Renyi entropy-based detection method for low-rate interest flooding attacks

Ziyi Zhao

School of Computer Science and Engineering Tianjin University of Technology
Tianjin, China
794948443@qq.com

Kai Shi†

School of Computer Science and Engineering Tianjin University of Technology Tianjin, China
† Corresponding Author: Kai Shi:
shikai0229@tjut.edu.cn

ABSTRACT

Named Data Networking (NDN) has excellent security performance compared with TCP/IP networks. Because of this advantage, in the era of big data, the NDN is likely to become the mainstream network in the future, and it has high research value and development prospects. However, in practical application, NDN still has certain functional defects, which is easy to cause security problems. Especially when dealing with complex interest flooding attacks, NDN predisposes to damage. Based on this, in conjunction with low-rate interest flooding attacks in NDN, the article proposes a Renyi entropy-based interest flooding attack detection method to improve the network's defense capability against complex interest flooding attacks.

CCS CONCEPTS

• Networks→ Network properties→Network security→ Denial-of-service attacks.

KEYWORDS

Named data networking, interest flooding attacks, low-rate attacks,Renyi entropy

1 Introduction

NDN is a new network architecture that has emerged in recent years. Compared to traditional TCP/IP networks, NDN uses a content-distribution form of network architecture, which directly adopts the name content as the dominant communication method. This communication mode enables users in the network to initiate requests in the network only through the information name. This new network architecture reduces the routing information carried by information in the network. In NDN, the data transmitted in the network is divided into interest packets and data packets. Interest packets are packets sent by network users when they make a request; data packets are packets that are sent by the network in response to a user's request to fulfil their request. The router node is divided into three data structures: the content store (CS), the pending interest table (PIT) , the forward information base (FIB). The CS is responsible for caching packets passing through the router; the FIB is responsible for storing interest packet name prefixes, output interface fields, and forwarding policies; and the PIT stores interest packet entries.

When the interest packet arrives at the network node, it will first look out whether there is a corresponding packet from the content cache. If there is a matching packet, it will return the data according to the arrival path of the interest packet and discard the interest packet; if not, it will look for a corresponding entry in the PIT, add the source interface of the interest packet to the entry and discard the interest packet; if not, it will add an entry in the PIT and send the interest packet to the next hop router according to the longest matching name. The interest packet is sent to the next-hop router according to the output of the query.

NDN uses named content as the centre for verifying name-content bindings, it record interest packet requests in the router's pending interest table.Interest flooding attacks(IFA), in which an attacker sends a large number of malicious interest packets to a network node to fill up the NDN router's resources, become a major security threat to NDN.The main target of IFA is the router's PIT, where the attacker initiates a request by sending a large number of malicious interest packets to exhaust the PIT memory resources, making it impossible for normal requests to create a PIT , and eventually normal requests are discarded to achieve the purpose of the attack.

As a more complex form of IFA, low-rate flooding attack(LIFA) has a high similarity between its interest packet request rate distribution and normal flow. In the LIFA, multiple attackers send out conspiracy interest packets at the same time, while users also send out interest packets that can be matched at the same time, and since each attacker sends out a small number of conspiracy interest packets, no anomaly is detected at the adjacent router node, while malicious interest packets sent by multiple attackers are aggregated at the downstream router node, causing the PIT at the downstream router node to overload, at which point the attacker stops sending conspiracy interest packets. All subsequent interest packets passing through the downstream router node will be dropped. Figure 1 shows an example of a LIFA .

EITCE 2021, October 22–24, 2021, Xiamen, China

ACM ISBN 978-1-4503-8432-2/21/10…$15.00
https://doi.org/10.1145/3501409.3501537

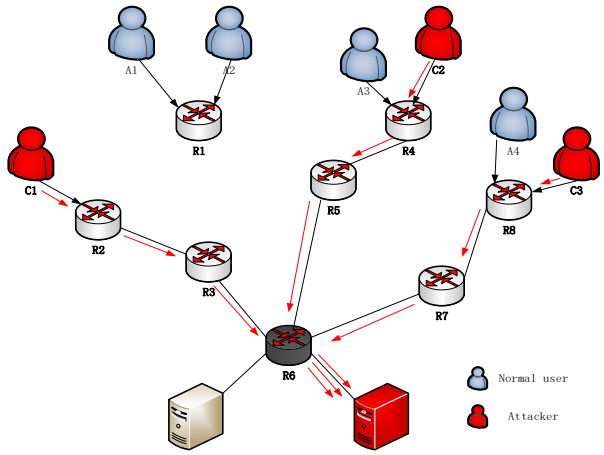

Figure 1: Example of a low rate attack

While the number of interest packets received by the routers increases significantly when the attack first occurs, and then decreases to normal levels again within a short period of time. In addition, the attacker generates an answer packet when the entry in the router's PIT is about to expire, based on the expiry time of the entry, and then proceeds to launch the next wave of attacks. Such an attack will cause the PIT of the downstream router to be overloaded again each time it has just been released, reflecting the cyclical and intermittent nature of LIFA.

2 Related Work

The literature[1] first introduced the concept of IFA as a security threat to NDN. The literature [2] illustrates the importance of PIT in the Content Centric Network (CCN) and NDN for the proper connectivity of the network, and shows that if the PIT is attacked, the normal operation of the NDN will be seriously affected. The literature [3][4] directly investigates IFA and demonstrates the threatening and destructive nature of IFA in NDN by changing the means of attack. The literature[5] proposed IFA detection based on entropy method, by monitoring the attack on router nodes for random distribution characteristics of interest packets. This method cannot distinguish well between network burst traffic and IFA traffic based on information entropy for IFA detection.The literature [6] proposes an attack detection method based on relative entropy. The method using relative entropy theory for IFA detection has low computational complexity and is sensitive to changes in the entropy value of network features, but the method also has disadvantages such as more network traffic data required to calculate relative entropy and high computational overhead, and the detection effect is relatively poor when distinguishing different attack types. The literature [7] performs attack detection through GINI impurity analysis for interest packets, and notifies neighbouring routers for collaborative defence when an attack is detected. Its drawbacks include: when a LIFA occurs, the router nodes close to the producer are the first to be harmed and when the PIT of this part of the node is full, the PIT internal interest request records will be discarded, but normal user interest requests contained within the PIT will also be discarded, making normal user network requests equally affected. Current research on LIFA is less. In the literature [8], they proposed a satisfaction-based push-back detection mechanism, and this PIT satisfaction-based detection method has a better resistance effect for IFA, but it is not effective for LIFA detection due to the high rate of interest packets being satisfied during LIFA.

The main contributions of this article are as follows.

In this paper ,we propose a detection method based on Renyi entropy. The prefix distribution of packet names of interest stored in the PIT module of router nodes in the NDN is used as a feature. While LIFA has occurred, the interest packet name prefixes are more dispersed.As multiple attackers all periodically send malicious request interest packets to the router node, Renyi entropy is more sensitive to perceived differences in the random distribution of name prefixes in small traffic traffic.When LIFA occurs, minor changes in the distribution of interest name prefixes stored in the PIT in the routing node can also be accurately detected, using Renyi entropy theory to enhance the differentiation between normal traffic and LIFA traffic.

3 Detection mechanism based on Renyi entropy

In this section,we proposes a LIFA detection method based on Renyi entropy, which can improve the accuracy of LIFA detection. And its characteristic is to distinguish LIFA from normal network state more specifically, enhancing the success rate of detection of IFA.

3.1 Renyi entropy theory

In order to provide an accurate measure of abstract information, Shannon introduced the concept of "information entropy" in 1984.In information theory is used to measure the uncertainty and complexity of a random variable.The greater the uncertainty of the random variable, the greater the information entropy value; the smaller the uncertainty of the random variable, the smaller the information entropy value.Information entropy theory is currently used in a wide range of fields such as computer science, communication technology and electrical engineering. Renyi entropy is a generalization of Information entropy by Alfred Renyi in 1961.Compared to Information entropy, Renyi entropy can increase the difference between different probability distributions. Therefore, Renyi entropy can be used to distinguish normal flow and abnormal flow, it is suitable for LIFA detection.The formula for calculating the probability is:

$$P(x_i) = \frac{x_i}{\sum_{i=1}^{n} x_i}$$

Where n denotes the type of interest package name and x_i denotes the total number of interest packages with name prefix i. The information entropy is calculated according to the probability

of the interest prefix distribution, and the information entropy is defined as:

$$H_t(x) = -\sum_{i=1}^{n} p(x_i)\log_2^{p(x_i)}$$

The general definition of Renyi entropy is:

The renyi entropy of order α is

$$H_\alpha(x) = \frac{1}{1-\alpha}\log_2(\sum_{i=1}^{n} p_i^{\alpha})$$

Renyi entropy is maximized when $\alpha = 0$:

$$\max H(\alpha) = \log_2 n$$

The Renyi entropy converges to the Information entropy as $\alpha \to 1$. The proof proceeds as follows.

$$\lim_{\alpha\to 1} H_x(\alpha) = \lim_{\alpha\to 1}\frac{1}{1-\alpha}\log_2(\sum_{i=1}^{n} p_i^{\alpha}) = \lim_{\alpha\to 1}\frac{\sum_{i=1}^{n} p_i^{\alpha}\ln p_i}{\sum_{i=1}^{n} p_i^{\alpha}\ln 2}$$

$$\sum_{i=1}^{n} p_i^{\alpha} = 1 \quad \lim_{\alpha\to 1} H_X(\alpha) = -\sum_{i=1}^{n} p_i^{\alpha}\times\log_2 p_i$$

,

$$\alpha \to 0, \quad \frac{\partial H_\alpha(x)}{\partial \alpha} \le 0$$

Renyi entropy is a decreasing function that decreases as α increases. As the order α increases, the deviation degree of Renyi entropy is bigger.In this detection mechanism, When $\alpha = 10$, the largest difference in Renyi entropy values between normal and abnormal traffic.Therefore, we sets the order α to 10.

3.2 Sliding window model

This detection method uses the sliding time window model for Renyi entropy value collection. The sliding window model is continuously updated with the most recently arrived stream data.The advantage of sliding window model is low complexity and low resource cost.

In defining the sliding window model, we define three elements: the interest package d, the window width w, and the sliding length l. The window model is denoted W(d,w,l). At detection, the window of width w slides from the start sampling point i to j with a sliding length a. The data stream changes from b(i,i+w-1) to b(i+a,i+a+w-1). Over time, the data in the window is continuously updated with continuous detection. Figure 4 shows the sliding window model.

3.3 Overall detection mechanism

This method recursively extracts data from the sliding window cache queue to calculate Renyi entropy, and sends an interest flooding attack warning to the router when the Renyi entropy value is abnormal.

Firstly, the detection method extracts the data stream from the sliding window sequence and then uses it as input data for defence detection. The method continuously collects statistics and monitoring data from the cache queue and calculates the Renyi entropy. If the entropy value exceeds a set threshold, a flood warning message is issued. The detailed testing steps are as follows:

Step 1: Predetermine the detection threshold and the dumber of times to set the detection threshold.

Step 2: Read the data from the sliding time window and calculate the Renyi entropy. If the entropy value is higher than the preset threshold, revert to the previous step, otherwise continue.

Step 3:Start the counter count and add 1 to the counter value.

Step 4:Determine if the counter count value is greater than the alarm threshold. When the Renyi entropy exceeds the threshold several times, we determine that the current time period is under LIFA attack and issue a warning.

3.4 Set threshold

To reduce the false alarm rate, the detection mechanism requires preset warning thresholds.When setting the threshold, we combine the mean and the standard deviation to determine the Renyi entropy threshold.Dividing network traffic into segments at fixed intervals, the Renyi entropy values H_i were calculated for n different time periods in turn. The mean value was calculated using the n Renyi entropy values as samples, and the mean value was calculated as follows.

$$\overline{H_t} = \frac{\sum_{t-n}^{t-1} H_i}{n}$$

By standard deviation σ_t Formula:

$$\sigma_t = (\frac{1}{n-1}\sum_{i=t-n}^{t-1}(H_i - \overline{H_t})^2)^{\frac{1}{2}}$$

Choose $3\sigma_t$ as the upper and lower limits of the threshold value, at this point the threshold value range is initially determined as $H^t = [H^t - 3\sigma_t,\ H^t + 3\sigma_t]$

4 Experiments and results analysis

In order to verify the effectiveness of the Renyi entropy-based detection method for LIFA detection, simulations are evaluated on the ndnSIM simulation platform in this paper.

4.1 Simulation parameter setting

The experiments are based on the ndnSIM simulation platform, using the NDN protocol stack of the ns-3 network. In the simulation scheme the author have implemented, a simple tree network topology is built and the detection device is installed on a router node directly connected to the user, as shown in Figure2. The

author perform the LIFA simulation for 40s, where the LIFA is launched continuously at 20s, LIFA launched every 5 seconds, and the number of interest packets and packets received by the core router are sampled every 100ms.

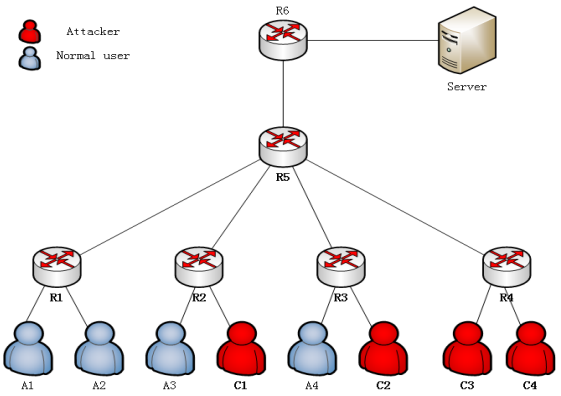

Figure 2: Experimental topology diagram

In this experiments, We set two LIFA models: When the ratio of malicious interest packets to normal interest packets is 1, the attack mode is defined as " Ratio （R） = 1";When the ratio of malicious interest packets to normal interest packets is 3, defined as "Ratio （R） =3"

4.2 Experimental results and their analysis

The results of the simulation experiments are shown in Figure 3 - Figure 5.Methods based on Renyi entropy , the greater the alpha order, the greater the Renyi entropy deviation when LIFA occurs.Figure 3 shows that when 200 packets of interest are cached in the sliding window, we launch the LIFA with R=1 at the 20th second.Methods based on information entropy have little change in entropy values in the face of LIFA.

Figure 4 shows that when 300 packets of interest are cached in the sliding window, we launch the LIFA with R=1 at the 20th second.When α = 10, the difference in Renyi entropy increases from 0.0062 to 0.0396 between the normal situation and when attacked by the LIFA.Figure 5 shows that when 300 packets of interest are cached in the sliding window, we launch the LIFA with R=3 at the 20th second.When α = 10, the difference in Renyi entropy becomes more obviously, it increases from 0.0071 to 0.5082 between the normal traffic and when attacked by the LIFA.

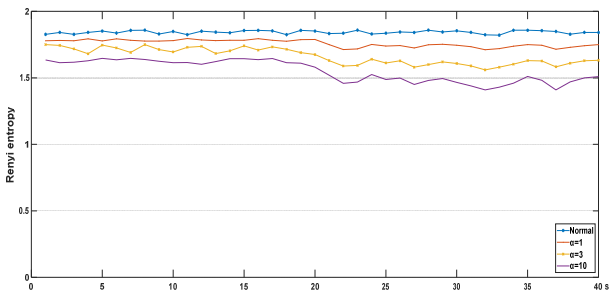

Figure 3: Window 200, Ratio=1

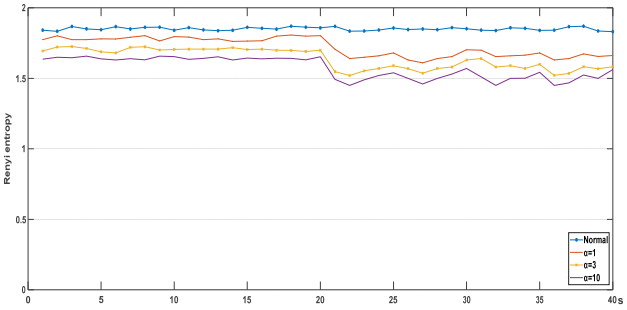

Figure 4: Window 300, Ratio=3

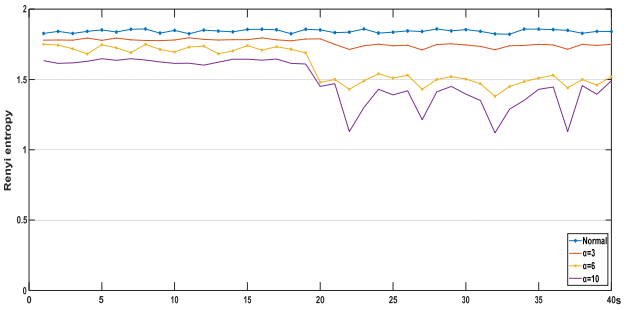

Figure 5: Window 300, Ratio=3

Table 1 to 3 show the average entropy values for different windows of Average entropy values for normal and abnormal flows.As for the means of IFA detection based on the Renyi entropy method, as the order α changes, it can be found that the Renyi entropy changes more and more obviously.This means that the Renyi entropy method is able to amplify the difference in entropy values between normal traffic and the LIFA, regardless of the ratio of the attack, indicating that the Renyi entropy is more effective for detecting LIFA .

Table 1 Window 200 R=1 Renyi entropy of different orders

Order	Average	Minimum value	Inflection point difference
Information Entropy	1.843	1.821	0.022
α =3	1.722	1.610	0.112
α =6	1.639	1.520	0.119
α =10	1.550	1.410	0.140

Table 2 Window 300 R=1 Renyi entropy of different orders

Order	Average	Minimum value	Inflection point difference
Information Entropy	1.843	1.821	0.022
α =3	1.761	1.710	0.051
α =6	1.596	1.380	0.216
α =10	1.486	1.121	0.365

Table 3 Window 300 R=3 Renyi entropy of different orders

Order	Average	Minimum value	Inflection point difference
Information Entropy	1.851	1.831	0.020
α =3	1.760	1.711	0.049
α =6	1.662	1.560	0.102
α =10	1.573	1.450	0.123

In order to evaluate the effectiveness of this method more intuitively, the author need to use the Information entropy and Renyi entropy for the calculation of the false alarm rate, defined as

$$FAR = \frac{F}{F+A}$$

F is the number of samples of normal traffic that were false alarmed as abnormal traffic and A is the total number of normal.

Set the median of the difference between normal flow and abnormal flow as the threshold value, and identify normal flow samples that exceed the threshold value as false alarm sample.F_x and F_y are the number of false alarm samples under the information entropy method and Renyi entropy method.According to Table 2, based on the Renyi entropy method, the false alarm rate decreases as the order α increases. The false alarm rate reaches 100% at α =10, indicating that it has good detection effect for LIFA.

Table 4 Comparison of false alarm rates

Order	Number of false	False alarm rate
α =3	12	0.24
α =6	5	0.1
α =10	0	0

5 Conclusions

In order to further promote the practical application and development of NDN, many researchers have devoted great attention to NDN security issues. The IFA, as a more serious threat to NDN, is a security issue that cannot be ignored in NDN research. In this article, the author exploits the characteristics of NDN that request and forward packet names, collect and monitor the information of packet name distribution, and combine the characteristics of Renyi entropy theory to perform the detection of LIFA. It is experimentally expressed that the method proposed in this article has good detection performance with low false alarm rate in the face of LIFA .

ACKNOWLEDGMENTS

This work was supported in part by a Tianjin Science and Technology Project under grant No.19JCTPJC43300.

REFERENCES

[1] Li L , Zhou J , Xiao N . DDoS attack detection algorithms based on entropy computing[C]// Information and Communications Security, 9th International Conference, ICICS 2007, Zhengzhou, China, December 12-15, 2007, Proceedings. DBLP, 2007.

[2] Wang K , Zhou H , Qin Y , et al. Cooperative-Filter: countering Interest flooding attacks in named data networking[J]. Soft Computing, 2014, 18(9):1803-1813.

[3] Gasti P , Tsudik G , Uzun E , et al. DoS and DDoS in Named-Data Networking[J]. IEEE, 2013.

[4] Compagno A , Conti M , Gasti P , et al. Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking[J]. IEEE, 2014.

[5] Xin Y , Yang L , Wei W , et al. A Novel Interest Flooding Attacks Detection and Countermeasure Scheme in NDN[C]// GLOBECOM 2016 - 2016 IEEE Global Communications Conference. IEEE, 2016.

[6][1] Afanasyev A , Mahadevan P , Moiseenko I , et al. Interest flooding attack and countermeasures in Named Data Networking[C]// Ifip Networking Conference. IEEE, 2013.

[7] Zhi T , Luo H , Liu Y . A Gini Impurity Based Interest Flooding Attack Defence Mechanism in NDN[J]. IEEE Communications Letters, 2018:1-1.

[8] Signorello S , Marchal S , J François, et al. Advanced Interest Flooding Attacks in Named-Data Networking[C]// The 16th IEEE International Symposium on Network Computing and Applications (NCA 2017). IEEE, 2017.

[9]Ab A , Aekt A , Caka E , et al. MSIDN: Mitigation of Sophisticated Interest flooding-based DDoS attacks in Named Data Networking - ScienceDirect[J]. Future Generation Computer Systems, 2020, 107:293-306.

[10] Yan R , Zheng Q , Peng W . Multi-scale Entropy and Renyi Cross Entropy Based Traffic Anomaly Detection[C]// IEEE Singapore International Conference on Communication Systems. IEEE, 2008.

[11] Wang W , Wang L , Huang Y . Detection of Low Rate DDoS Attacks Based on Renyi Entropy in SDN Environment[J]. Journal of South-Central University for Nationalities(Natural Science Edition), 2017.