Computers, Materials & Continua CMC, vol.64, no.2, pp.1075-1089, 2020

Research on Detection Method of Interest Flooding Attack on Content Centric Network

Yabin Xu[1, 2, 3, *], Ting Xu[3] and Xiaowei Xu[4]

Abstract: To improve the attack detection capability of content centric network (CCN), we propose a detection method of interest flooding attack (IFA) making use of the feature of self-similarity of traffic and the information entropy of content name of interest packet. On the one hand, taking advantage of the characteristics of self-similarity is very sensitive to traffic changes, calculating the Hurst index of the traffic, to identify initial IFA attacks. On the other hand, according to the randomness of user requests, calculating the information entropy of content name of the interest packets, to detect the severity of the IFA attack, is. Finally, based on the above two aspects, we use the bilateral detection method based on non-parametric CUSUM algorithm to judge the possible attack behavior in CCN. The experimental results show that flooding attack detection method proposed for CCN can not only detect the attack behavior at the early stage of attack in CCN, but also is more accurate and effective than other methods.

Keywords: CCN, interest flooding attack, self-similar feature, information entropy, bilateral detection method.

1 Introduction

Content Centric Network (CCN) is a promising technology for the future of the internet. In contrast to traditional TCP/IP network, CCN replaces IP address with content name as the unique identifier for information transmission. Compared with the network attack defense problem [Tian, Ji, Liu et al. (2019)] existing in traditional TCP/IP networks, CCN can eliminate security problems such as source address forgery attack and flood attack targeted at specific hosts in traditional networks. However, CCN introduces new security threats, among which the interest flooding attack (IFA) is the most prominent.

CCN identifies the content and transmits the information through interest packet and data packet in the network. Interest packet is the request and data packet is the response. An

[1] Beijing Key Laboratory of Internet Culture and Digital Dissemination Research, Beijing, 100101, China.

[2] Beijing Advanced Innovation Center for Materials Genome Engineering, Beijing Information Science and Technology University, Beijing, 100101, China.

[3] School of Computer, Beijing Information Science & Technology University, Beijing, 100101, China.

[4] Department of Information Science, University of Arkansas at Little Rock, Little Rock, 72204, USA.

[*] Corresponding Author: Yabin Xu. Email: xyb@bistu.edu.cn.

Received: 22 January 2020; Accepted: 08 April 2020.

Interest packet carries content name that specifies the desired data; the Data packet also encapsulates this name and as the right to satisfy the interest packet. For unsatisfied interest packets, router nodes store the prefix information and the detailed content name information in a pending interest table (PIT), with a PIT entry in the forwarding process, and delete this entry when receive the corresponding Data. The IFA attackers use this feature of CCN to initiate a large number of malicious interest packets, which will exhaust PIT resource and disabled router to receive interest packets requested by legitimator. As a result, CCN faces congestion or even paralysis.

According to the difference of malicious interest packets sent by attacker, the IFA can be divided into two forms: (1) attackers send interest packet which contains fake content name; (2) attackers send real interest packet but non-popular. Both types of IFA can have a certain impact on CCN. If the latter is adopted, attackers need to collect a large amount of unpopular content in advance and guarantee low-rate attacks to ensure that the content will not be cached by the intermediate router, which increasing cost, but the attack effect is not obvious. Therefore, attackers are more likely to take the first form. In this paper, we conduct research on the IFA only aiming at fake content names.

Through further analysis, we find that the IFFA against CCN has the following three characteristics:

(1) The content name prefix of the interest packet sent by the attacker is real, but the rest is forged, so that those interest packets are continuously forwarded on the intermediate router nodes, but will not be satisfied. Thereby expanding the impact on the whole CCN;

(2) The attacker requests the content under the same prefix to ensure that interest packets are forwarded to the same content source. This can cause the greatest harm to the content source and routers along the forwarding path;

(3) The attacker uses a large amount of different content names and avoid duplicate requests, so as to ensure that those interest packets are difficult to implement name aggregation in PIT. Thus, it can occupy PIT to the maximum extent and affect the normal operation of router nodes.

Therefore, there will be a large number of interest packets that are requested once in the CCN when IFA occurs. While a certain interest packet usually be requested more than once under normal circumstances. Because a duplicate request is made when the responding Data packet is not received for legitimator and different legitimators also request the same content.

It can be seen that the IFA attack mechanism and network performance characteristics of CCN are significantly different from the DOS/DDOS in traditional network. Therefore, the attack detection method in traditional network cannot be easily transplanted to the CCN, which brings new challenges for us to detect IFA. To this end, we study the characteristics of IFA, and propose a new detection method which adapted to CCN to promote its healthier and faster development.

The innovations of this paper are as follows:

(1) The self-similarity feature of network traffic is applied to IFA detection of CCN for the first time. Hurst index is used to reflect the slight change of flow in CCN, so as to improve the sensitivity of IFA attack detection and effectively realize the early detection

of IFA attack.

(2) The bilateral detection method based on non-parametric CUSUM algorithm is adopted to detect IFA in CCN, which can not only effectively avoid the misjudgment caused by normal network fluctuation on attack detection, but also improve the effectiveness and accuracy of detection.

2 Related work

Since the introduction of CCN, IFA has received extensive attention from domestic and foreign scholars. The key to IFA detection is how to identify attackers-initiated evil packets and user-initiated normal packets from a large number of interest packets. In the next, we will introduce the current research work based on the categories of attack detection.

Currently, there are three main categories of IFA detection method.

(1) Based on abnormal change of the PIT state after an IFA occurs. This type of method mainly takes the PIT size, the number of PIT entries expired, and the number of PIT entries, and then extracts PIT occupancy rate, interest packet satisfaction ratio, PIT expiration rate and other indicators.

(2) Based on the principle of balance of CCN data streams. This type of method mainly utilizes the fact that whenever an interest packet is sent upstream, at most one packet will be generated for downstream reply [Li, Xin, Han et al. (2017)]. Therefore, the judgment is made by extracting the number of interest packets sent by each exit but not received a response, i.e., pending interest (PI), the number of interest packets per entry, and the number of PI for each namespace.

(3) Based on traffic behavior characteristics. This type of method takes advantage of basic characteristics of traffic itself, and detect attack by extracting information entropy and other indicators.

Afanasyev et al. [Afanasyev, Mahadevan, Moiseenko et al. (2013)] proposed a token bucket mechanism based on interface fairness, an interest packet receiving mechanism based on content acquisition success rate and a reverse feedback mechanism based on content acquisition success rate. These three mechanisms determine whether there is an IFA by comparing the PIT usage ratio and the interest satisfaction ratio with a certain threshold. Lin [Lin (2014)] improved token bucket algorithm in the traditional IP network and used actual physical link capacity of current port as the threshold to detect IFA. When this threshold is exceeded, IFA is considered to occur.

Compagno et al. [Compagno, Conti, Gasti et al. (2013)] calculated the probability value that interest packet was satisfied based on different interfaces of the router, and used it as the indicator to detect IFA. Finally, interest packet admission rate of the corresponding interface of router is dynamically adjusted through the change of this indicator. Dai et al. [Dai, Wang, Fan et al. (2013)] proposed an interest packet backtracking mechanism, which used the number of PIT expired entries as the indicator of detection. It is considered that the current network has an IFA when the number exceeds the threshold. Wang et al. [Wang, Zhou, Luo et al. (2014)] proposed a strategy named TDM, which counted the number of timeout interest packets corresponding to each name prefix and compared with the threshold to determine whether there was an IFA. Based on Wang et

al. [Wang, Zhou, Luo et al. (2014); Wang, Zhou, Liu et al. (2014)] continued to propose a collaborative countermeasure strategy by counting the occupancy ratio of PIT and the timeout ratio of PIT.

Tang et al. [Tang, Zhou, Liu et al. (2014)] detected IFA based on the two indicators of PIT occupancy ratio and interest packet satisfaction ratio. Ding [Ding (2015)] established a space vector model based on three indicators: PIT occupancy ratio, non-response rate of interest packet and geographical distribution rate. Finally, judging whether there was an attack based on the integrated vector distance. Salah et al. [Salah, Wulfheide and Strufe (2015)] proposed CoMon that integrating content access information and forwarding status of interest packets by setting up a domain controller in CCN. CoMon utilized PIT utilization ratio and PIT expiration rate to detect distributed low-rate IFA. Tang et al. [Tang, Zhang, Liu et al. (2013); Wang, Zhou, Qin et al. (2013)] counted the number of PIT entries that have expired and set thresholds to detect possible IFA in the network.

The research work described above are based on the abnormal changes of the PIT state after IFA occurs to detect possible attacks in the CCN. It mainly depends on the abnormal characteristics of the PIT structure after being attacked, so there is a certain delay in the detection time.

Gasti et al. [Gasti, Tsudik, Uzun et al. (2013)] calculated three indicators, i.e., the number of PI for each exit, the number of interest packets for each entry, and the number of PI for each namespace, and comprehensively detected attack by comparing with threshold.

Since the above three indicators are related to the average content packet size, the timeout period of PIT entry, and the bandwidth delay of link, the burst stream cannot be distinguished, and thus the request of the legitimate interest packets may be misjudged.

A large number of studies have shown that traffic has obvious burstiness and long-range-dependent [Cheng, Xie and Wang (2009)]. In view of the shortcomings of the above two methods, some researchers utilized those important characteristics of traffic to detect anomalies. Thereinto, information entropy is used as a measure to characterize the uncertainty of random variables. It is the most commonly used indicator when detecting network anomalies. Hurst index is an indicator of self-similarity of traffic.

Although in the traditional network and Software Defined Network (SDN), some researchers have used information entropy [Bin (2015); Wang, Wang and Huang (2017)] and self-similarity [Zhang, Ji and Wang (2015); Ren, Jin, Zheng et al. (2016)] to detect DOS/DDOS attack. However, the current research work mainly uses information entropy to detect the IFA of CCN. Xin et al. [Xin, Li, Wang et al. (2017)] utilized cumulative entropy to calculate the randomness of the distribution of different content names in the network to find traffic anomalies. This strategy has a shorter detection delay and higher detection accuracy, and further reduces the misjudgment for legitimate interest packets. The information entropy is also used to calculate and analyze the probability distribution of content name of the interest request in Rong [Rong (2015)], so as to determine whether there is an IFA in the network.

Xin et al. [Xin, Li, Wang et al. (2017); Rong (2015)] used information entropy to identify IFA in the CCN. Compared with the method based on the abnormal change of the PIT state after an IFA occurs, this method does not rely on the abnormal change of the PIT

state after attack. Accordingly, the detection delay is lower. At the same time, the calculation process of information entropy is independent of the size of the content packet, the delay of the link bandwidth, and the timeout period of the PIT entry. Therefore, compared to the method based on the balance principle of the CCN data stream, this method has a lower false alarm rate for normal burst traffic. From the above analysis, the detection method based on information entropy is the best.

However, under the low-rate IFA, the indicators based on the abnormal change of the PIT state and the balance principle of the CCN data stream are not obvious on the first few attacked routers; and for the detection method based on information entropy, the probability distribution of request does not change significantly, hence information entropy change too small to detect anomalies. Therefore, the above three methods have a poor detection effect the IFA with low-rate.

In fact, the self-similarity is the essential feature of traffic and is very sensitive to the change of traffic. Taking advantage of self-similarity, it can identify the initial attack behavior of IFA and ensure the detection effect under low-rate attacks. Moreover, information entropy reflects the random change of traffic. This change can be detected effectively when the traffic changes to a certain extent, so it can be used to detect the severity of the IFA. It is obvious that the two indicators have different polarities and effects. In this way, we simultaneously calculate the Hurst index and information entropy; then adopt bilateral detection method based the non-parametric CUSUM algorithm to identify and warn different levels of IFA in CCN.

3 IFA detection

3.1 IFA detection system design

The overall process of IFA detection is shown in Fig. 1.

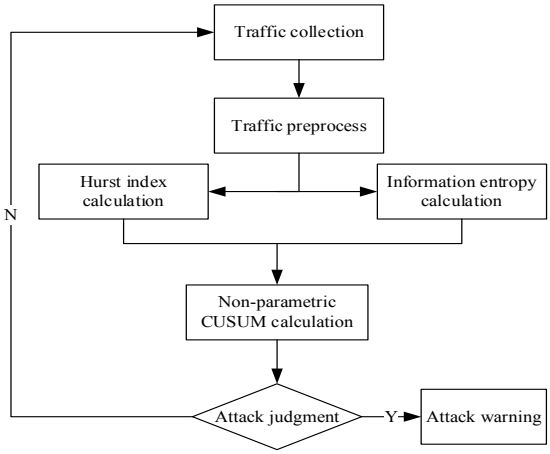

Figure 1: IFA detection flow chart

Specific steps are as follows:

Step 1: Traffic collection, i.e., collect information such as the content name, the number of be requested, and the time of arrival when CCN receives an interest packet.

Step 2: Traffic preprocessing, i.e., divide the collected traffic into series so as to process each segment traffic easily;

Step 3: Indicator calculation. It can be divided into Hurst index calculation and information entropy calculation. According to the processing result in Step 2, the Hurst index value and the information entropy value in the current series are calculated;

Step 4: Apply the Hurst index and the information entropy to the non-parametric CUSUM algorithm for the cumulative sum calculation;

Step 5: Attack judgment. Determine whether there is an IFA by comparing the two cumulative sums with threshold. If the threshold is exceeded, a warning is given; otherwise, traffic information continues to be monitored.

3.2 Hurst index

The Hurst index is a measure of whether a sequence has self-similarity. The relationship between self-similarity of a random sequence and Hurst index is as follows: (1) Hurst index of a random sequence is equal to 0.5, which indicates that this sequence is completely random; (2) Hurst index is in the (0.5, 1) interval, which indicates that the random sequence has self-similarity, and the higher the value of Hurst index, the higher the degree of self-similarity; (3) Hurst index is in the (0, 0.5) interval, which indicates that random sequences have the opposite characteristics of past trends, i.e., volatility, and do not have self-similarity.

Through the analysis of the Introduction session, there will be a large number of interest packets that are requested once in the CCN when IFA occurs. For our convenience, we extend the original PIT of each router with a field named count to record the number of times the current content is requested (shown in Fig. 2).

Prefix	Info	Count

Figure 2: Extended PIT structure

We adopt the Variance-time plots method to calculate Hurst index and the specific calculation process is as follows:

(1) Let the sequence of length L be $X=\{X_k, k=1, 2, 3,\ldots, L\}$, and divide the sequence into d data blocks of size m;

(2) Calculate the sample mean $E_k(m)$ of each data block;

(3) Calculate the sample variance $\sigma^2(m)$ of each data block;

(4) Take the logarithm of m and $\sigma^2(m)$ as the horizontal and vertical coordinates respectively;

(5) Adopt Linear fitting according to the least squares method and the slope $-\beta$ is the Hurst index of the current data block, i.e., $H=1-\beta/2$.

In this paper, we take the ratio of the number of interest packets with that are re-quested once as the statistical object of the Hurst index. It can not only measure the self-similarity of interest requests in CCN, but the false alarm ratio of attack detection in the case of sudden traffic can be reduced to some extent.

In this paper, we take the ratio of the number of interest packets with that are requested once as the statistical object of the Hurst index. It can not only measure the self-similarity of interest requests in CCN, but the false alarm ratio of attack detection in the case of sudden traffic can be reduced to some extent.

3.3 Information entropy

According to Shannon's theory, information entropy can be used to measure the random variation of an information sequence. The smaller the entropy value is, the more stable the information sequence is. In the CCN, user initiates a content request to the network through interest packet. In the whole process, there are no concept of IP address and port, and the content name is a unique identifier for information transmission. Therefore, we can judge the random change of CCN according to the distribution difference of content name under normal and attack situation.

The calculation of information entropy can be expressed by Eq. (1).

$$E(X) = -\sum_{i=1}^{n} p(xi) log_2 p(xi) \quad (1)$$

n refers to the number of independent events in the information sequence and $p(X_i)$ represents the probability of each event occurring. In this paper, n refers to the total number of interest packets received in each time period and $p(X_i)$ refers to the proportion of interest packets with the same content name. When an IFA occurs, a large number of interest packets of different content names appear in CCN, which destroying the distribution model of the content name under normal conditions and leading changes in information entropy.

3.4 Bilateral detection method

The non-parametric CUSUM algorithm is a commonly method in the statistical process, which accumulates small offsets to amplify the offset. It is a sequence detection method that can analyze and judge the data in real time and has the characteristics of short detection time and low false positive rate. Therefore, we adopt this algorithm to discriminate the two indicators comprehensively in the statistical process.

There are Hurst index and information entropy indicators. When the attack occurs, the abnormal changes of the two indicators are opposite, i.e., Hurst index becomes smaller and the information entropy becomes larger. For different indicators, there are two recursive processes as shown in Eqs. (2) and (3).

$$y_n^+ = (y_{n-1}^+ + Z_n)^+ \quad (2)$$

$$y_n^- = (y_{n-1}^- - Z_n)^+ \quad (3)$$

$y_0^+ = y_0^- = 0$ and we define $Zn = E - \alpha - \beta$, α represents the average of the indicator and β is a constant so that Zn in Eq. (2) has a negative mean and be a positive Eq. (3).

Information entropy becomes larger when the IFA occurs, so the upper test is taken i.e., adopt Eq. (2) to calculate the offset of information entropy; Hurst index becomes smaller in the event of IFA so as to adopt downside accumulation. So Eq. (2) is used to calculate the offset of Hurst index.

The decision function of the IFA is shown in Eq. (4).

$$d_N(y_N) = \begin{cases} 0\ (y_N \le Th) \\ 1\ (y_N > Th) \end{cases} \quad (4)$$

Th is the threshold for non-parametric CUSUM detection, $d_N(y_N)$ indicates the decision value at time n. It indicates that there is IFA on CCN if the value is 1, otherwise there is no IFA.

4 Experiment and evaluation

4.1 Network model and settings

The experiment is designed and implemented on the open source ndnSIM, and the network topology is shown in Fig. 3.

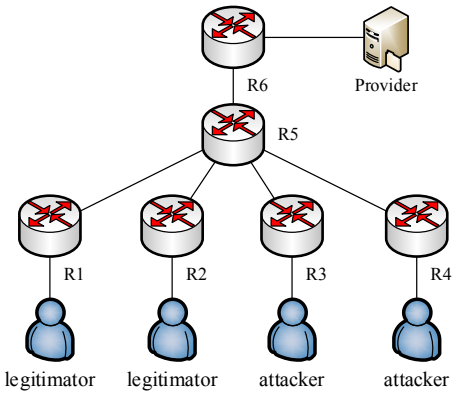

Figure 3: Experiment topology

R1, R2, R3, and R4 are edge routers that implement end user access, in which R1 and R2 routers connect to legitimator, and R3 and R4 connect to attacker. R5 is an intermediate router that implements aggregation and forwarding. R6 is directly connected to the producer. Our experiment assumes that all legitimators send interest packets at the same rate and conform to the Zipf-Mandelbrot distribution.

The parameters and values are summarized in Tab. 1.

Table 1: Simulation parameters

Parameters description	Values
Link bandwidth (Mbps)	100
Link delay (millisecond)	10
Content items	10000
PIT capacity	1000
PIT entry life time (second)	2
Legitimate request rate (packets/s)	200
Simulation time (second)	0-200
Attack time (second)	100-120

4.2 Harmful consequences of IFA

Fig. 4 shows the change of PIT occupancy rate for router R4, R5, and R6 during the simulation time.

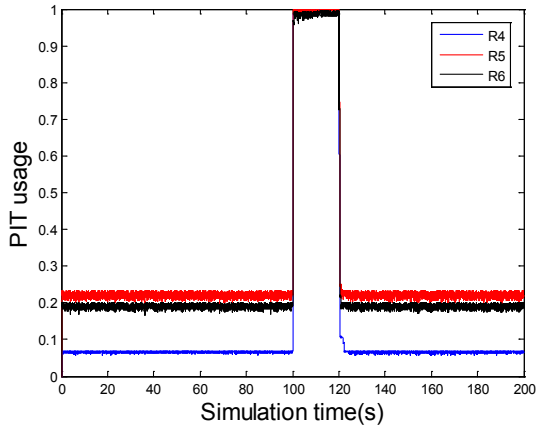

Figure 4: Change of PIT occupancy rate for router

Obviously, the PIT occupancy rate for the router can be divided into three phases during the entire simulation period: (1) in the normal state, the PIT occupancy rates of the three routers are lower, specifically 7%, 22% and 19%, respectively. (2) when the IFA starts, the PIT occupancy rates of the three routers increase rapidly, reaching 100% after 0.469 seconds, 0.396 seconds, and 0.407 seconds, respectively. (3) after the IFA complete, the PIT occupancy rate of each router gradually returns to the original level.

As shown in Fig. 4, the PIT occupancy rate for the router is relatively small when no attack occurs, meeting the demand of a large number of legitimators to request data. However, IFA can have a great impact on the CCN in a very short time, and the influence on intermediate router is more serious than that on edge router.

Fig. 5 shows the variation of the Hurst index during the simulation time.

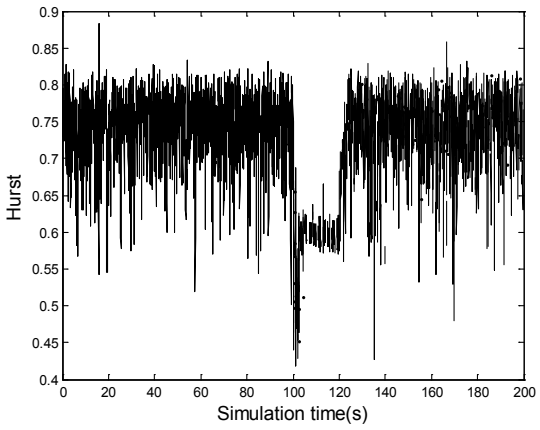

Figure 5: Change of Huret index

As shown in Fig. 5, the Hurst index average value is about 0.75 when network is in a normal state, and most of them are greater than 0.5, which indicates that the current traffic has a certain self-similarity and its degree is higher. When the IFA starts, the Hurst index value change a lot: in the initial stage, it decreases rapidly and less than 0.5, which indicates that the self-similarity state of the network changes, and the current traffic has a great volatility; the whole network enters a relatively stable state in the later period, so the Hurst index value increases to about 0.6. It has improved compared with the previous period, but is still less than that under normal conditions, indicating that the degree of self-similarity of the network is lower. When the attack is over, the Hurst index value gradually returns to normal.

Taking into account the changes of the Hurst index value during the entire simulation time, it is confirmed that we can utilize the Hurst index as an indicator for IFA detection.

Fig. 6 shows the change of information entropy during the simulation time.

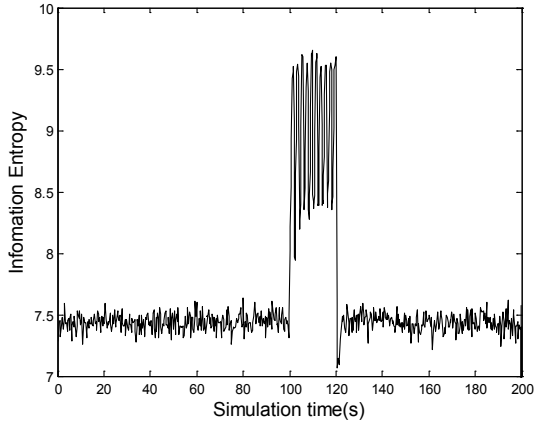

Figure 6: Change of information entropy

As shown in Fig. 6, the information entropy value is relatively stable when the network is normal and it fluctuates slightly around 0.75, indicating that the distribution of content name requested by legitimator is relatively stable. When the IFA starts, the information entropy value increases rapidly and varies greatly between 0.83 and 0.96, indicating that the distribution of content name changes greatly. Moreover, the information entropy value gradually returns to normal when the attack is over.

Taking into account the changes of the information entropy during the entire simulation time, it is confirmed that we can utilize the information entropy as an indicator for IFA detection.

4.3 Evaluation

4.3.1 IFA detection analysis

In order to more conveniently represent the attack strength, we define AD to express the ratio that legitimate request rate to illegal request rate, which shown in Eq. (5).

$$AD = \frac{Rate_{attack}}{Rate_{normal}} \tag{5}$$

Figs. 7-9 show IFA detection when AD is 1, 2.5 and 5, respectively.

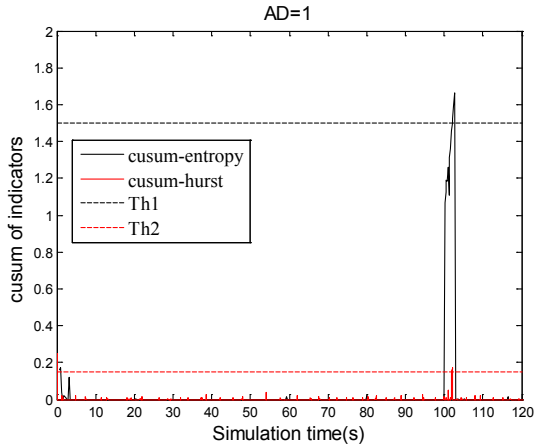

Figure 7: IFA detection under AD=1

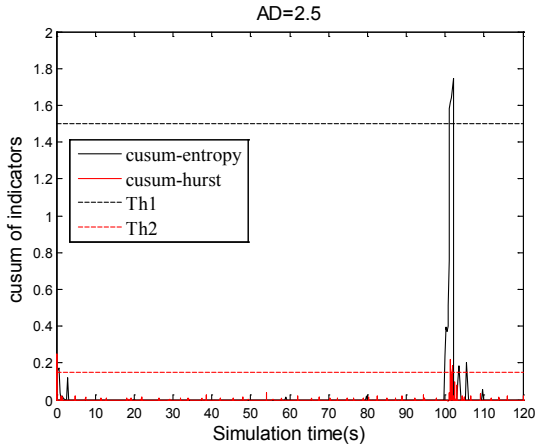

Figure 8: IFA detection under AD=2.5

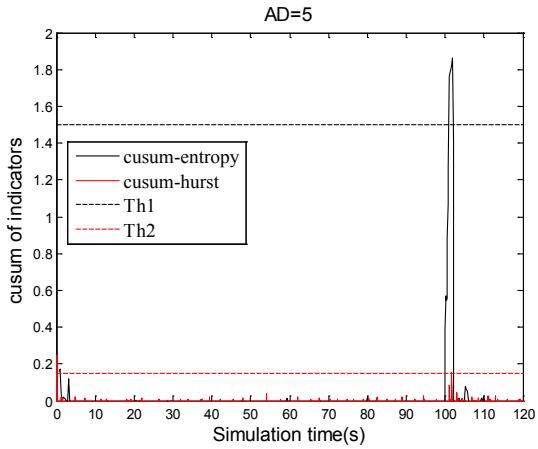

Figure 9: IFA detection under AD=5

In Figs. 7-9, Th1 represents the detection threshold that upper test of non-parametric CUSUM algorithm, i.e., the threshold when the non-parametric CUSUM algorithm is applied to accumulate information entropy; and Th2 is another detection threshold to accumulate Hurst index. From the analysis in Section 4.2, the average value of information entropy under normal state and attack state is 9, 7.5, respectively, so the difference between the two can be used as the detection threshold, that is, Th1=1.5; The mean value of Hurst index in normal state is about 0.75, and the change in the early attack period is relatively large, while relatively stable at the later, with an average of about 0.6. Therefore, we use the difference between the two as the detection threshold, i.e., Th2=0.15.

As shown in Figs. 7-9, as simulation time increases, the fluctuations of Hurst index and information entropy cause the cumulative sum increase. In the absence of IFA, it increases small and returns to zero frequently; while in the event of IFA, it increases rapidly and exceeds the threshold.

From Fig. 7, the non-parametric CUSUM algorithm applying Hurst index first detects IFA with a time of 102.025 seconds when AD=1. While the non-parametric CUSUM algorithm applying information entropy first detects the attack, and the time is 101.192 seconds and 101.184 seconds, respectively when AD=2.5 and AD=5, it can be seen in Figs. 8 and 9.

From the above analysis, we know that the time of IFA detection decreases as the attack strength increases. Further analysis shows that the non-parametric CUSUM algorithm with Hurst index has better detection effect under the low-rate attack and the non-parametric CUSUM algorithm with information entropy is opposite.

4.3.2 Comparative experimental analysis

In this section, we compare our method with the algorithm based on information entropy in Xin et al. [Xin, Li, Wang et al. (2017)]. The result is shown in Tab. 2.

Table 2: Comparison of IFA detection method

Attack strength	Method in Xin et al. [Xin, Li, Wang et al. (2017)] (s)	Our method (s)
1	2.07	2.025
2.5	1.192	1.192
5	1.184	1.184

As shown in Tab. 2 that the detection time of this two-method decreases as the strength increase. And our detection method has a shorter detection time at the attack strength is 1.

In order to verify the advantages of the IFA detection method which we proposed, we calculate the PIT satisfaction ratio changes with the simulation time in CCN (as shown in Fig. 10.)

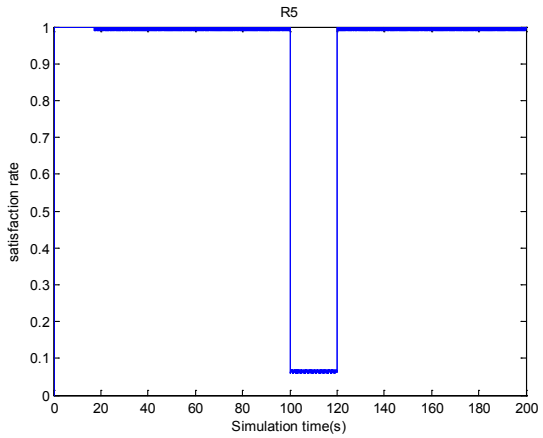

Figure 10: Change of satisfaction radio

As shown in Fig. 10, the router's PIT satisfaction ratio is very high, closing to 100% when the network has not IFA; when IFA occurs, it drops rapidly, and the legitimator interest request is greatly affected.

The method based on attack hazard feedback (PIT satisfaction ratio) is greatly affected by the lifetime of PIT entry. Therefore, we compare our method with the algorithm based on PIT satisfaction ratio under the lifetime is 1 s, 2 s and 3 s respectively. The result is shown in Tab. 3.

Table 3: Comparison of IFA detection method

PIT entry lifetime (s)	Method based on PIT satisfaction ratio (s)	Our method (s)
1	>=1	0.965
2	>=2	1.184
3	>=3	1.495

As shown in Tab. 3, as the lifetime of PIT entry increases, the detection time of our method increases slightly. But for the method based on PIT satisfaction ratio, it calculates the indicator until the PIT entry expire. So, the detection time is generally greater than lifetime of the PIT entry. Obviously, our method has outstanding advantages in IFA detection.

5 Conclusion

Aiming at the problem of IFA in CCN, we summarize and analyzes current research findings of domestic and foreign scholars. On this basis, we continue to propose an IFA detection method based on traffic self-similarity and information entropy. We firstly extend the original PIT with a field named count to record the number of times the current content is requested, so as to conveniently calculate the Hurst index value; next calculate the information entropy according to the probability of each content requested by user; finally, adopt the non-parameter CUSUM bilateral detection algorithm to determine whether there is an IFA. Experiment results show that our detection method

can quickly detect possible IFA in the early stage of attack whether the IFA is under low-rate or high-speed. At the same time, it is less affected by the life-time of PIT entry, which can minimize the impact of IFA on the entire CCN.

Funding Statement: This work was supported by the National Natural Science Foundation of China No. 61672101, the Beijing Key Laboratory of Internet Culture and Digital Dissemination Research (ICDDXN004)* and Key Lab of Information Network Security, Ministry of Public Security, No. C18601.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Afanasyev, A.; Mahadevan, P.; Moiseenko, I.; Uzun, E.; Zhang, L. (2013): Interest flooding attack and countermeasures in named data networking. *IFIP Networking Conference*, pp. 1-9.

Bin, X. (2015): *Research on the Detection and Defence of DDoS Attack in SDN-Based Wlan (Master's Thesis)*. Shanghai Jiao Tong University, Shanghai, China.

Cheng, X.; Xie, K.; Wang, D. (2009): Network traffic anomaly detection based on self-similarity using HHT and wavelet transform. *The Fifth International Conference on Information Assurance and Security*, pp. 710-713.

Compagno, A.; Conti, M.; Gasti, P.; Tsudik, G. (2013): Poseidon: mitigating interest flooding DDoS attacks in named data networking. *38th Annual IEEE Conference on Local Computer Networks*, pp. 630-638.

Dai, H.; Wang, Y.; Fan, J.; Liu, B. (2013): Mitigate DDoS attacks in NDN by interest traceback. *IEEE Conference on Computer Communications Workshops*, pp. 381-386.

Ding, K. (2015): *Research on the Countermeasure of Interest Flooding Attack in Named Data Networking (Master's Thesis)*. Beijing Jiaotong University, Beijing, China.

Gasti, P.; Tsudik, G.; Uzun, E.; Zhang, L. (2013): DoS and DDoS in named data networking. *22nd International Conference on Computer Communication and Networks*, pp. 1-7.

Li, Y.; Xin, Y.; Han, Y.; Li, W.; Xu, Z. (2017): A survey of DoS attack in content centric networking. *Journal of Cyber Security*, vol. 2, no. 1, pp. 91-108.

Ren, Y.; Jin, D.; Zheng, D.; Liu, L.; Wei, X. (2016): An analytical model of data plane performance subject to prioritized service. *IEEE Trustcom/BigDataSE/ISPA*, pp. 1537-1542.

Rong, Y. (2015): *Detecting and Mitigating DDoS Attack in Content Centric Network (Master's Thesis)*. Shanghai Jiao Tong University, Shanghai, China.

Salah, H.; Wulfheide, J.; Strufe, T. (2015): Coordination supports security: a new defence mechanism against interest flooding in NDN. *40th Conference on Local Computer Networks*, pp. 73-81.

Tang, J.; Zhang, Z.; Liu, Y.; Zhang, H. (2013): Identifying interest flooding in named data networking. *IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber*, pp. 306-310.

Tang, J.; Zhou, H.; Liu, Y.; Zhang, H. (2014): Mitigating interest flooding attack based on prefix identification in content-centric networking. *Journal of Electronics & Information Technology*, vol. 36, no. 7, pp. 1735-1742.

Tang, L. (2014): *Research on Congestion Control in Content-Centric Networking (Master's Thesis)*. University of Electronic Science and Technology of China, Chengdu, China.

Tian, W.; Ji, X.; Liu, W.; Liu, G.; Lin, R. et al. (2019): Defense strategies against network attacks in cyber-physical systems with analysis cost constraint based on honeypot game model. *Computers, Materials & Continua*, vol. 60, no. 1, pp. 193-211.

Wang, K.; Zhou, H.; Luo, H.; Guan, J.; Qin, Y. et al. (2014): Detecting and mitigating interest flooding attacks in content-centric network. *Security & Communication Networks*, vol. 7, no. 4, pp. 685-699.

Wang, K.; Zhou, H.; Qin, Y.; Chen, J.; Zhang, H. (2013): Decoupling malicious interests from pending interest table to mitigate interest flooding attacks. *IEEE Globecom Workshops*, pp. 963-968.

Wang, K.; Zhou, H.; Qin, Y.; Zhang, H. (2014): Cooperative-Filter: countering interest flooding attacks in named data networking. *Soft Computing*, vol. 18, no. 9, pp. 1803-1813.

Wang, W.; Wang, L.; Huang, Y. (2017): Detection of low rate DDoS attacks based on renyi entropy in SDN environment SDN. *Journal of South-Central University for Nationalities*, vol. 36, no. 3, pp. 131-136.

Xin, Y.; Li, Y.; Wang, W.; Li, W.; Chen, X. (2017): A novel interest flooding attacks detection and countermeasure scheme in NDN. *IEEE Global Communications Conference*, pp. 1-7.

Zhang, Y.; Ji, S.; Wang, H. (2015): WSN intrusion detection technology based on SDN architecture. *Journal of Henan University (Natural Science)*, vol. 45, no. 2, pp. 211-216.