Research on Node Routing Security Scheme Based on Dynamic Reputation Value in Content-centric Network

Jianwei Zhang[1][0000-0002-9291-3602], Chunfeng Du[2][0000-0003-0097-5003], Zengyu Cai[2][0000-0001-8824-0815] and Zuodong Wu[1][0000-0003-1204-9381]

[1] Zhengzhou Institute of Light Industry, School of Software, china
[2] Zhengzhou Institute of Light Industry, School of Computer and Communication Engineering, china
lncs@springer.com

Abstract. Content-centric network (CCN), as a new generation of network architecture with subversive changes to traditional IP networks, has attracted widespread attention and in-depth study from domestic and foreign scholars for its efficient content distribution, multi-path and secure routing features. The CCN network design architecture has many advantages and it is also easily used illegally, which brings certain security problems. For example, objectified requesters, publishers, content, and node routes face privacy disclosure, privacy detection, content disclosure, fraud, and denial of service attacks. At present, the domestic research focus on CCN network is still more about its cache advantages and how to improve routing performance. A node routing security scheme based on dynamic reputation value is proposed for the security of node routing. It can detect if a node route is attacked and defends it in a timely manner, without affecting the node's routing advantages and normal user requests, which to provide security for content-centric network node routing.

Keywords: Content-centric Network, Security Problems, Dynamic Reputation Value, Node Routing.

1 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 quality of service (QOS) of the service provider, and to comply with the development of the future network, Since 2006, domestic and foreign scholars have carried out many new-generation Internet architecture research projects. Among these designs with content information as the core of the network architecture, the CCN network is the most representative[1-5].

The CCN network implements the process of communication from "host-host" to "request content-acquisition content". The main body of the service is more content

than storage location. Different from traditional IP networks, node routing can cache content information in order to shorten information request time and improve communication efficiency. The special architecture design and unique advantages of CCN have also been paid attention by attackers when receiving extensive attention from academic circles. At present, the research content of CCN networks in the academic community is mostly concentrated on caching and routing, and there are not many studies 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].

2 Analysis of CCN Network Objectification Division and Security Issues

2.1 CCN network objectification

In the communication process, the request data packet is issued by the content requester and is routed by the node. In the node route, if the interest request content is already cached, the data packet is returned. Otherwise, the node route broadcast or the default port forwarding is used to continue to request the data packet until the interest packet reaches 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 [8,9] as shown in fig. 1.

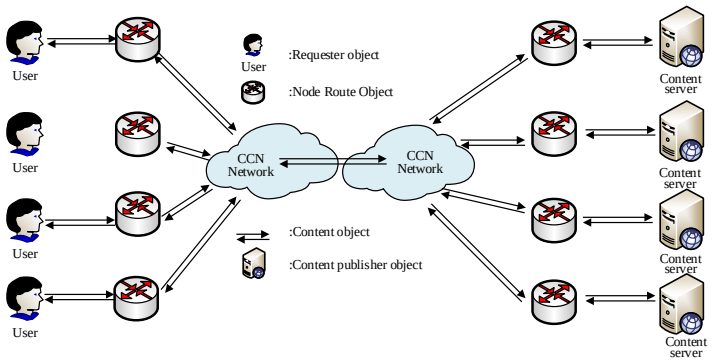

Fig. 1. CCN network resource objectification

Content requester objects: subscribers and consumers of content information in the CCN network, origins of network communications, and data content service subjects.

Content publisher object: The originator and producer of content information in the CCN network and the source of communication content information.

Content objects: The core of network communications, information delivery entities, including specific content information such as interest packages, data packages, and cached copy contents.

Node-routing object: The infrastructure of communication in a CCN network. This is specialized as a router node and contains the core and edge routes.

2.2 Analysis of Node Route Object Security

The request and release of content information in the CCN network is the basis of the communication of the service subject[10,11]. The secure communication between agents can only be achieved if the process consistency between the requester object and the issuer object is guaranteed. Currently, the security problems of node routing include resource exhaustion, interference attacks, and flooding.

Resource exhaustion: Resource exhaustion attacks in the CCN network are divided into overall and partial resource exhaustion. The former is by sending a lot of request information. After storage and forwarding of routing nodes, a large amount of request information and content information are directly or indirectly distributed in the network. The network link is congested and the network load is increased. As a result, the resources in the CCN network are exhausted, and the node route rejects the service. The latter transmits a large number of data packets. The purpose is to route individual edge nodes in the CCN network to reduce the routing performance, increase the response time of the routing, and reduce the data response efficiency.

Interference attack: The attacker masquerades as a trusted legal user and sends a large number of malicious or unnecessary interest packets to the node to disrupt the flow of information in the system[12,13]. Unlike resource exhaustion, an attacker who is disguised attacks the shared node in the link and forwards this node to other nodes, as shown in Fig 2.

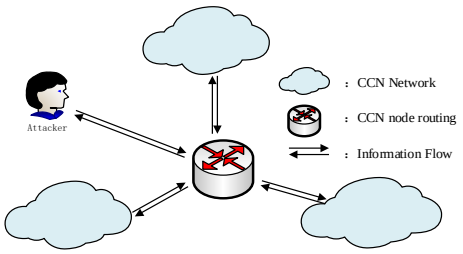

Fig. 2. Interference attack

Flooding attacks: There is no host identifier in the CCN network and it cannot be searched by IP as it is in an IP network. When a CCN node receives a flooding attack, the subsequent requests are ignored because the nodes can process a limited number of requests[14]. This attack does not consider whether the request is legitimate or not. Eventually it will cause the node to reject all service requests.

3 CCN network node routing security protection scheme

3.1 Related research

In 2014, Tang et al. [15] proposed that a two-stage hierarchical detection method for node flooding attacks can be used to reflect the proportion of malicious interest packets according to the interest packet satisfaction rate. S(t)=ΔD/ΔI, ΔD represents the average number of received packets per 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. [16] 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 [17], the information entropy-based interest flooding detection mechanism is adopted in the article. By comparing the randomness of the content name of the interest request in the PIT entry, it is judged whether the network node is attacked under normal conditions and when the network is attacked.

$$\mathrm{H(X)} = -\sum_i^n p(x_i) \log_2 p(x_i) \tag{1}$$

Where $\mathrm{p}(x_i)$ 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.

3.2 An Introduction

Brief description of the plan. Considering the attack of node routing objects in CCN network, we propose a node routing protection scheme based on dynamic reputation mechanism. 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, and then to determine whether the user is an illegal user based on the detection result of the detection algorithm running daily user behavior. In addition, not one based on a user's behavior on the judge legally or illegally, abnormal user will be separated into the AU from LU, only when the user repeatedly been detected as abnormal, reputation value will become smaller and smaller . Once the reputation value is reduced below our

originally set threshold, then the user is detected as an illegal user and moved from the AU to the ILU collection.

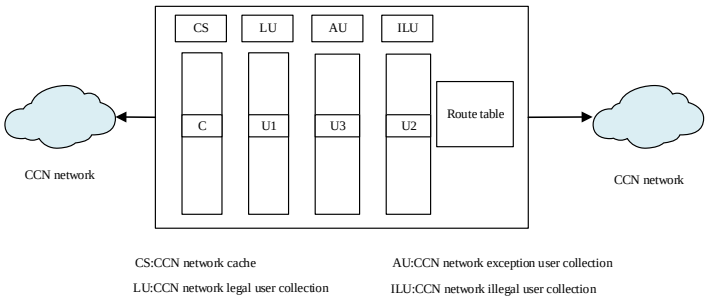

Fig. 3. Node routing set classification

In the scheme, four algorithms are set: the Initialization algorithm is the entire network initialization algorithm; Illegal user detection: The algorithm is used to detect whether the user has abnormal behavior; Calculate the reputation value: The algorithm is used to calculate the value of the reputation value, which is a dynamic process; Defense function The 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.

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, $U = \{u_1, u_2, u_3, \dots, u_n\}$. Set legal user $LU = \{lu_1, lu_2, \dots, lu_{n1}\}$, abnormal user $AU = \{au_1, au_2, au_3, \dots, au_{n2}\}$, Illegal user $ILU = \{ilu_1, ilu_2, \dots, ilu_{n3}\}$, 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, that is, U and LU represent all node users in the network, and have U=LU, AU=∅, ILU=∅.

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 $\in \{1,2,3,\dots,n\}$, 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:

- Message response rate（MRR）is abnormal. The MRR value continues to decrease and $I_n \gg D_n$. MRR $= \frac{\widehat{D_n}}{\widehat{I_n}} \times 100\%$, $\widehat{I_n}$, $\widehat{D_n}$ 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.
- 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 under normal conditions is 1. 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.
- 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 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.

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.

$$F_s(R, T_j, u_i) = \begin{cases} 1, & u_i \notin AU \\ 1 - L_s(R,\ T_j,\ u_i), & u_i \in AU \end{cases} \tag{3}$$

Indicates that the node route R calculates the reputation value of the user u_i at time T_j. Where $L_s(R,\ T_j,\ u_i)$ 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.

$$L_s(R,\ T_j,\ u_i) = \partial \cdot L_t(R,\ T_j,\ u_i) + (1 - \partial) \cdot L_s(R, T_{j-1}, u_i) \tag{4}$$

$L_t(R,\ T_j,\ u_i)$represents the user integrity change function, $L_s(R, T_{j-1}, u_i)$ represents the loss of user reputation value in the first T_{j-1}time, ∂ is a measure A parameter of reputation weight ($0 \le \partial \le 1$). If an abnormal user of a suspected attacker is in a good state and has no abnormal behavior, but because the previous behavior is abnormal, the reputation value may be low. Only when a user maintains good performance for a long time and no abnormal behavior occurs, can a good reputation be maintained.

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

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 number of times the user is detected as an abnormal user who may have an attack and the time The ratio of the total number of detections within.

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 set. The set contains the abnormal node users marked as attack objects. The node routing generates a random delay for each node user through the delay generation algorithm. The routing response to two different requester nodes is shown in Fig 4.

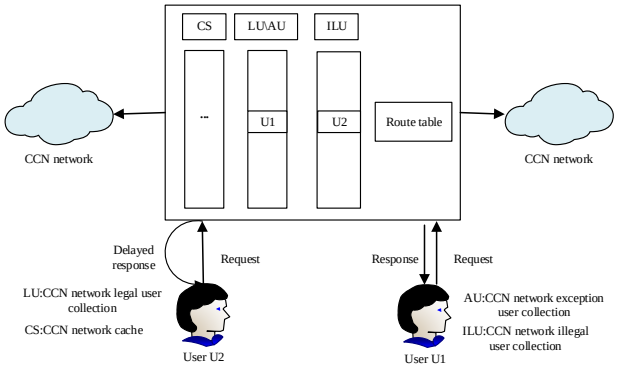

Fig. 4. Schematic diagram of a legal/illegal user request

When the legitimate user U1 requests the node to cache the content, it will get a timely response, and when the U2 request is made by the illegal user, it will be delayed for a certain 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. After receiving the coordinated data packet, the neighboring node automatically parses the data packet to obtain the marked illegal user, and checks the ILU table in the own node. If such a node already exists, the cooperative packet is forwarded through the broadcast or default port. Otherwise, the node user information is added to the ILU table.

4 Case analysis

Each network resource after objectification has certain security risks, and 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 scheme for node routing while maintaining the advantages of the CCN network. In the existing literature, the protection schemes for node routing security in the text are mostly single and have certain defects.

The purpose of the scheme design is to effectively combine the advantages of each detection and defense scheme, and at the same time provide security for node routing without affecting the normal request of legitimate users. Compared to other detection and defense schemes, as shown in the tab. 1.

Table 1. Scheme Performance Analysis Table.

Design	Detection	defense	granularity	Advantages and disadvantages
Literature [10] 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 [11] 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 [12] 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 [9] Dai program	PIT table exception	Interest package "reverse path" traceability	Abnormal port	Restrictions on legitimate users during the tracking process
Literature [13] 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.

In [9] Dai's scheme, it is established that the flooding attack has been detected accurately. Use the routing port number to perform "reverse path" tracking 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 not perfect or the malicious attack request is scattered, it will also increase the network burden; (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 cause the legitimate server to "fallen".

In the [18] 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 is drawback to using this method of traffic limitation: it affects the services of legitimate users. The port is not only an interest request port, but also a packet response port. Limiting the malicious interest packet will also make Legitimate user requests are delayed, and they also limit the response of legitimate packets.

5 Conclusion

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.

Acknowledge

This work is supported by National Natural Science Foundation of China (No.61672471, No.61502436), 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), Cernet Network (NGII20160103).

References

1. Xylomenos G,Ververidis C, Siris V, et al.: A survey of information-centric networking research[J]. In: IEEE Communications Surveys & Tutorials, 16(2): 104-1049 (2014).
2. Koponen, Teemu, et al.: A data-oriented(and beyond)network architecture. ACM SIGCOMM Computer Communication Review 37.4(2007): 181-192.

3. Poutsma, Arjen.: Data-oriented Translation. In: 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，14(2): 7-9 (2011).
6. Nabeel M, Shang N: Bertino E.Efficient privacy preserving content based publish subscribe systems[C]. In: Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, 133-144 (2012).
7. Li Qi，Ravi S，Zhang Xinwen，et al.: Mandatory content access control for privacy protection in information centric networks[J]. In: IEEE Transactions on Dependable and Secure Computing, 1-13(2015).
8. Liu Yi, Bai Xuefeng, Yang Yubin.: Content Center Network Privacy Protection Strategy Based on Multi-layer Encryption Mechanism[J]. Computer Engineering and Applications, 53(5): 1-5 (2017).
9. Mirkovic J, Reiher P.: A taxonomy of DDoS attack and DDoS defense mechanisms[J]. In: ACM SIGCOMM Computer Communication Review, 34(2): 39-53 (2004).
10. Uzun E，DiBenedetto S V，Gasti P，et al.: ANDaNA：anonymous named data networking application[C]. In: Proceedings of the Network and Distributed System Security Symposium，San Diego，California，USA(2012).
11. Chaabane A，Cristofaro E D，Kaafar M A，et al.: Privacy in content-oriented networkin g：threats and countermeasures[J]. ACM SIGCOMM Computer Communication Review, 43(3)：25-33 (2013).
12. TAMOI S, KUMWILAISAK W, JI Y．: Optimal cooperative routing protocol based on prefix popularity for content centric networking [C]. In: Proceedings of 2014 IEEE 39th Conference on Local Computer Networks(LCN),Edmonton，AB: IEEE,414 -417 (2014).
13. Mpitziopoulos A, Gavalas D, Konstantopoulos C, et al.: A survey on jamming attacks and countermeasures in WSNs[J]. Communications Surveys & Tutorials, IEEE, 11(4): 42-56 (2009).
14. Dai H, Wang Y, Fan J, et al.: Mitigate ddos attacks in ndn by interest traceback[C]. In: Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on. IEEE, 381-386 (2013).
15. Tang J, Zhang Z, Liu Y, et al.: Identifying interest ?ooding in named data net-working[C]. In: 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, 306-310 (2013).
16. Goergen D, Cholez T, Francois J, et al.: Security monitoring for content-centric networking[M]. In: Data Privacy Management and Autonomous Spontaneous Security. Germany: Springer, 274–286 (2013).
17. You Rong.: DDoS attack detection and prevention in content center network [D]. Shanghai Jiaotong University(2015).
18. Compagno A,Conti M, Gasti P, et al.: Poseidon: Mitigating interest flooding DDoS attacks in named data networking[C]. In: Local Computer Networks (LCN), 2013 IEEE 38th Conference on. IEEE, 630-638 (2013).