ISBN 978-981-11-0008-6
Proceedings of 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016)
Tokyo, Japan, 17-19 June, 2016, pp. 261-271
doi: 10.18178/wcse.2016.06.041

Modeling and Defense Denial-of-Service in Content-Centric Networking

Tao Feng [1], Jiong Zhao [1], Xian Guo [1] and Chunyan Liu [2 +]

[1] School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China
[2] School of Economics and Management, Lanzhou University of Technology, Lanzhou 730050, China

Abstract. In order to solve Denial-of-service problems in Content-Centric Networking (CCN), we develop an analytical model by using queuing theory and consider several important parameters of CCN such as request rate, TTL of PIT entry, the size of CS, finally we use MATLAB to simulate the effect of these parameters on the probability of Denial-of-service and make a brief analysis. Our simulation results show that if we control rate of interest requests, as well as a reasonable set of CS size and TTL of each PIT entry according to different requirements, we could effectively mitigate the damage of Denial-of-service on CCN.

Keywords: content-centric networking (CCN), modeling, denial-of-service, queuing theory.

1. Introduction

With the rapid development of Internet-scale and its original design flaws increasingly showing, IP network is facing new challenges in content delivery and architecture. Traditional Internet is a kind of communication model for the center with the host address, which is relatively rigid and difficult to realize the nearest access to and transmission of network information / content, resulting in low utilization of network resources and unsatisfactory quality of service. Content Centric Networking(CCN)[1-6] is one of the most promising candidates for Future Internet Architecture Program, it makes the content itself become the main means of communication networks, that we focus on “what is” rather than “where”.

In CCN, communication is driven by its receiving end, i.e., the data consumer. In order to obtain an effective content, a consumer needs to send out an Interest packet, which carries a name that identifies a desired content. Another special packet is a Data packet, which carries the real data of the desired content for consumers. In CCN, each node acts as a router function. In order to support data caching and adaptive packet forwarding functions, each CCN router maintains at least three core data structures shown in Figure 1: a Forwarding Information Base (FIB), a Pending Interest Table (PIT), and a Content Store (CS) [7]. CS module is a temporary cache of Data packets that the router has received, in order to meet future Interest packets request; PIT module stores all unsatisfied Interest packets, recording the Interest's name, incoming and outgoing interface(s). When a router receives a plurality of interest packets with the same name, it only forwards the first one upstream toward the data producer; FIB module is populated by a name-prefix based routing protocol, similar to the traditional forwarding table, and guides Interests toward data producers.

In CCN, any consumer asking for the content needs to issue a corresponding Interest that carries the name of the desired content. Forwarding process at a CCN node is shown in Fig. 1: Whenever an Interest packet arrives, CCN router first time to check whether the contents stored in CS could hit it, if the answer is yes, then the router returns the Data packet on the interface from which the Interest came. Otherwise the router looks in its PIT to see whether there is already a corresponding PIT entry with the same name as this interest, and if a matching entry exists, it records the incoming interface of this interest into the PIT entry. In

+ Corresponding author. Tel.: +18794217092; fax: +0931-2976016.
E-mail address: liucy_811@163.com.

the absence of a matching entry, the router will look in its FIB and forward the interest toward the data producer(s), and then both its name and incoming interface are recorded into PIT entry. Whenever a Data packet matching this interest arrives, CCN router first need to find the matching PIT entry and forward the data to all downstream interfaces listed in the PIT entry. Then these PIT entries will be removed, and cache the Data into CS.

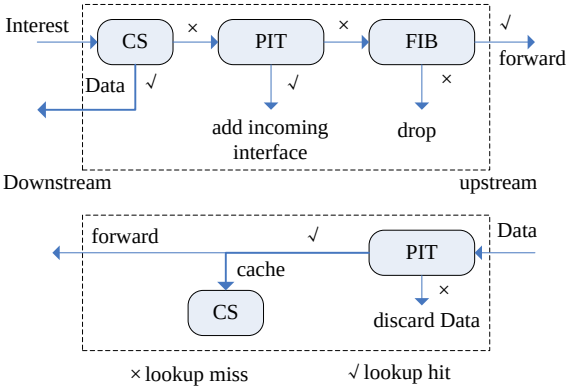

Fig. 1: Forwarding process at a CCN node.

CCN embeds security requirements into its protocol stack at the beginning of architecture design, compared to the traditional Internet "patch" type of trap network security policy, it has inherent advantages [8]. However, CCN similar to the traditional network, still can't completely avoid some threat of network attacks, one of the most typical attacks is Interest Flooding Attack [9]. We know the computing resources and storage space of PIT entries are limited in CCN routers, attackers send a large number of malicious interest packets can exhaust the storage space of a PIT, so that the router cannot create a new PIT entry for storing interest packets and interfaces of legitimate user, resulting in PIT overflow and network congestion. According to different types of malicious interest packets, the attack can be divided into real interests flooding attack and fake interests flooding attack. Real Interest Flooding Attack issues interests with the name of the same prefix information, but its specific name information change constantly, that is, the attackers put a large number of content data packets into CCN networks through a similar "polling" approach, to achieve the purpose of malicious congested network links. Fake Interest Flooding Attack issues interest packets with nonexistent names to miss the CS hit at the CCN router, this kind of interests will not be deleted or be satisfied until the time-to-live (TTL) of PIT entry reaches, so when a large amount of such interest arrives, its memory space will soon be exhausted. Both the two kinds of Interest Flooding Attack can realize Denial-of-service and lead to severe service degradation, or even crash our entire network.

2. Related Work

Interest Flooding Attack as one of the major security threats of CCN, the research of its impacts and countermeasures are being hotspot in the field of network security. The authors in [10] propose a novel and flexible resource management system, and they add control fields in their scheme. According to a given objective function, it can be used to control caching resources and store the contents of high popularity, that consumers have a large number of popularity to get the desired content when CCN suffers Interest Flooding Attack. In [11], the authors summarize the form of network attacks may cause DoS to consumers in CCN, and briefly emphasize the Interest Flooding Attack. The authors in [12] introduce Poseidon: a framework for detecting and mitigating Interest Flooding Attack, it relies on both local metrics and collaborative techniques for early detection of interest flooding. In [13], the authors propose a Interest traceback mechanism, which traces back to the originator of the attacking Interest packets, whenever the size of PIT increases at an alarming rate or exceeds a threshold, Interest traceback process will be triggered. The CCN router sends out the spoofed Data packets, and they are forwarded back to the edge router, then it is notified that the host directly connected with this interface is an attacker.

In [14-16], the authors analyze Interest Flooding Attack and put forward some countermeasures: In [14], they analyze the effect of different forwarding strategies on Interest Flooding Attack, to exploit the best

forwarding strategy that should be implemented in each CCN router when CCN is suffering DoS attacks. In [15], they propose a threshold-based detecting and mitigating (TDM) scheme to detect and mitigate denial of service against content source (DACS attack) based on the frequency that PIT entries in CCN routers expire and by implementing the rate limiter in each router. The results show that TDM achieves high detection ability and good effect on mitigating malicious traffic while bringing in small overhead on countering DACS attack. In [16], they derive a closed-form expression for the DoS probability for users suffering DoS-PIT in their analytical model, while several important factors of NDN networks, such as PIT size, TTL of each PIT entry, popularity of content, and cache size, are considered. Moreover, they demonstrate the accuracy of the proposed model on evaluating the damage effect of DoS-PIT by extensive simulation experiments, simulation results: the CS size can be set to about 16.7% of the total content items of Internet, and the TTL of each PIT entry can be set to about three times of the average RTT of Internet.

In this paper, according to the content popularity distribution in [19] and the data transfer model of CCN in [20], we establish our analytical model for DoS. Compared with [16], we model the forwarding process of CCN by using the different mathematical queuing thought, and extend the scope of the model against DoS, it contains both DoS resulting from excessive legitimate requests and malicious requests, so our paper is a further reflection and expansion to [16].

3. Modeling Denial-of-Service Attacks

In this section we build an analytical model for Denial-of-service attacks. First, we make some reasonable assumptions for our model. Then we introduce some important parameters associated with the model and establish a basic model from the perspective of a single CCN router. Finally we extend our model for a single router to the range of CCN.

3.1. Assumption

(1) We only consider the original sketch of CCN as a case study, regardless of any other modification CCN, such as CCN with interest NACK mechanism.

(2) In the modeling process, we choose the default persistent strategy for PIT: if a router PIT memory space has been filled with large number of interests in a short time, which resulting in PIT memory overflow, the new arriving interest packets will be rejected by the router.

(3) We apply the content of CCN as a Zipf popularity distribution [19]. Suppose there are M content items in CCN, and they are equally divided into K classes of popularity, each content item is segmented into several chunks and has different sizes: σ denotes the average content size in terms of number of chunks (chunks are fix sized). We assume content items of class k are requested with probability $\{q_k\}_{k=1,\ldots,K}$, hence:

$$q_k = c/k^{\alpha} \tag{1}$$

$$c = \left(\sum_{k=1}^{K} 1/k^{\alpha} \right)^{-1}, \ \alpha > 1 \tag{2}$$

(4) We assume interests arrive according to the Poisson distribution, that is, the request of interests is a Poisson process of intensity λ. According to [18], it is reasonable because the process of requests in CCN can be perfectly modeled with Poisson processes, although the whole Internet traffic characteristics coincide with long-range dependent [17], so we can model through Poisson process.

(5) The working process of PIT in CCN routers coincides with the single service window queuing model of mixed M/M/1/n, where n is the queuing capacity of system. According to the nature of the Poisson process, the time interval of Poisson process obeys negative exponential distribution in stationary independent increments process, which corresponds to requirements of queuing model. In this model, the memory of PIT is n. When the PIT is filled, new arriving interests will be discarded if it does not hit the corresponding content in the CS.

3.2. Model Parameters

In the modeling process, we need some important parameters to help us analyze, and these parameters will be used in our derivation below. Table 1 list these key parameters.

Table 1: Parameters of Modeling Denial-of-Service Attacks

parameters	Definition
k	Class of popularity
K	Number of different classes
M	Number of different content items
x	Cache size
σ	Average content size in number of chunks
q_k	Popularity distribution for class k
n_i	PIT size of the *i*th level router
t_{RTT}	Round trip time
t_{TTL}	Time-to-live of the PIT entry
λ	Total rate of interest requests
$\lambda_k(i)$	The rate of interest requests for content of class k at the *i*th lever routers
$p_k(i)$	Miss probability for class *k* at the *i*th level router
$P(i)$	Probability that the *i*th lever router drops Interests with any class because of PIT overflow
$S_k(i)$	Probability that issuing Interests of class *k* cannot be satisfied at the *i*th level router
R_k	Denial-of-service probability for issuing Interests of class k

3.3. A Simple Denial-of-Service Attack Model for One Router

We first derive packet loss rate of a single router in the steady state. In CCN, request aggregation can mitigate the damage of Denial-of-service attacks. In this paper, when Denial-of-service attacks occur, the attackers will choose different names corresponding to different content or the interest packets corresponding to nonexistence content, so we do not consider request aggregation when we build an analytical model for Denial-of-service attacks.

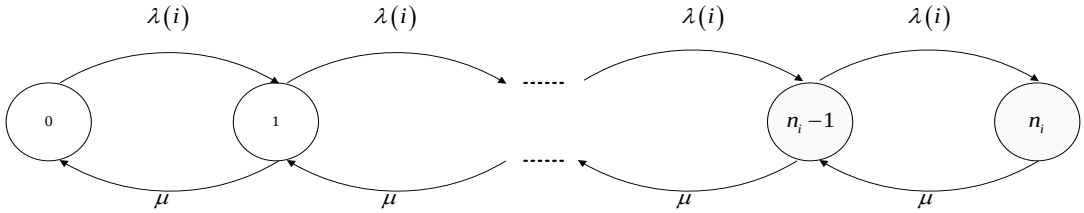

Fig. 2: State flow diagram of PIT of a CCN router.

In the router of CCN, whenever an interest packet arrives and misses CS hit, it would be pended in the PIT entry, and then it would make the number of PIT entries incremented by one. On the contrary, whenever its corresponding Data packet of content arrives or the PIT pending time reaches its TTL, this PIT entry would be deleted and the total number of PIT entries would be reduced by one. We can easily model this process as a continuous time homogeneous Markov chain and assume the total number of PIT entry at the ith level router is n_i , the corresponding Markov chain is defined as follows: In the ith router, state 0 represents there is no interest record, state 1 represents there is an interest record, and by this analogy, state n_i represents

there are n_i interest records. State n_i means the memory resources of PIT entry are completely exhausted, and resulting in denial of service, the following interest packet will be dropped. The corresponding queue model is $M/M/1/n_i$, its state flow diagram is shown in Fig. 2.

Because all the states are interoperability in the system, and the state is limited, so it must have stationary distribution. According to the knowledge of queuing theory, we can obtain the loss probability of the system as follows:

$$P_{loss} = \pi_{n_i} = \rho^{n_i}\pi_0 = \frac{1-\rho}{1-\rho^{n_i+1}}\rho^{n_i} \tag{3}$$

In equation (3), $\rho = \lambda(i)/\mu$.

As the Table 1, we denote $P(i)$ as the Probability that the ith lever router drops Interests with any class because of PIT overflow, which can be expressed as follows:

$$P(i) = P_{loss} \tag{4}$$

Then, we deduce $P(\mathrm{i})$.

Based on [20], the stationary miss probability denoted as $p_k(i)$ is as follows:

$$p_k(i) = p_k(1)\prod_{l=1}^{i-1} p_k(l) \tag{5}$$

$$p_k(1) \approx e^{-\frac{\lambda}{m}q_k g x^{\alpha}} \tag{6}$$

For large x, where $g = \left\{\lambda c\sigma^{\alpha} m^{\alpha-1}\Gamma\left(1-\frac{1}{\alpha}\right)^{\alpha}\right\}^{-1}$.

Now we deduce the $\lambda_k(i)$. In CCN, the interest packets arriving at each router may not totally arrive at its upstream router, because some of these interest packets may be satisfied by the CS hit or be dropped because of PIT overflow at the downstream router. So we can deduce the arriving rate of interest packets that requesting content of class k at the ith level router as follows:

$$\lambda_k(i) = \begin{cases} \lambda q_k & i = 1 \\ \lambda_k(i-1)\, p_k(i-1)\left[1 - P(i-1)\right] & i > 1 \end{cases} \tag{7}$$

Based on equations (5-7), the total rate of requesting interests that can enter PIT entry at the ith level router is $\lambda(i) = \sum_{k=1}^{K} \lambda_k(i)\, p_k(i)$, because only the requesting interests miss CS matching of the router, can it be recorded in the PIT entry. The requesting interests contain both legitimate interest packets and illegal interest packets. Illegal interest packets request nonexistence content, that is, it bypasses the CS directly into the PIT entry, its missed probability for class k is 1.

We define the number of PIT entry (queue length) caused by the arrival interest into the router as L, and the average service time of the interest packets is t, so the constraint relationship between the two is:

$$L = \sum_{k=1}^{K} \lambda_k(i) p_k(i) t \tag{8}$$

On the other hand, the service time of each legitimate interest packet is t_{RTT}, the time of interest packet timeout (including illegal interest packets and the unsatisfied legitimate interest packets). The queue length L can also be expressed as follows:

$$L=\left[\sum_{k=1}^{K}\lambda_k(i)\,p_k(i)\right]t_{RTT}+\lambda_k(i)t_{TTL} \tag{9}$$

Based on equations (8) and (9), we can calculate the average service time of each interest packet as follows:

$$t=t_{RTT}+\lambda_k(i)t_{TTL}\Big/\sum_{k=1}^{K}\lambda_k(i)\,p_k(i) \tag{10}$$

We denote the service rate μ as the average rate that PIT entries are deleted from router after hitting the corresponding data packets or its TTL arrives, so the relationship between μ and t can be expressed as follows:

$$\mu=1/t \tag{11}$$

If we set $\rho=\sum_{k=1}^{K}\lambda_k(i)\,p_k(i)\Big/\mu$, based on equations (10) and (11), we obtain,

$$\rho=\left[\sum_{k=1}^{K}\lambda_k(i)\,p_k(i)\right]t_{RTT}+\lambda_k(i)t_{TTL} \tag{12}$$

From equations (3), (4) and (12),we can obtain：

$$\begin{aligned}P(i)&=\frac{1-\rho}{1-\rho^{n_i+1}}\rho^{n_i}\\&=\frac{1-\left\{\left[\sum_{k=1}^{K}\lambda_k(i)\,p_k(i)\right]t_{RTT}+\lambda_k(i)t_{TTL}\right\}}{1-\left\{\left[\sum_{k=1}^{K}\lambda_k(i)\,p_k(i)\right]t_{RTT}+\lambda_k(i)t_{TTL}\right\}^{n_i+1}}\left\{\left[\sum_{k=1}^{K}\lambda_k(i)\,p_k(i)\right]t_{RTT}+\lambda_k(i)t_{TTL}\right\}^{n_i}\end{aligned} \tag{13}$$

3.4. Denial-of-Service Attacks Model for CCN

Based on the conclusion of [20], we can see, both in the binary tree topology or line topology, the hit ratio (or failure rate) of interests requesting for different popularity content is consistent in the network cache. Therefore, we adopt a unified line topology to study related theoretical derivation work. Fig. 3 is a compact topology of CCN.

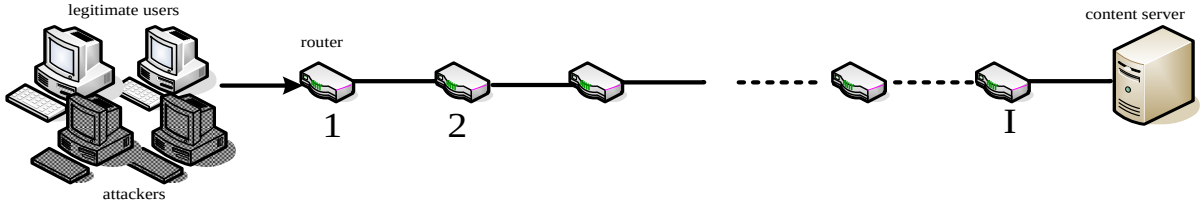

Fig. 3: A small line topology of CCN.

Denote the probability that issuing interests requesting for content of class k can't be satisfied at the ith level router as $S_k(i)$, that is, these interests can't be satisfied by any CS among all the downstream routers before the ith level router, and these routers don't appear Denial-of-service, so it guarantees that interest packets don't be discarded, such that they can be forwarded to the ith level router, but they are discarded till they successfully reach the ith level router.

Based on the above analysis, we can obtain:

$$S_k(i)=\left[\prod_{j=1}^{i}p_k(j)\right]\left[\prod_{l=1}^{i-1}\left(1-P(l)\right)\right]P(i) \tag{14}$$

As shown in Fig. 3, it has I levels of router in CCN. So we denote the Denial-of-service probability as R_k, which is defined as the probability that interests requesting for content of class k can't be satisfied throughout the whole CCN, this parameter can reflect the damage degree of Denial-of-service on CCN. According to our analysis, R_k is equivalent to the union set of dropping probability of interest packets from the first level router to the ith level router, so we can deduce it as follows:

$$\begin{aligned} R_k &= \sum_{i=1}^{I} S_k(i) \\ &= \sum_{i=1}^{I} \left\{ \left[\prod_{j=1}^{i} p_k(j) \right] \left[\prod_{l=1}^{i-1} \left(1 - P(l)\right) \right] P(i) \right\} \end{aligned} \tag{15}$$

Above all, we can act R_k as an indicator that quantify the harm degree of DoS attacks to CCN, it not only reflects the degree of malicious consumption of DoS attacks for network resource, but also reflects the loss probability of a network when DoS attacks occur. Obviously, the smaller value of R_k, the smaller loss probability of interest packets in CCN, and the service quality of network is better. Meanwhile, from the equation (13) to (15), we can see the change of some of the parameters will have a very important impact to the size of R_k. Therefore, if we can set network parameters scientifically and reasonably, it is possible to obtain better performance of network security, and also provide a theoretical basis for the safe deployment and application of CCN.

4. Model Simulation and Analysis

In this section we will analyze the theoretical model which we presented in the previous section by using MATLAB tools, including the impact of three parameters: the request rate of interest packets, cache size, TTL of the PIT entry. Then we are compared with the theoretical analysis results of Wang Kai.

We set up 10 popularity classes of content, each class has 12 content items, and each content item is segmented into 10 chunks, namely we have a total of 1,200 content chunks. The average round-trip time of content acquisition is 0.3s, and the number of PIT entry is 15 in our CCN router.

4.1. Probability of Denial-of-Service with Different Request Rates

When we simulate the impact of request rate to R_k, the TTL of PIT entry is set to 1s, its cache (CS) size is 200 chunks, request rates are respectively set to 30 Interests/s,100 Interests/s,1000 Interests/s. Fig. 4 is the simulation results.

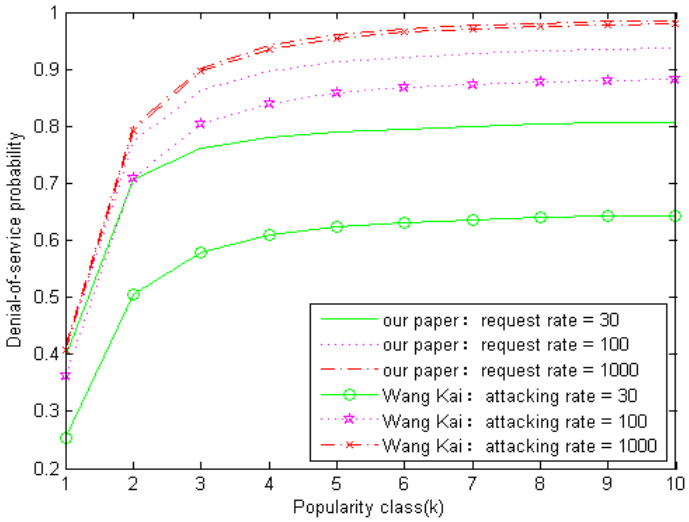

Fig. 4: Probability of Denial-of-service with different request rates.

From Fig. 4, we can see that DoS probability of this paper is much higher than Wang Kai's model at the same rate, but the trend is consistent. In fact, illegal requests and excessive legal requests both can lead

Denial-of-service, there is only illegal requests in Wang Kai's model, so we analyzes the impact of both requests on the DoS probability in this paper. Higher request rate can cause a larger DoS probability, when the request rate reaches 30 Interests/s, in addition to interests requesting content with the popularity of 1, interest DoS probability of others has reached more than 0.5, that is, more than half of the interest packets are discarded, by now the network service quality is very poor. When the rate is too fast, the effect of Denial-of-service in this two methods is the same, namely when the rate is up to 1000 Interests/s, the two curves is basically the same, so our model has a better tolerance on rate. Therefore, whether the request rate or attacking rate, in a certain situation, they will have a great impact on the quality of network services, rate-limiting can solve this problem in some degree, but speed has become the main melody of this world, the number of Internet users is increasing every day, only setting up an appropriate rate not only can meet the requirement of consumers, but also reduce the probability of Denial-of-service.

4.2. Probability of Denial-of-Service with Different CS Sizes

When we simulate the impact of the size of CS to R_k, the TTL of PIT entry is set to 1s, request rate of interest packets is set to 100 Interests/s, and the size of CS is respectively set to 20, 200, and 1100 chunks. Fig. 5 is the simulation results.

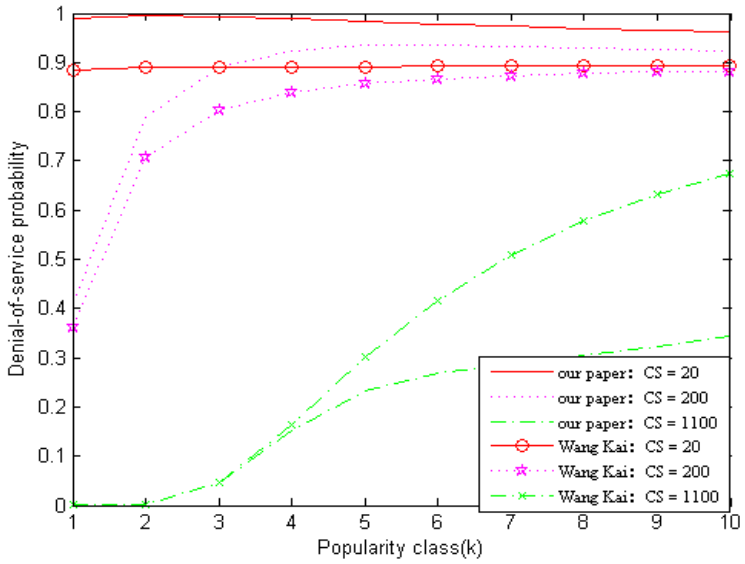

Fig. 5: Probability of Denial-of-service with different CS sizes.

From Fig. 5, we can see that when the CS size of a router is only 1.7% of the total content of the content server (CS is 20 chunks), the interest DoS probability is close to 1, but when the CS size of a router is 91.7% of total content (CS is 1100 chunks), the interest DoS probability of the high popularity is less than 0.2, which means, in this case, even if the network appears to Denial of service, the interest that requesting high popularity content is much more likely to obtain the appropriate content, the middle curve is the best memory size of Wang Kai's model, that is the CS size of a router is 16.7% of total content (CS is 200 chunks). We can't see the best memory size only from three curves in our paper, but the result achieved by our model is basically the same as Wang Kai's model. It can be seen that the model of this paper is also suitable for the Real Interest Flooding Attacks, extend the scope of the model. The larger cache space of a router, the stronger the ability that the router defense Interest Flooding Attack, so in order to resist and mitigate the harm of Interest Flooding Attack, the CCN router should have an appropriately bigger cache size in the case of network hardware conditions permit.

4.3. Probability of Denial-of-Service with Different TTL of PIT Entry

When we simulate the impact of the TTL of PIT entry to R_k, the size of CS is 200 chunks, the request rate of interest packets is set to 100 Interests/s, TTL of PIT entry is respectively set to 0.45s, 0.9s, 3s. Fig. 6 is the simulation results.

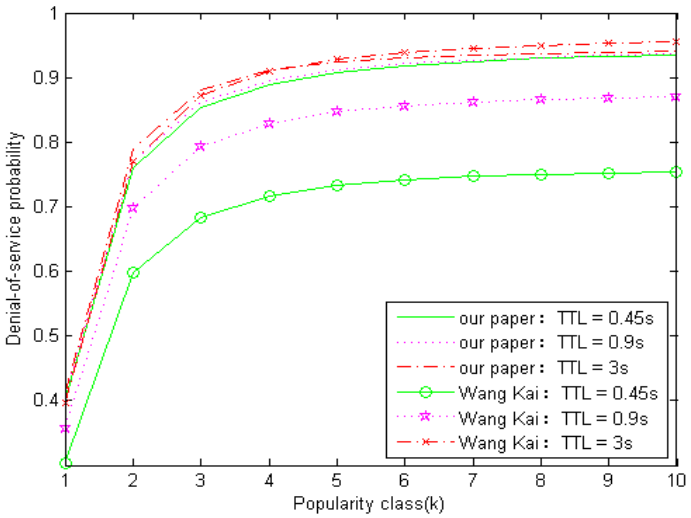

Fig. 6: Probability of Denial-of-service with different TTL of PIT entry.

In this paper, the results are concentrated, but the trend of curve is consistent. Namely, in the case of the same attack strength, the smaller TTL of PIT entry (the premise is that TTL must be greater than RTT), the lower the interest DoS probability, then we can have the higher success rate to obtain the corresponding contents. From Fig. 6, we can see our results more concentrated than Wang Kai's model, when the attack is the Real Interest Flooding Attack, interest request is legitimate, some of the PIT entry can be eliminated before TTL reaches, so TTL has little effect for this kind of attack. Therefore, comprehensive two attacks and from the point view of mitigating the damage degree of Interest Flooding Attack, we can set a smaller value of TTL in the condition of TTL of PIT entry greater than RTT. In this case, we not only can ensure that the interest packets state of PIT entry will not be erased before the corresponding content arrives, but also can obtain a smaller interest DoS probability.

Based on our simulation results and analysis, we know the best way to mitigate the damage of Denial-of-service is to configure the larger CS and the smaller TTL of each PIT entry, and control the request rate of interest packets in Content-Centric Networking (CCN). Whether malicious or legitimate request rate, they all can cause denial of service in the network if we don't control, excessive legitimate requests will cause network congestion, then packet loss will occur, and consequently lead to reduce the service quality of our network; while malicious requests can consume network resources, block the process of the network and also make the network lose interest packets, so it is necessary to control request rate. Meanwhile it is also necessary to reasonably configure the size of CS and TTL of each PIT entry in CCN routers. The larger CS size can cache the more content and the higher hit probability of interest packets, which makes legitimate users can get desired content in the network even if Denial-of-service appears; the smaller TTL of each PIT entry accelerates update frequency of each PIT entry, namely, PIT entry can be released quickly so that subsequent interest packets can enter into PIT entry, which can significantly mitigate the damage effect of Denial-of-service on exhausting the memory resource of PIT in the CCN router.

5. Summary and Future Work

In order to evaluate the damage of Denial-of-service attack in CCN, we build a theoretical mathematical model in this paper, and analyze the damage of Denial-of-service attack in theory. Finally, we simulated the probability of denial-of-service with different request rates, different CS sizes and different TTLs of PIT entry by using MATLAB. Comparing with Kai Wang's model, this paper contains not only DoS-PIT but also network congestion caused by the too fast request rate.

In this paper, we provided a method for the study of this type of Denial-of-service attacks and the theoretical basis for the security setting of controlling some parameters (e.g., request rate, CS size and TTL of PIT entry) of CCN router, but we have an absence of simulation verification with ndnSIM platform. For the future, our work is first using ndnSIM platform for simulation verification, and then extend this

theoretical model, so that it can depict more attack types, and put forward effective measures to limit the damage of this attack.

6. Acknowledgements

This work was supported by the fund: National Natural Science Foundation of China (Grant Nos. 61461027, 61462060), and Science and technology program of Gansu Province (Grant Nos. 1308RJZA277, 145RJZA078). We would like to thank the reviewers for their comments.

7. References

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman. A Survey of Information-Centric Networking. IEEE Communications Magazine 2012; 50(7): 26-36.

[2] G Xylomenos, C.N. Ververidis,V.A. Sins, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K.V. Katsaros, and GC. Polyzos. A Survey of Information-Centric Networking Research. IEEE Communications Surveys & Tutorials 2013; 50(12): 44-53.

[3] Named Data Networking Next Phase (NDN-NP) Proposal. Technical Report NDN-0026, NDN, 2014.

[4] Zhang L, Estrin D, Burke J, et al. Named Data Networking (NDN) Project 2011-2012 Annual Report.

[5] Van Jacobson, Jeffrey Burke, Deborah Estrin, and Lixia Zhang. Named Data Networking (NDN) Project. 2012 - 2013 Annual Report.

[6] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang. A Case for Stateful Forwarding Plane. Computer Communications 2013; 36(7): 736-749.

[7] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, kc claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named Data Networking," ACM Computer Communication Reviews, June 2014.

[8] A. Afanasyev, J. Shi, B. Zhang, L. Zhang, I. Moiseenko, etc. "NFD Developer's Guide," NDN, Technical Report NDN-0021, Revision 4, May 2015.

[9] A. Afanasyev, R Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang. Interest Flooding Attack and Countermeasures in Named Data Networking. Proceedings of IFIP Networking 2013. Brooklyn, New York, USA, May 2013; 1-9.

[10] Widjaja. Towards a Flexible Resource Management System for Content Centric Networking. Proceedings of 2012 IEEE International Conference on Communications (IEEE ICC 2012). Ottawa, ON, Canada, Jun. 2012; 2634-2638.

[11] GASTI P, TSUDIK G, UZUN E, et al. DoS & DDoS in Named-Data Networking. Computer Communications and Networks (ICCCN), 2013 22nd International Conference on. IEEE, 2013; 1-7.

[12] A. Compagno, M. Conti, P. Gasti, and Q Tsudik. Poseidon: Mitigating Interest Flooding DDoS Attacks in Named Data Networking. Proceedings of the 38th IEEE Conference on Local Computer Networks (IEEE LCN 2013). Sydney, Australia, Oct. 2013.

[13] H. Dai, Y. Wang, J. Fan, and B. Liu. Mitigate DDoS Attacks in NDN by Interest Traceback. Proceedings of IEEE INFOCOM 2013 Workshop on Emeiing Design Choices in Name-Oriented Networking (NOMEN 2013). Turin, Italy, Apr. 2013.

[14] K. Wang, J. Chen, H. Zhou, Y. Qin and H. Zhang. Effect of Denial-of-Service Attacks on Named Data Networking. ICIC Express Letters 2013; 7(7): 2135-2140.

[15] K. Wang, H. Zhou, H. Luo, J. Guan, Y. Qin and H. Zhang. Detecting and Mitigating Interest Flooding Attack in Content-Centric Network. Security and Communication Networks 2013; 7(4): 685-699.

[16] K. Wang, J. Chen, H. Zhou, Y. Qin and H. Zhang. Modeling Denial-of-Service against Pending Interest Table in Named Data Networking. International Journal of Communication Systems 2013; published online, DOI: 10.1002/dac.2618.

[17] R.G Clegg, C.D. Cairano-Gilfedder, and S.Zhou. A critical look at power law modeling of the Internet. Computer Communications 2009; 33(3): 259-268.

[18] C.D. Cairano-Gilfedder and R.G Clegg. A Decade of Internet Research: Advances in Models and Practices. BT Technology Journal 2005; 23(4):115-128.

[19] L. Muscariello, G Carofiglio, and M. Gallo. Bandwidth and Storage Sharing Performance in Information Centric Networking. Proceedings of the ACM SIGCOMM 2011 Workshop on Information-Centric Networking (ICN 2011). Toronto, ON, Canada, Aug. 2011; 26-31.

[20] G Carofiglio, M. Gallo, L. Muscariello, and D. Perino. Modeling Data Transfer in Content-Centric Networking. Proceedings of the 23 International Teletraffic Congress (ITC). San Francisco' USA, Sept. 2011; 111-118