Research on Node Routing Security Scheme Based on Dynamic Reputation Value in Content Centric Networks

Jianwei Zhang[1], Chunfeng Du[2], Zengyu Cai[2], Zuodong Wu[1], Wenqian Wang[2]
1. School of Software, Zhengzhou University of Light Industry
2. School of Computer and Communication Engineering, Zhengzhou University of Light Industry
Zhengzhou, China
mailzjw@163.com, dcf_wy@163.com, mailczy@163.com, 15038079618@163.com, 715847090@qq.com

***Abstract*—As a new generation of network architecture with subversive changes to traditional IP networks, Content Centric Networks (CCN) has attracted widespread attention from domestic and foreign scholars for its efficient content distribution, multi-path and secure routing features. The design atchitecture of CCN network has many advantages. However, it is also easily used illegally, which brings certain sectrity problems. For example, objectified network resources which include requesters, publishers, content, and node routes , are faced with many security threats, such as privacy attribute disclosure, privacy detection, content information disclosure, and spoofing and denial of service attacks. A node routing security scheme based on dynamic reputation value is proposed for the security problem of node routing. It is convenient for detecting node routing attacks and defending in time. And it could provide security for the Content Centric Networks node routing without affecting the node routing advantages and normal user requests.**

Keywords—content centric networks; security issues; dynamic reputation value; defensing; routing advantages

I. INTRODUCTION

With the rapid development of the network and the diversification of applications, traditional IP networks have shown weaknesses in many areas, such as exhaustion of address resources and scalability problems, poor reliability, intranet penetration problems, mobility, and multipath problems. At present, the main body of network applications is also gradually evolving towards content and information services [1]. In order to ensure the service quality (QOS) of the service subject remains unchanged and adapt to the development of the future network, many scholars at home and abroad have carried out many new-generation Internet architecture research projects. “Data Oriented Network Architecture (DONA)[2]”, was proposed by RAD Lab, University of California, Berkeley. “Data Oriented Translation(DOT), was proposed by Carnegie Mellon University, USA [3]. "Content-Centric Networking (CCN) [4]" was jointly proposed by the Department of Computer Science, University of California, Los Angeles, and the Palo Alto Research Center in the United States. And Content Aware Network proposed by the Chinese Academy of Sciences [5]. Among these designs with content as the core of the network architecture, the CCN network is the most representative.

The CCN network implements the process of communication from "host-host" to "request content-acquisition content". The main body of the service is content, not storage location. Unlike traditional IP networks, node routing can cache content information in order to shorten the information request time and improve communication efficiency. CCN's special architectural design and unique advantages have attracted the attention of attackers while being widely concerned by the academic community. The hidden danger zone in the architecture is used to attack and steal private information on various objects in the network. At present, academic research on CCN network content mostly focuses on caching and routing. There is not much research on its security and privacy. The object of the requester, information dissemination, content, and other network node routing resources are still faced with many issues of privacy and security[6~7].

II. CCN NETWORK OBJECTIFICATION AND SECURITY ANALYSIS

A. CCN network object division

During the communication process, the request packet is issued by the content requester and arrives at the node route. The packet is returned if the interest request content is already cached in the node route. Otherwise, node-routed broadcast or default port forwarding is used. The request packet continues to be passed until the interest packet arrives at the content server, and the content server returns the content data packet. According to the different roles of various resources in the CCN network, CCN network resources can be divided into different objects such as content requester, content publisher, content, and node routing [8]. CCN network resource objectification as show in Fig 1.

Content requester object: The content requester object is the subscriber of the content information in the CCN network. Meanwhile, it is the consumer, the origin of the network communication, and the data content service subject.

Content publisher object: The content publisher object is the publisher. And it is producer of the content information in the CCN network, and the source of the communication content information.

978-1-5386-6243-4/19/$31.00 ©2019 IEEE

Content object: The content object is the core of network communication, and it is the information delivery entity, including specific content information such as interest packages, data packages, and cached copy contents.

Node-routing object: The node routing object is the infrastructure for communication in the CCN network, which is specialized as a router node, containing routing of core and edge parts.

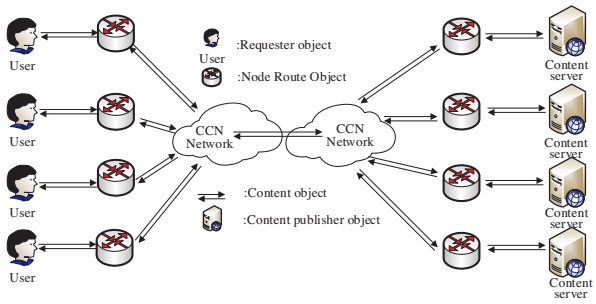

fig. 1. CCN network resource objectification

B. Analysis of node routing object security problem

The request and release of content information in the CCN network is the basis of the communication of the service subject[9~10]. Communication between subjects is guaranteed only if the consistency of the process between the requester object and the publisher object is guaranteed. And these depend on the node routing object is relatively safe. Currently, the security problems of node routing include resource exhaustion, timing attacks, interference attacks, and flooding.

Resource exhaustion: Resource exhaustion attacks in the CCN network are divided into overall and partial resource exhaustion. The former is stored and forwarded by the routing node by sending a large amount of request information. A large amount of request information and content information are directly or indirectly distributed in the network, causing network link congestion and increasing network load. Eventually, the resources in the CCN network will be exhausted, and the node route will refuse service. The latter sends a large number of packets. The purpose is to reduce the routing performance of the individual edge nodes in the CCN network, increase the routing response time, and reduce the data response efficiency.

Timing attack: The main goal of the attack is to disrupt the consistency of information requests and release times. Reduce node router performance by sending a large amount of request information. Thereby increasing the response delay of the source end, so that the user request can not get a timely response.

Interference attack: The attacker pretends to be a trusted legitimate user. A large number of malicious or unnecessary interest packets are sent to the node route, which disturbs the flow of information in the system [11~12]. Unlike resource exhaustion, a spoofed attacker attacks a shared node in the link and forwards it to other nodes, as shown in Fig 2.

Flooding attack: The CCN network has the role of replacing the IP address of the IP network by name. However, there is no host ID in the CCN network, and it can not be searched by IP address. When a CCN node receives a flooding attack, the number of requests that the node can handle is limited, so the latter request is ignored [13]. This type of attack does not consider whether the request is legitimate, and will eventually cause the node route to reject all service requests.

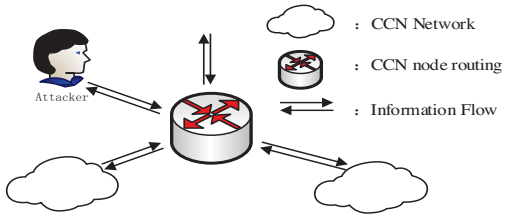

fig. 2. Interference attack

III. CCN NETWORK NODE ROUTING SECURITY PROTECTION SCHEME

A. Program background

In order to effectively identify whether the node route has been attacked, some scholars have done some research on it, and proposed a defense scheme to mitigate and weaken the attack. In 2014, Tang et al. [14] proposed a two-stage hierarchical detection method for node flooding attacks. The proportion of malicious interest packages is reflected according to the interest package satisfaction rate. $S(t)=\Delta D/\Delta I$, ΔD represents the average number of received packets per port in unit time t, and ΔI represents the average number of received interest packets per unit time t. Under normal circumstances, the interest packets and data packets passing through the port are basically equal in number. This balance is broken due to the occurrence of node routing flood attacks. According to this, it can be roughly judged which port has been attacked and enters the deep precision detection stage. By collecting and sorting the number of interest prefixes of various prefixes and pre-set thresholds, the abnormal name prefix is identified to determine whether the node route is attacked. Goergen et al. [15] proposed using data mining algorithms to monitor whether the network was attacked. The specific principle is to collect data in two different cases by using a classifier (also called a support vector machine) to classify. Then, the nodes are monitored in real time, and the data is analyzed to determine whether the node has been flooded by interest. In [16], the article uses information entropy-based interest flooding detection mechanism. Determine whether the network node is attacked by comparing the randomness of the content of the interest request content in the PIT entry under normal conditions and when the network is attacked.

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

$p(x_i)$ represents the probability that the same prefix will appear after the interest packet is fragmented. At the same time, the PIT usage rate, PIT information entropy change rate and PIT information entropy are maintained at high values as a basis for accurate judgment.

B. Brief description of the plan

In this paper, we propose a node routing protection scheme based on dynamic reputation mechanism. In the CCN network, the information transfer mechanism must pass through the routed port. We assign an initial dynamic reputation value to each user and adjust the user's reputation value based on the user's daily behavior. The user is classified by the level of the reputation value to determine whether the node route has received the attack.

In the scheme, we set the threshold K in advance according to actual factors, and establish a set U including all users in the node route, a legal user LU , an abnormal user AU and an illegal user ILU , as shown in Fig. 3. All credit value of the user initialization algorithm are set to 1, that is a legitimate user in this state. The user is judged to be an illegal user according to the result of the detection algorithm of the running user's daily behavior. In addition, it is not legal or illegal based on the user's behavior. Users with abnormalities are separated from the LU and placed in the AU . Only when the user is detected as abnormal for many times, the reputation value becomes smaller and smaller. Once the reputation value is reduced below our originally set threshold, the user is detected as an illegal user and moved from the AU to the ILU collection.

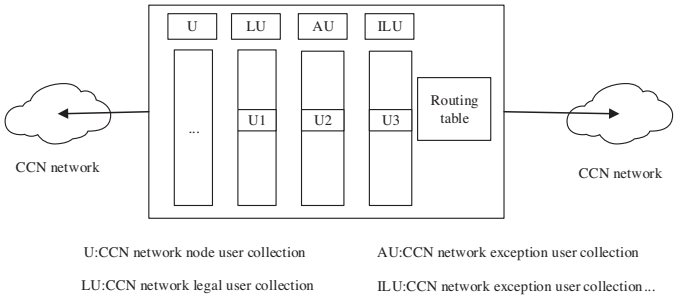

fig. 3. Node routing set classification

In the scheme, four algorithms are set. the Initialization algorithm is the entire network initialization algorithm. Illegal user detection algorithm is used to detect whether the user has abnormal behavior. Calculate the reputation value algorithm is used to calculate the value of the reputation value, which is a dynamic process. Defense function algorithm is used to defend against the illegal user's defense algorithm, and the algorithm can alleviate or mitigate the situation of the user's attack.

C. Specific plan

In this scenario, we consider the entire CCN network as a graph, and the vertices in the graph represent users in the network. Let all users in the network be in the set U, $U=\{u_1,u_2,u_3,...,u_n\}$. Set legal user $LU=\{lu_1,lu_2,lu_3,...,lu_n\}$, abnormal user $AU=\{au_1,au_2,au_3,...,au_n\}$, Illegal user $ILU=\{ILu_1,ILu_2,ILu_3,...,ILu_n\}$, where $n1+n2+n3<=n$. With the above settings, users in the CCN network can be classified into legal, abnormal, and illegal categories. Assume that each user is a legitimate user and set the user's reputation value to 1 at initialization. The abnormal behavior detection function in the Illegal user detection algorithm is used to detect whether the user behavior is legal. According to the result of the Calculate the reputation value algorithm, the user reputation value is dynamically changed. The user is moved from the LU to the AU when the reputation value changes. When the reputation value is below the threshold K, the user will be moved into the ILU set.

Initialization algorithm: In the initialization algorithm, we set each user to be legal. U and LU represent all node users in the network, satisfying $U=LU$, $AU=\varnothing$, $ILU=\varnothing$.

Illegal user detection algorithm：Illegal user detection is a crucial part of the solution. The abnormal user is detected by a certain detection function and added to the AU . The specific method is as follows:

$$f_d(u_i)=\begin{cases}1 & e_{u_i}\in SG\\ 0 & other\end{cases} \tag{2}$$

e_{u_i} represents a user signature, where $i\in\{1,2,3,...,n\}$, and SG represents the signature of the abnormal behavior. If it is found through the detection that the user's behavior characteristics and abnormal behavior characteristics match, we can think that the user belongs to the abnormal user. And then add the user into the AU collection. In the scheme, in order to easily detect abnormal behavior, we need to define several abnormal behavior characteristics, which are defined as follows:

(1) Message response rate (MRR) is abnormal. The MRR value continues to decrease and $I_n>>D_n$. $MRR=\frac{\hat{D}_n}{\hat{I}_n}\times 100\%$, $\hat{I}_n$, $\hat{D}_n$ represent the average receiving port node routing packets and data packets of interest. Under normal circumstances, the number of interest packets and data packets received by the node routing port in the CCN network is equal. When a large file or content is encountered, the MRR value may occur in a short period of time. However, if the number of interest requests is much larger than the data message, it may be a flood attack.

(2) The message response rate (MRR) is abnormal, and the MRR value continues to increase and $D_n>>I_n$. As described in 1, the MRR value is 1 under normal conditions. When the MRR value is abnormal and the number of data packets is much larger than the interest request packet, a spoofing attack may occur at this time. A forged content server continuously injects data packets into the network, disrupting the information flow in the network.

(3) The PIT (Pending Interest Table) usage rate exceeds 80% of the total amount in a short time. The data request message hit rate is extremely low, and the randomness of the data request in the PIT entry is maintained at a very high level. Under normal circumstances, the interest request message may also have a short rise and fall at a certain moment. However, as the entry times out, malicious requests for interest are deleted and maintained within a certain range. In the case of interest flooding or denial of service attacks, there is a short-term increase in PIT usage and a high level of randomness.

(4) A cache is fixed for a fixed node, and the request is repeated for multiple contents in a short time. The goals of interest requests in the network are generally random. If the interest request packet is cached for a fixed node in a short time, and the request is for duplicate content, it may be determined that the routing port of the node is in an abnormal state.

Calculate the reputation value algorithm: After initializing the users in the network, we set the reputation value to 1. The new reputation value is calculated only by the reputation value calculation method when the user behavior is abnormal. Each node route in the algorithm will have its own calculation and evaluation system.

$$F_S(R,T_j,u_i)=\begin{cases}1 & u_i \notin AU \\ 1-L_S(R,T_j,u_i) & u_i \in AU\end{cases} \quad (3)$$

This formula indicates that the node route R calculates the reputation value of the user u_i at time T_j. $L_S(R,T_j,u_i)$ refers to the amount of loss of the user's reputation value, which is determined according to the characteristics of the user's behavior. A user's reputation value is determined not only by the current state, but by the behavioral state over time.

$$L_S(R,T_j,u_i)=\partial \cdot L_t(R,T_j,u_i)+(1-\partial)\cdot L_S(R,T_{j-1},u_i)(0 \le \partial \le 1) \quad (4)$$

$L_t(R,T_j,u_i)$ represents the user integrity change function. $L_S(R,T_j,u_i)$ represents the amount of loss of user reputation value during the first T_{j-1} time. ∂ is a parameter that measures reputation weight $(0 \le \partial \le 1)$. An abnormal user of a suspected attacker is currently in good shape. However, because the previous behavior abnormalities are serious, its reputation value may also be low. Only when a user maintains good performance for a long time and no abnormal behavior occurs, can a good reputation be maintained.

$$L_t(R,T_j,u_i)=\lambda \cdot L_r(R,T_j,u_i)+(1-\lambda)\cdot L_r(R,T_{j-1},u_i) \quad (5)$$

λ is a weight value $(0 \le \lambda \le 1)$, and the $L_r(R,T_j,u_i)$ function represents the loss of integrity of the user u_i. In the scheme, because there is more emphasis on the current state of the user, whether there is an abnormal attack, we set the value of λ to be greater than 0.5. The definition of the function $L_r(R,T_j,u_i)$: $L_r(R,T_j,u_i)=\frac{n_{u_i \in AU}}{n}$ represents the ratio of the number of abnormalities that the user is detected as a possible attack and the total number of detections during that period of time.

Defense function algorithm: The defense mechanism algorithm of the node routing object consists of two parts: (1) delay mechanism, (2) cooperative defense. The delay mechanism mainly uses each node routing object to have an ILU collection, and the collection contains the abnormal node user marked as the attack object. Node routing generates a random delay for each node user through a delay generation algorithm. The node responds immediately to a user interest request that is not considered an attacker. The routing response to two different requester nodes is shown in the figure below. When the legitimate user $U1$ requests the node to cache the content, it will get a timely response. When a $U2$ request is made by an illegal user, it is delayed for a certain period of time. In the collaborative defense, the node route sends a cooperative defense data packet to the neighboring node to inform the attacker of the information. The neighboring node automatically parses the data packet after receiving such a cooperative data packet, and obtains the marked illegal user. Check the ILU table in the node. If such a node already exists, forward the cooperative packet through the broadcast or default port. Otherwise the node user information is added to the ILU U table.

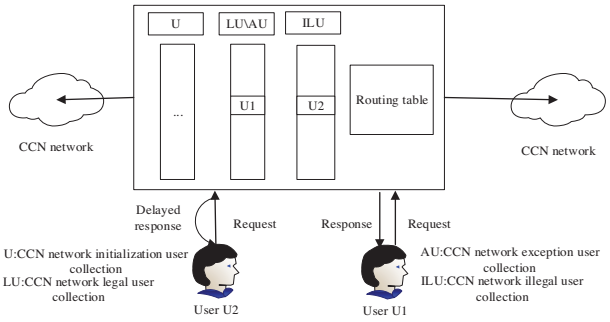

fig. 4. Legal and illegal user request schematic

IV. CASE ANALYSIS

Each network resource after objectification has certain security risks. We need to further study a more complete security solution to ensure the security of various network object resources. The design purpose of this solution is to provide a security guarantee for node routing while maintaining the advantages of the CCN network. In the existing literature, the protection of node routing security in the text is mostly single and has certain defects. In [13] Dai's scheme, it is established that the flooding attack has been detected accurately. Use the routing port number to perform the "reverse path" tracking defense mechanism and return the forged interest packet to mitigate the attack hazard. There are also two drawbacks to using the tracking method: (1) Too much reliance on a single detection mechanism. If the detection mechanism is imperfect or the malicious attack request is scattered, the network burden will be increased. (2) If the malicious interest is an attack against a legal naming prefix, the method of returning the forged interest packet is still adopted, and the request of the normal user is also affected. For example: a legal name for the name "ccn/maze/download/videos/Sun Wukong.mp4", and the detected malicious interest prefix for the naming prefix is "ccn/maze/download/...". Then legitimate users will also be returned a fake backtracking package. If the network is flooded with such a large number of malicious interest packages, legitimate requests for interest will not reach the content server or will not respond at all, which will lead to legitimate server "fraud". In the [17] Compagn scheme, when a port that has detected a node route is subject to a flooding of interest, the node route adopts a method of limiting the traffic of the attack port, so as to achieve the purpose of mitigating, weakening or even eliminating the attack. However, there are two drawbacks to this method of traffic restriction: (1) It will affect the services of legitimate users. The port is not only an interest request port, but also a packet response port. Restricting malicious interest packets can also delay legitimate user requests and also limit legitimate message packets. (2)

Due to the wide range of interest attacks, malicious interest packets are distributed to each network node port after being forwarded by the node. If most of the network port is restricted in traffic, the connectivity of the entire network is bound to be affected.

The purpose of the program design is to effectively combine the advantages of each detection and defense solution. At the same time, it provides security for node routing without affecting the normal request of legitimate users. Compared to other detection and defense schemes, as shown in the table I:

TABLE I. SCHEME PERFORMANCE ANALYSIS TABLE

Design	Detection	defense	granularity	Advantages and disadvantages
Literature [14] Tang scheme	Multi-level, interest package satisfaction rate + abnormal prefix recognition	AIMD collaborative feedback defense	Abnormal prefix	The detection granularity is fine, but the calculation overhead is too large
Literature [15] Goergen scheme	Data mining monitoring	Interest packet number limit	Exception interface	Detection is high on data collection and may limit requests from legitimate users
Literature [16] tour plan	Information entropy change rate	Combination of information entropy fast and slow defense	Abnormal prefix	Timely detection, the defense program has little impact on legitimate users, but the calculation of PIT information entropy is not clear enough and perfect
Literature [13] Dai program	PIT table exception	Interest package "reverse path" traceability	Abnormal port	Restrictions on legitimate users during the tracking process
Literature [17] Compagno scheme	Port data anomaly detection	Port traffic limit	Abnormal port	Normal user services may be affected, and in severe cases, the network may be compromised.
Our solutions	User behavior anomaly detection + reputation value K limit	Port delay + cooperative defense	Abnormal port + Abnormal prefix	Dynamic and timely detection makes it better than other solutions. Port delay + collaborative defense makes it basically not affecting legitimate users.

V. CONCLUSIONS

The CCN network resources are divided into different objects according to their roles in the network. Faced with different network resource objects for security analysis, it highlights several types of attacks faced by node routing objects in the network. For the attack of the node routing object, a node routing security scheme is proposed, which aims to provide security for the node routing without affecting the request of the legitimate user.

VI. ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China No.61672471, Key Technologies R & D Program of He'nan Province (No.172102210059 and No.172102210060), He'nan Province University science and technology innovation team(No.18IRTSTHN012) and Plan For Scientific Innovation Talent of Henan Province (No.184200510010).

REFERENCES

[1] Xylomenos G,Ververidis C, Siris V, et al.. A survey of information-centric networking research[J].IEEE Communications Surveys & Tutorials, 2014, pp. 104-1049.

[2] Koponen, Teemu, et al. A data-oriented(and beyond)network architecture. ACM SIGCOMM Computer Communication Review 37.4, 2007, pp. 181- 192.

[3] Poutsma, Arjen. Data-oriented Translation. Proceedings of the 18th conference on Computational linguistic-Volume 2. Association for Computational Linguistics, 2000.

[4] Zhang, Lixia. et al. Named data networking (ndn) project. Relatorio Tecnico NDN-0001, Xerox Plao Alto Reseatch Center-PARC, 2010.

[5] LIN Tao , TANG Hui , HOU Ziqiang . Content aware network architecture[J]. ZTE Technology Journal, 2011, pp 7-9.

[6] Nabeel M，Shang N，Bertino E.Efficient privacy preserving content based publish subscribe systems[C]//Proceedings of the 17th ACM.

[7] Li Qi，Ravi S，Zhang Xinwen，et al.Mandatory content access control for privacy protection in information centric networks[J].IEEE Transactions on Dependable and Secure Computing, 2015, pp. 1-13.

[8] Liu Yi, Bai Xuefeng, Yang Yubin. Content Centric Networking Privacy Protection Strategy Based on Multi-layer Encryption Mechanism[J]. Computer Engineering and Applications, 2017, pp. 1-5.

[9] Uzun E, DiBenedetto S V, Gasti P, et al.ANDaNA：anonymous named data networking application[C]//Proceedings of the Network and Distributed System Security Symposium , San Diego , California , USA, 2012.

[10] Chaabane A，Cristofaro E D，Kaafar M A，et al.Privacy in content- oriented networking：threats and countermeasures[J].ACM SIGCOMM Computer Communication Review, 2013, pp. 25-33.

[11] TAMOI S, KUMWILAISAK W, JI Y. Optimal cooperative routing protocol based on prefix popularity for content centric networking [C]//Proceedings of 2014 IEEE 39th Conference on Local Computer Networks(LCN). Edmonton, AB: IEEE, 2014, pp. 414 -417.

[12] Vadlamani S, Eksioglu B, Medal H, et al. Jamming attacks on wireless networks: A taxonomic survey[J]. International Journal of Production Economics, 2016, pp. 76-94.

[13] Dai H, Wang Y, Fan J, et al. Mitigate ddos attacks in ndn by interest traceback[C]//Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on. IEEE, 2013, pp. 381-386.

[14] Tang J,Zhang Z,Liu Y,et al.Identifying interest ?ooding in named data net-working[C]//Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things iThings/CPSCom),IEEE International Conference on and IEEE Cyber, Physical and Social Computing. NY: IEEE, 2013, pp. 306-310.

[15] Goergen D, Cholez T, Francois J, et al. Security monitoring for content- centric networking[M]//Data Privacy Management and Autonomous Spontaneous Security. Germany: Springer, 2013, pp. 274–286.

[16] You Rong. DDoS attack detection and prevention in content center network [D]. Shanghai Jiaotong University, 2015.

[17] Compagno A,Conti M, Gasti P, et al. Poseidon: Mitigating interest flooding DDoS attacks in named data networking[C]//Local Computer Networks (LCN), 2013 IEEE 38th Conference on. IEEE,2013, pp. 630-638.