoS attacks by calculating Pearson correlation coefficients between different flows and setting the detection threshold. The current detection methods are basically to detect the hidden LDoS attack traffic from the complex background traffic. For CIFA in NDN, the mechanism of period attack pulse is like the LDoS attack mode in TCP/IP. We can draw on the analysis of the characteristics of LDoS attacks to detect CIFA attacks. Take the current mainstream and typical algorithms as examples to summarize. The comparison results are shown in Table 1.

Combined with the above analysis, the problems existing in the traditional research on detection and defense of CIFA mainly include the following aspects:(1) the detection granularity is relatively coarse. The current research cannot distinguish between malicious interest packets and legal interest packets;(2) unreasonable feature extraction. The current defense strategy is only based on the satisfaction of the interest packets or the size of the PIT, which lacks sufficient detection basis to distinguish attack traffic of CIFAs hidden in the background traffic. It is easy to confuse malicious interest packets with burst traffic; (3) destructive to the performance of NDN architecture. At present, most of the prevention schemes are deployed in the NDN network architecture, which is easy to cause false interception of the original legitimate interest packets and affect the performance of NDN network [17]. Aiming at the existing problems in detecting CIFA attacks, we propose a new detection method based on prediction error to identify CIFA. The frequency domain of CIFA is transformed by the multi-typing of network traffic, then the frequency domain characteristics are detected by the prediction error between particle filter and one-step prediction. Experiments demonstrate that the proposed approach can not only distinguish the abnormal traffic well, but also deploy the detection method modularly in the NDN network, which will not destroy the original NDN network architecture and improve the network processing capacity and efficiency.

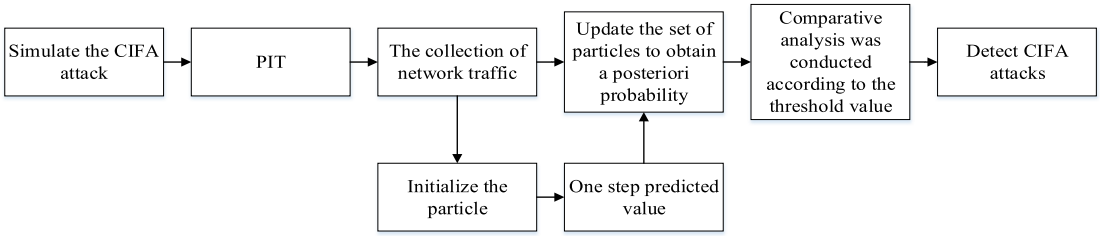


FIGURE 1. Flow chart of CIFA detection based on prediction error.

III. AN ATTACK DETECTION METHOD BASED ON PREDICTION ERROR

Network traffic data is a kind of time series. Traditional traffic analysis is based on linear model. In a large network topology, due to the complexity of its own network behavior and topology structure, the network traffic presents strong nonlinearity. NDN retains the "thin waist" structure of traditional TCP/IP network, so the multi-typing feature is also applicable to NDN.NDN network traffic will show different characteristics in the time-frequency domain. This paper uses this feature to extract CIFAs easily hidden in the background traffic in the frequency domain and detect CIFAs through the frequency-domain features. The specific detection scheme is shown in Fig.1.

In Fig.1, the specific program steps for detecting CIFA based on particle filter are as follows: 1) collect the normal flow of NDN network, and obtain the prior probability of the predicted value of one step after the particle initialization;2) collect the NDN network traffic after CIFA attack, update the particle set and obtain the posterior probability through particle filtering algorithm;3) compare the difference value between the one-step prediction value containing the previous stream and the latest observation value obtained by the particle filter with the set threshold. The CIFA is detected by the comparison result.

A. CIFAs TRAFFIC ANALYSIS

CIFA is very different from traditional IFA attacks and has malicious effect on the network by sending periodic pulsed data streams, usually represented by triplet $A(T, L, R)$. As shown in the Fig.2, where T represents the period of CIFA attack, L represents the time interval of the colluding interest packets sent by the malicious attacker within the attack period and R represents the number of colluding interest packets sent by the attacker within the period L. The average attack rate can be expressed as $R * (L/T)$. The average rate of attackers in CIFA is less than or equal to the rate of legitimate users sending interest packets. This attack method greatly improves the concealment of CIFA attacks.

Fig.2 shows that when the attacker launches CIFA attack, each attacker in the upstream link sends colluding interest packets with a smaller pulse. With the help of a colluding server, the colluding interest packets sent by multiple attackers converge on Node D. At this point, the PIT entries

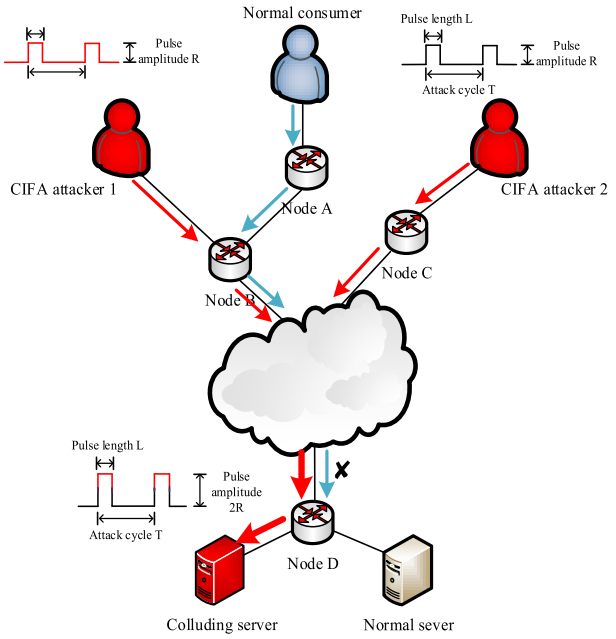
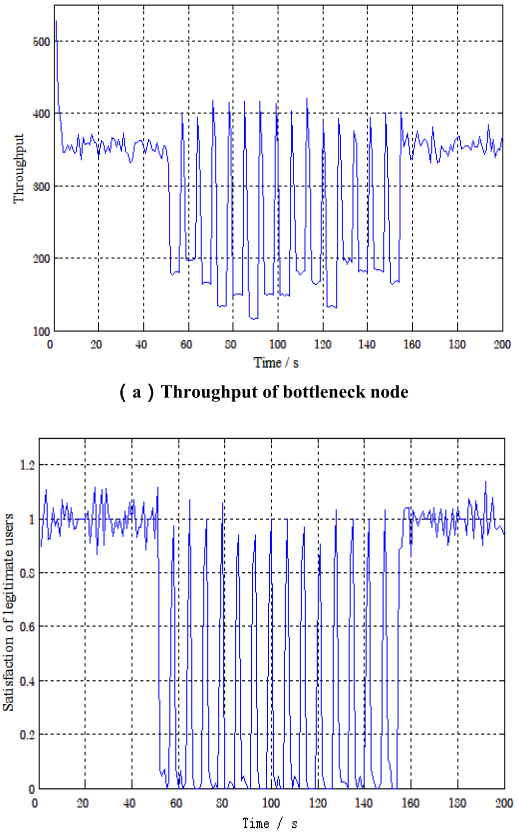


FIGURE 2. The attack scenario of CIFA.

generated by the colluding interest packets fill up the PIT in Node D, causing subsequent legitimate interest packets to be discarded. Because the NDN architecture weakens the concept of addresses, each malicious attack network traffic is well hidden in the legitimate data stream and the response is delayed with the assistance of the colluding server. However, the colluding interest packets of multiple attackers will intermittently cause abnormal network traffic of the downstream link. This paper takes this as the main evidence to detect CIFAs.

In order to detect CIFAs, the abnormal mutation of network traffic caused by the attacks in normal network environment should be studied in the first place, so as to extract the characteristics of abnormal network traffic. CIFAs are mainly caused by attackers sending seemingly legitimate interest packets that occupy limited PIT resources in intermediate routing nodes. Therefore, when this type of attack is launched, the "one-to-one" flow balance between interest packets and data packets will be seriously damaged, thus greatly affecting the routing node's ability to forward interest

packets. Experimentally found that CIFAs has the greatest impact on the routing node of bottleneck link. Therefore, the process of CIFA to attack bottleneck routing nodes to forward interest packets was analyzed and the simulation experiment was carried out in the tree topology. There are 12 legitimate users and 4 malicious users. Inject CIFAs between the 50s and the 150s.The PIT size of the intermediate route node is 200 PIT entries. The attack parameter is set as = (6s, 1s, 50) and the statistical time is 200s.Data were counted at sampling interval of 1s. The packet forwarding volume of the bottleneck node and the satisfaction of legitimate users are shown in Fig.3 below.



(a) Throughput of bottleneck node

(b) Satisfaction of legitimate users

FIGURE 3. Throughput of bottleneck node and satisfaction of legitimate users.

As shown in Fig.3. When no CIFA was launched (0-50s), the throughput of the bottleneck routing node was maintained at a stable value. The satisfaction of legitimate users was maintained at 100% on average. When CIFA attack occurs (50s-150s), the throughput shows a step-down decline, as does the satisfaction of legitimate users. In severe cases, the satisfaction drops to 0, which means that all legitimate users' interest packets are discarded. After the attack stopped (150s-200s), it quickly returned to normal. Compared with normal network environment, the network throughput was reduced by 41.5% when the attack occurred and 75.8% of the legitimate interest packets were discarded, which indicates the seriousness of CIFAs. CIFA is a new type of intelligent attack with intermittent and high concealment. The impact of CIFA on throughput and the satisfaction of interest packets has certain characteristics. The PIT entries generated by the malicious attacker sending colluding interest packets need to occupied in the intermediate routing node for a long time before the colluding server replies. When all colluding interest packets are satisfied, the next round of attack continues. Meanwhile, the PIT of intermediate routing node will not be overloaded instantly and the legitimate server will meet the legitimate interest packets in a short time before the next round of attack. In order to achieve the best attack effect of CIFA, the time of delayed gratification of colluding interest packets should be close to the normal survival time of interest packets. Based on this feature, the extracted traffic is filtered and the filtered results are shown in Fig. 4.

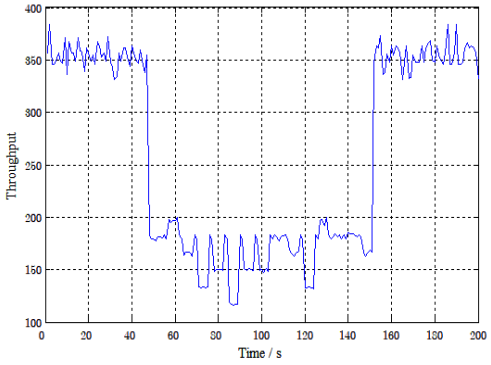


FIGURE 4. Characteristics of network traffic.

In Fig.4, we filter the traffic in the congestion phase caused by the CIFA from the beginning of the attack. In this way, the network false normal stage caused by CIFA is weakened and the network traffic shows the most serious state caused by CIFA. In the actual network, the routing node filters out the traffic with normal throughput at the beginning of the attack, so the overall throughput is at a low level (within the range of 100-200). This traffic is finally used as the input for particle filter detection.

B. THE PREDICTION ERROR DETECTION APPROACH

In this paper, the error value $\xi_{t+1} = |\hat{X}_{t+1|t} - \hat{X}_{t+1|t+1}|$ of one-step prediction and optimal estimation based on the particle filter algorithm is used as the basis for detecting abnormal network traffic. $\hat{X}_{t+1|t}$ can only be obtained by the state at time t and the historical network traffic, while the estimation of $\hat{X}_{t+1|t+1}$ also uses the state information at time $t + 1$. When the network state is abnormal, there will be a big error between the estimated value and the predicted value. The network state can be detected in real time by setting the threshold value. Since the beginning and end of the attack will cause sudden changes in the network traffic, the error at the beginning and end of the attack is large. In this way, CIFA attacks can be detected quickly and corresponding measures

can be taken in a timely manner to further deteriorate the network environment.

The "thin waist" model of NDN makes it exhibit the multi-fractal characteristics consistent with TCP/IP networks. Since the network environment is a nonlinear system, the noise distribution is non-gaussian. Therefore, particle filter algorithm can eliminate noise interference compared with other filtering algorithms, accurately analyze the cross-correlation model and have more accurate detection effect [18]. This section mainly takes the frequency domain signal in 3.2 as the observed value, and uses the particle filter algorithm for estimation. CIFAs can be detected in real time by comparing the error value of one-step predicted value and estimated value with the set threshold value.

According to the NDN network characteristics and CIFA model, the specific steps of detecting CIFA based on particle filter are as follows:

1. Initializes particles and c ($t = 0$):

$$x_o(i) \sim p(x_o), \quad i = 1, 2, \ldots, N, \ w(x_o(i)) = 1/N \tag{1}$$

2. Prediction of state:
   According to the filtering process in the state space (the normal collection and filtering process of NDN network traffic), the prediction is made, $x_k(i) \sim p(x_k|x_{0:k-1}(i)), i = 1, 2, \ldots, N$ and then get a new set of particles $x_{0:k}(i) = \{x_k(i), x_{0:k-1}(i)\}, i = 1, 2, \ldots, N$, calculate the further predicted value at time k:

$$x_{k|0:k} = \sum_{i=1}^{N} v_k(x_{0:k-1}(i))x_{k|0:k}(i) \tag{2}$$

   where $v_k(x_{0:k-1}(i))$ is the normalized weight at time $k-1$.
3. Status update: calculate the new sample weight;
   According to the latest observed values, the weight $w_k(x_{0:k}(i))$ of the new sample is calculated by using the probability density of importance:

$$w_k(x_{0:k}(i)) = w_k - 1(x_{0:k-1}(i))\frac{p(y_k|x_k(i))p(x_k|x_{k-1}(i))}{q(x_{k|x_{k-1}}(i), y_{1:k})} \tag{3}$$

4. Data update:
   The estimated value of NDN network traffic is obtained according to the posterior probability. However, when calculating the best estimated value of network traffic, the variance of sample weight shall be considered to increase gradually with the increase of the number of iterations. This will lead to particle deletion. This problem can be solved by resampling. The main idea is to suppress or eliminate lightweight particles and to obtain a new particle set $\{\hat{x}_{k|0:k}(i), 1/N\}_{i=1}^{N}$ by high-power value replication of heavyweight particles. The estimated value of NDN network traffic state after filtering at moment K is calculated as:

$$\hat{x}_{k|k} = \sum_{i=1}^{N} w_k(x_k(i))x_k(i) \tag{4}$$

5. Result analysis:
   According to the best estimate, the difference between one-step prediction and the estimated flow value after NDN filtering can be obtained as:

$$w_k = |x_{k|0:k} - \hat{x}_{k|0:k}| \tag{5}$$

6. Return state prediction and continue a new detection cycle.

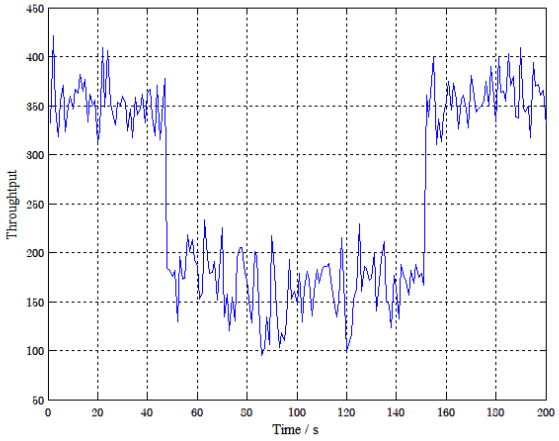
The particles in the particle filter algorithm represent the state distribution information of the sample. The selection of the number of particles is an important factor affecting the filtering effect. The throughput after sampling is taken as input data. The filtering effect of different particle numbers is shown in the Fig.5.

Fig.5 shows that the greater the number of particles selected, the better the estimation effect. However, its drawback is that it will lead to excessive computation of network resources and further increase of network resource consumption [19]. If the number of particles is too few, the state distribution information of the sample cannot be accurately represented. Therefore, the final experimental results prove that the estimation effect of particle number 100 is basically the same as that of particle number 500 by setting different particle Numbers. Considering the filtering effect and resource loss, this paper selects 100 particles to estimate and detect the throughput of network bottleneck nodes in NDN.

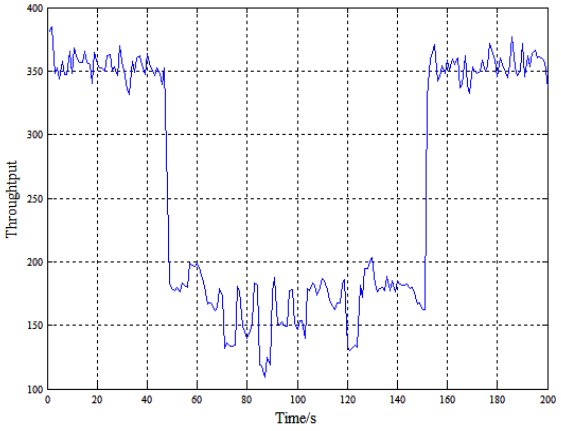
In the Section 3, we first introduce CIFA features. According to the characteristics in NDN, a new detecting CIFA method is proposed. In terms of the particularity of CIFA features, the number of particles is tested and preliminary experimental results is obtained.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

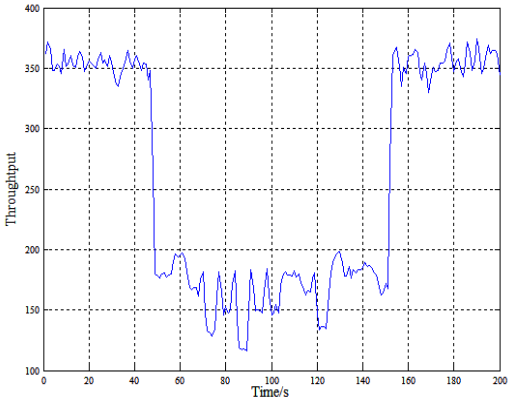
In this section, two NDN topologies are built to test the detection performance of the proposed detection approach. Through comparative analysis with other methods, the relevant detection performance indicators are obtained. The open source platform used in the experiment in this paper is ndnSIM, which realizes the relevant functional structure of NDN architecture in ns-3 network simulator and can run various network topologies and scene simulation. Using the design threshold of hypothesis test, the experiment is carried out in two kinds of network topologies with different sizes. It is proved that the method proposed in this paper can detect this type of attack well and has a good effect by simulating CIFA in different experimental environments. Finally, the detection algorithm is compared with the detection algorithm in the paper [7], which proves the high efficiency of the detection algorithm in this paper.



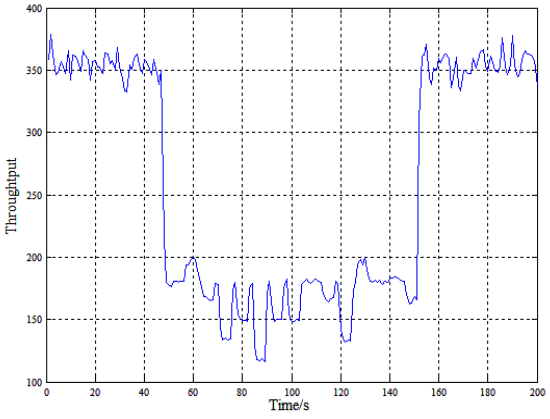
(a) The number of particles selected is 1



(b) The number of particles selected is 10



(c) The number of particles selected is 100



(d) The number of particles selected is 500

FIGURE 5. Filtering effect with different number of particles.

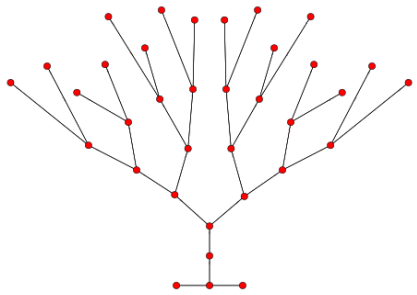
A. EXPERIMENTAL ENVIRONMENT

In order to further explore the detection capability of the scheme under different network traffic scale and network traffic jitter caused by attacks. The simulation is carried out in a binary tree network topology and an ISP-like topology. We use a binary tree topology as it represents one of the worst cases to defend against DDoS attacks. The larger ISP topology reflects how our detection methods would perform when deployed on the real internet [8]. The large ISP topology is based on a modified version of the AT&T topology in Rocketfuel [20].

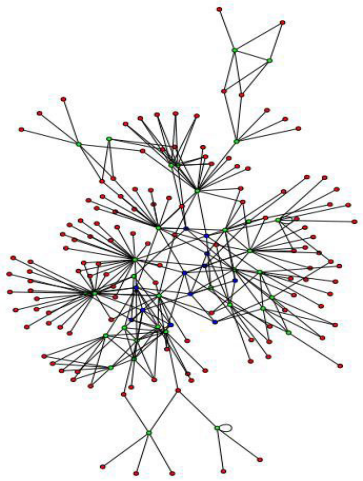
In the network topology of binary tree, the topological node is composed of 34 nodes, including 16 user nodes, 8 gateway nodes and 6 backbone nodes. In the large ISP topology, the topology node consists of 130 user nodes, 33 gateway nodes and 13 backbone nodes. Its experimental topology is shown in Fig. 6.

The experiment assumes that legitimate users send interest packets at a constant average rate. The random time interval between two continuously sent interest packets provides a reasonable approximation for the traffic model for all users. The content distribution of each legitimate user's request satisfies Zipf-Mandelbort distribution. In this traffic mode, the traffic pattern can provide a reasonable approximation of the traffic mix from all network users without excessive buffering. The distribution of each attacker follows uniform distribution [21], [22]. To quantify the worst-case behavior of our mitigation strategy, the cache cannot satisfy any interest packets (including legitimate interest packets).

The number of attackers should be in the minority in the network [6], [7] and the ratio of 3:1 can ensure that the attackers could be evenly distributed in various parts of the network to launch the most serious CIFA attack with the least network resources. In the experiment, 25% of user nodes were randomly selected as attackers and two backbone nodes were designated as legitimate server and colluding server in the binary tree network topology. In the large ISP network topology, 25% of user nodes are also selected as attackers, two backbone nodes are randomly selected as legitimate server and colluding server. As shown in Fig.7. When the PIT capacity is set to 200, the average occupancy rate of routing nodes in the entire network will not exceed 20% under the



(a) Binary tree topology



(b)AT&T topology

FIGURE 6. Experimental topology.

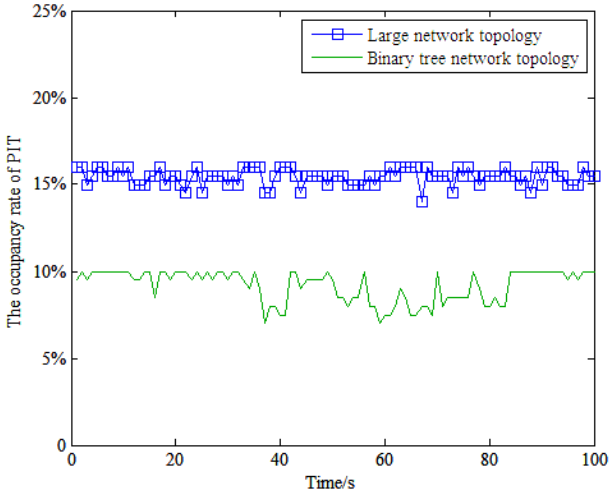


FIGURE 7. The occupancy of PIT in normal network state.

normal state of the network. It can ensure that the requests of legitimate users in the entire network are satisfied.

In this paper, the changes of normal interest packets in the whole network after the network is attacked are counted. As shown in Fig.8.

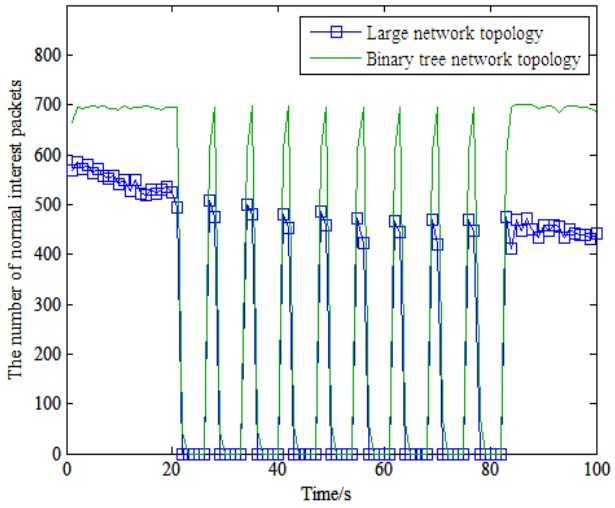


FIGURE 8. The number of normal interest packets.

When CIFA attack occurs, the PIT space of a large number of nodes in the network is occupied by PIT items generated by the colluding interest packets, resulting in the subsequent legitimate interest packets being discarded. The number of legitimate interest packets in the network has been greatly reduced.

The specific setup of the experiment is shown in Table 2.

TABLE 2. Specific parameter value.

Parametric Description	Value
PIT size	200
Survival time of interest packets	5s
Data Packet size (Byte)	1100
Rate of interest packets sent by legitimate users (binary tree)	10/s
Rate of interest packets sent by malicious users (binary tree)	8/s
Rate of interest packets sent by legitimate users (binary tree)	15/s
Rate of interest packets sent by malicious users (binary tree)	10/s
Request prefix for legitimate users	/good/Names::FindName (*node)/…
Request prefix for malicious users	/evil/Names::FindName (*node)/…
The reply prefix for normal server	/good/…
The reply prefix for colluding server	/evil/…
Simulated time	200s
Activity time for legitimate users	0-200s
Activity time for malicious users	50s-150s
Threshold	0.5

B. ANALYSIS OF TEST RESULTS

The link bandwidth in the topological environment in this article is set high enough to avoid interest packet and data

packets loss due to insufficient bandwidth. The link delay is set to low to prevent the PIT entries generated by legitimate interest packets from expiring due to high link delay, thereby affecting the accuracy of the attack effect. In binary tree network topology, the network latency is 80ms and the bandwidth of each link is 10Mbps. The random propagation delay fluctuates between 1-10ms, randomly assigned by 4 malicious users and 12 legitimate users. The root node sets up the legitimate producer and the collusive producer respectively. Malicious attackers launch attacks from the 50s and stop at 150s.After frequency domain transformation, the collected data are subject to one-step prediction and particle filter estimation. The output results are shown in Fig.9.

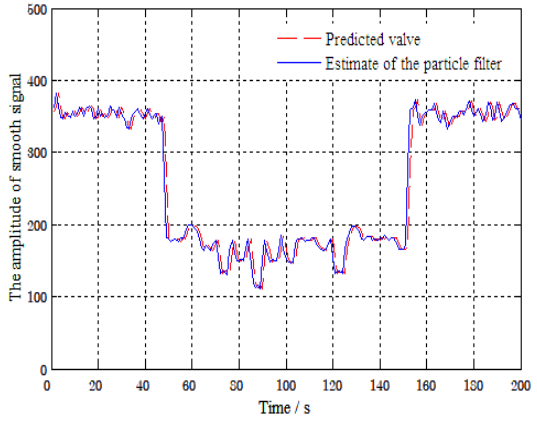


FIGURE 9. Prediction and particle filter estimation.

In Fig.9, the solid line is the result of particle filter estimation. The dotted line is the result of further prediction. In order to express the errors of the two more clearly, normalization is carried out [23]. The relative error results are shown in Fig. 10

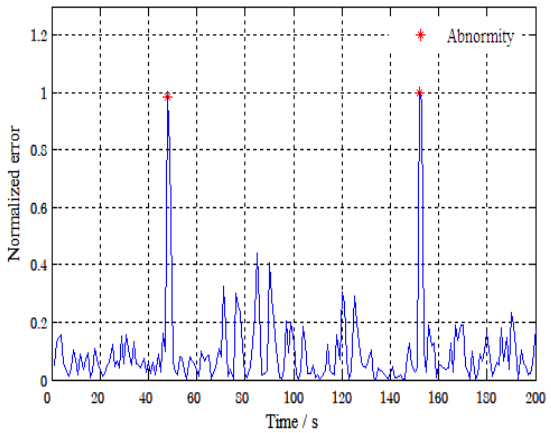


FIGURE 10. Relative error value.

As can be seen from Fig.10, there is a large difference between the one-step prediction value and the particle filter estimation value at the time of attack (the 50s) and the end (the 150s). The normalized error in the attack duration stage is significantly higher than that in the non-attack stage, which indicates that CIFAs will cause large fluctuations in the normal network. The detection of CIFAs can be achieved by the difference value between one-step prediction and particle filtering.

CIFA was first proposed in paper [7] and a detection scheme based on wavelet analysis was discussed. The detection method based on wavelet analysis can detect the existence of CIFA attack by detecting network traffic. The detection scheme can detect CIFA attack in real time by network anomaly caused by each attack pulse. When the detected index exceeds the set threshold, the network is considered to be attacked. This article reproduces it and its detection effect is the same as that in the paper [7]. As shown in Fig.11, attackers generate attacks in the 50s and launch the second round of attack in the 130s. If the detection threshold is set too high, the attacks will result in missed judgments. If the detection threshold is set too low, when there is no attack in the network, misjudgment may occur.

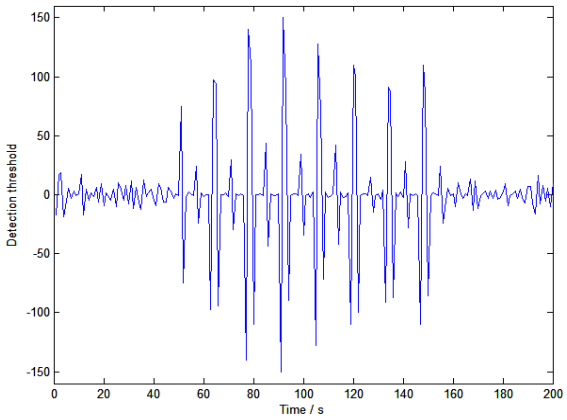


FIGURE 11. Detection algorithm based on wavelet analysis in binary tree topology.

The detection algorithm was tested in a larger network topology. According to the same proportion as in the small binary tree network, malicious consumers and consumers are randomly assigned (malicious users account for 25% of the total user nodes). The delay time is set to 330ms.Other experimental parameters are the same as above. The throughput of the bottleneck node varies over time as shown in Fig.12.

As can be seen from Fig.12, the throughput of the bottleneck node is relatively stable before the attack starts. Starting from the time of the attack, the throughput jitter is strong and the network presents an unstable state. At this time, it is difficult for legitimate users to obtain requested data packets. The throughput of legitimate users is sampled and filtered to get the throughput shown in Fig.13.

The throughput of legitimate users decreases obviously when each attack pulse is launched. This shows that this attack has a great impact on legitimate users. The sampling characteristics can clearly show the influence of CIFA on network state. The sample value is used as input to

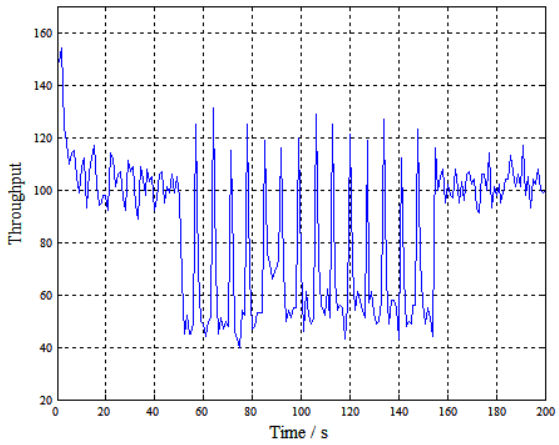


FIGURE 12. Bottleneck throughput.

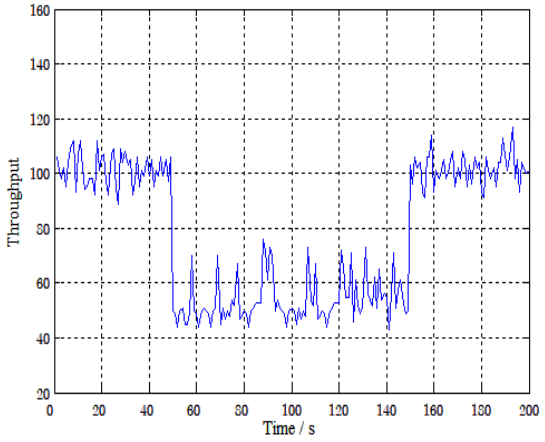


FIGURE 13. Sampling filter value.

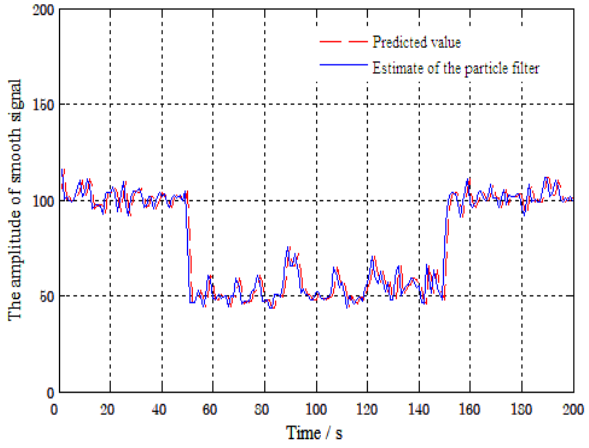


FIGURE 14. Prediction and particle filter estimation.

obtain one-step prediction and particle filter estimation values, as shown in Fig.14.

Fig.14 shows the estimation results of the predicted value and the particle filter value in the large network topology environment. The solid line is the estimated value and the dashed line is the predicted value. The one-step estimate of NDN throughput includes only previous network throughput information, the particle filter estimate of network throughput includes the latest observed data information. Therefore, when the network traffic appears abnormal mutation, the one-step predicted value of throughput and the estimated value of particle filter will have a large error. In order to show the error more obviously, the error is normalized. The corresponding normalized error statistical is further obtained, as shown in Fig.15. The attack took place in the 50s and lasted until the end of the 150s.Similar to the topology theory analysis of small networks, the network will show obvious instability after receiving CIFA attack. This shows that CIFAs have strong attack efficiency against large networks, and the detection method of particle filter can detect CIFAs well.

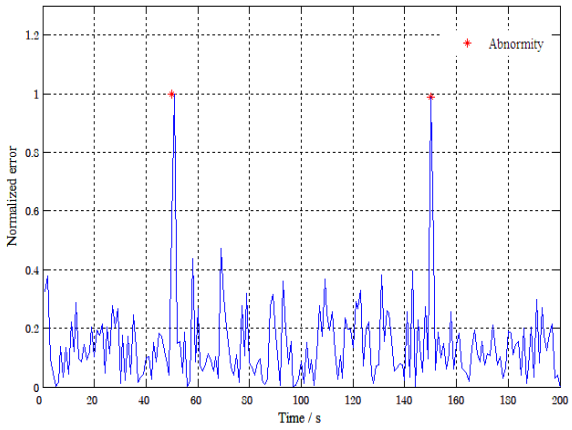


FIGURE 15. Relative error value.

However, the detection algorithm based on wavelet exposes more disadvantages for large network topologies. As can be seen from Fig.16. Facing the more massive and complex network traffic in large networks. The detection scheme based on wavelet analysis greatly reduces the accuracy of each attack pulse.

The detection algorithm has been unable to detect CIFAs in time. CIFA is generated from the 50s. When we set the detection threshold to 10, the detection algorithm can detect the first attack pulse of CIFA. But when the network is in normal state. This detection algorithm will produce very serious misjudgment. In order to verify the accuracy of the algorithm in this paper, different thresholds are set to compare the detection effect of the algorithm. The detection results of the particle filter algorithm in this paper are shown in table 3 and table 4. The rate of false detection is equal to the number of normal samples wrongly reported as abnormal divided by the total number of normal samples. The detection rate is equal to the number of detected exceptions divided by the total number of abnormal samples. The Missed detection rate is equal to the number of undetected exceptions divided by the total number of abnormal samples.

TABLE 3. The detection effect based on particle filter in small network topology.

Indicators	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
Detection rate	73.6%	87.2%	90.4%	97.4%	98.0%	97.8%	98.5%	100%
False alarm rate	1.2%	2.4%	3.5%	3.1%	2.2%	10.2%	16.8%	26.3%
Missed detection rate	26.4%	12.8%	9.6%	2.6%	2.0%	2.2%	1.5%	0%

TABLE 4. The detection effect based on particle filter in large network topology.

Indicators	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
Detection rate	8.0%	32.3%	89.3%	98.0%	98.5%	98.2%	99.3%	100%
False alarm rate	2.2%	2.1%	4.3%	6%	3.1%	14.6%	25.1%	33.3%
Missed detection rate	92.0%	67.7%	10.7%	2.0%	1.5%	1.8%	0.7%	0.0%

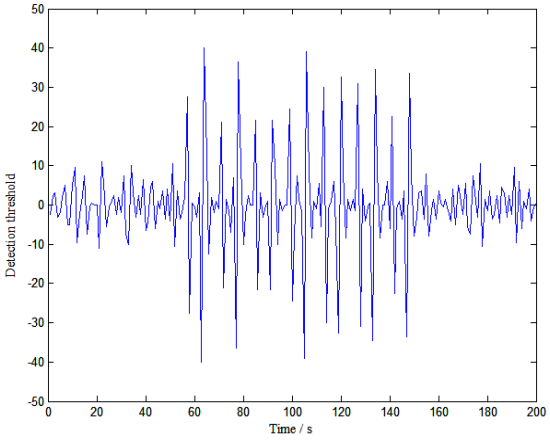


FIGURE 16. Detection algorithm based on wavelet analysis in large topology.

Table 3 and table 4 represent the detection results in the small binary tree topology and AT&T topology respectively. It can be seen from the table that if the threshold is too low, it will seriously affect the detection rate and cause the false alarm rate to increase. When the threshold value is large, the false alarm rate decreases, but the detection rate also decreases, affecting the detection performance. Therefore, the selection of the optimal threshold is a key factor affecting the detection effect [24]. Through the experimental analysis, the threshold value of 0.5 can be selected to optimize the detection performance. At the same time, this detection method can more accurately detect the time of the beginning and the end of the attack by properly designing the threshold. The error between the detection time of the beginning and the end of the attack and the actual situation is no more than 0.1s, which can better cooperate with the subsequent defense strategy to resist CIFA attack. In this part, the prediction error detection method is compared with wavelet analysis [7], Poseidon [6] and Satisfaction-based pushbasck method [8]. The above detection schemes were deployed on the ndnSIM platform and the average values of relevant indicators were calculated through 10 experiments. The performance of each detection method is comprehensively analyzed form three aspects: detection rate, false alarm rate and missed detection rate. The performance comparison of each detection scheme is showed in table.5.

TABLE 5. The performance comparison of various detection schemes.

Detection method	Detection rate	False alarm rate	Missed detection rate
Based on wavelet analysis	90%	36%	10%
Poseidon	1.2%	6.7%	98.8%
Satisfaction-based pushback	10.7%	3.5%	89.3%
Detection scheme in this paper	98.5%	3.1%	1.5%

It can be seen from table 5. Among them, Poseidon and Satisfaction-based pushback are detection schemes to detect IFA-type attacks, whose detection characteristics cannot sensitively detect the abnormal changes caused by CIFA attacks on the network, resulting in a low detection rate. The detection scheme based on wavelet analysis has certain detection rate, but the corresponding error detection rate is also very high. The reason is that the attack mode of CIFA belongs to periodic pulse mode, so the scheme based on wavelet analysis cannot detect each attack pulse sensitively in a short time. The detection method proposed in this paper can obtain a higher detection rate. At the same time the false alarm rate and the missed alarm rate are also relatively low. Therefore, the proposed method has greater advantages in detection rate and false alarm rate and has higher detection performance for CIFA compared with other methods.

V. CONCLUSION

In this paper, a new detection method for CIFA in NDN is proposed. The approach is deployed in the bottleneck routing node and detects the subtle changes in network traffic in the overall network topology when the attack occurs. Compared with other methods, the proposed method has a higher detection rate and a lower false alarm rate. **The main contributions of the detecion method for CIFA can be summarized as 3 points:**(1) An efficient CIFA detection algorithm based on particle filter is proposed, and the detection algorithm is deployed to the bottleneck router interface to detect network traffic in real time. During an attack, throughput changes sensitively when malicious traffic disrupts the stability of network traffic. Therefore, the algorithm can detect the start and end of the attack in time, with an error of no more than 100ms. (2) The detection scheme of colluding benefit flood attack is implemented in ndnSIM. The detection scheme does

not need to acquire a large number of attack features for a long time, and can be detected during the attack, with good real-time performance. At the same time, the detection mechanism is an independent detection module, which does not affect the forwarding mechanism within NDN and the transmission state within NDN. (3) Experimental results show that, compared with the existing detection scheme, the detection scheme has a higher detection rate and a lower false alarm rate. At the same time, this detection approach only needs to be deployed on the route node of the closest downstream server, which can better reduce the actual cost. The proposed approach can accurately reflect the time when the attacker starts the attack and closes the attack, so the corresponding defense strategy can be implemented in a timely manner to prevent the bad effects of the attack from further worsening. The prediction error detection approach for CIFA can help to design a secure and efficient NDN routing and forwarding strategy.

The proposed approach can detect CIFA attacks without changing the internal forwarding mechanism in NDN through modular deployment. However, the scope of the discussion in the paper is limited to modular detection, but no corresponding to modular defensive measures. In future research work, we will continue our research on modular defense to CIFA attacks in NDN. Inspired by the proposed methods, attack detection for NDN networks can be modeled as a classification problem that distinguishes between ''Normal'' and ''Abnormal'' states of interest packets. Select appropriate classification features to abstract the interest packets into feature vectors. Each feature vector is given mark {normal, abnormal}. The two marks represent normal interest packets and malicious interest packets respectively. The classification algorithm can be chosen to learn the sample and the machine learning classifier can be established to detect the unlabeled samples. By limiting the forwarding of malicious interest packets identified by the classifier, the CIFA attacks can be defended Therefore, the combination of NDN defense and machine learning is the focus of our research. Such methods not only take advantage of machine learning algorithms, but also can be modularly deployed at the edge of NDN routing nodes without occupying internal space.

REFERENCES

[1] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. C. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang ''Named data networking,'' *SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, Jul. 2014.

[2] 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, Jul. 2014.

[3] J. Tang , H. Zhou, and Y. Liu, ''Method of flood prevention of interest packet based on prefix recognition under content-centered network,'' *J. Electron. Inf.*, vol. 36, no. 7, pp. 1735–1742, Jul. 2014.

[4] P. Gasti *et al.*, ''DoS & DDoS in named-data networking,'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, pp. 66–73, Aug. 2012, doi: 10.1109/ICCCN.2013.6614127.

[5] K. Wang, J. Chen, H. Zhou, Y. Qin, and H. Zhang, ''Modeling denial-of-service against pending interest table in named data networking,'' *Int. J. Commun. Syst.*, vol. 27, no. 12, pp. 4355–4368, Dec. 2014.

[6] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, ''Poseidon: Mitigating interest flooding DDoS attacks in named data networking,'' presented at the Local Comput. Netw., Aug. 2013.

[7] 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.*, Baltimore, MD, USA, Oct. 2017, p. 557.

[8] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, ''Interest flooding attack and countermeasures in named data networking,'' in *Proc. IFIP Netw. Conf.*, Brooklyn, NY, USA, May 2013, pp. 1–9.

[9] K. Ding, Y. Liu, H.-H. Cho, H.-C. Chao, and T. K. Shih, ''Cooperative detection and protection for interest flooding attacks in named data networking,'' *Int. J. Commun. Syst.*, vol. 29, no. 13, pp. 1968–1980, Sep. 2016, doi: 10.1002/dac.2883.

[10] R. Hou, M. Han, J. Chen, W. Hu, X. Tan, J. Luo, and M. Ma, ''Theil-based countermeasure against interest flooding attacks for named data networks,'' *IEEE Netw.*, vol. 33, no. 3, pp. 116–121, May/Jun. 2019.

[11] 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.

[12] Y.-K. Kwok, R. Tripathi, Y. Chen, and K. Hwang, ''HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks,'' in *Proc. Int. Conf. Netw. Mobile Comput.*, Aug. 2005, pp. 423–432.

[13] Y. Xiang, K. Li, and W. Zhou, ''Low-rate DDoS attacks detection and traceback by using new information metrics,'' *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 426–437, Jun. 2011.

[14] Y. Hayashi, J. Y. Zhen, S. Nishiyama, and A. Misawa, ''Method for detecting low-rate attacks on basis of burst-state duration using quick packet-matching function,'' in *Proc. IEEE Int. Symp. Local Metrop. Area Netw.*, Jul. 2017, pp. 1–2.

[15] C. Paul, K. Myong, and V. Alexander, ''Spectral analysis of low rate of denial of service attacks detection based on Fisher and Siegel tests,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2016, pp. 1–6.

[16] W. Wei, F. Chen, Y. Xia, and G. Jin, ''A rank correlation based detection against distributed reflection DoS attacks,'' *IEEE Commun. Lett.*, vol. 17, no. 1, pp. 173–175, Jan. 2013.

[17] Y. Li *et al.*, ''Overview of DoS attack in content center network,'' *J. Cyber Secur.*, vol. 2, no. 1, pp. 92–108, Jan. 2017, doi: 10.19363/j.cnki.cn10-1380/tn.2017.01.007.

[18] W. Li, Z. Wang, Y. Yuan, and L. Guo, ''Particle filtering with applications in networked systems: A survey,'' *Complex Intell. Syst.*, vol. 2, no. 4, pp. 293–315, Oct. 2016.

[19] J. Ren, L. Li, and S. Wang, ''DoS attack modeling and analysis for name resolution system in content center network,'' *Comput. Appl. Res.*, vol. 33, no. 2, pp. 495–497, Feb. 2016.

[20] N. Spring, R. Mahajan, and D. Wetherall, ''Measuring ISP topologies with Rocketfuel,'' *ACM SIGCOMM Comput. Commun. Rev.*, vol. 32, no. 4, pp. 133–145, 2002.

[21] L. Qi, H. Huang, F. Li, R. Malekian, and R. Wang, ''A novel shilling attack detection model based on particle filter and gravitation,'' *China Commun.*, vol. 10, pp. 112–132, Oct. 2019.

[22] C. Yang, Y. Z. Zhang, and Z. S. Pang, ''Network traffic monitoring techniques and analysis of performances,'' *J. Air Force Univ. Eng., Natural Sci.*, vol. 4, no. 1, pp. 57–60, Feb. 2003.

[23] Y. Li, J. Dong, Z. Shang, and Y. Wang, ''Network traffic monitoring technology and performance,'' *Electron. Technol. Softw. Eng.*, vol. 143, no. 22, p. 3, Aug. 2018.

[24] Z. J. Wu, L. Liu, and M. Yue, ''Detection method of LDoS attacks based on combination of ANN & KPCA,'' *J. Commun.*, vol. 39, no. 5, pp. 11–22, May 2018.

LIANG LIU received the master's degree in communication and information system from the Civil Aviation University of China. He currently works as an Assistant Experimenter with the School of Electronic Information and Automation, Civil Aviation University of China. His main research interests include network information security, including defense of future network security and denial of service attacks.

WENZHI FENG is currently pursuing the master's degree in information security with the Civil Aviation University of China. His research interest includes security of named data networking.

MENG YUE received the Ph.D. degree in information and communication engineering from Tianjin University, China, in 2017. He is currently an Associate Professor with the School of Electronics and Information Engineering and Automation, Civil Aviation University of China. His current research interests include information security and cloud computing.

ZHIJUN WU received the B.S. and M.S. degrees in information processing from Xidian University, China, and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, China. He was a Professor with the Department of Communication Engineering, Civil Aviation University of China. His research interests include denial-of-service attacks and security in big data and cloud computing.

RUDAN ZHANG is currently pursuing the master's degree in information security with the Civil Aviation University of China. Her research interest includes security of named data networking.