A Charging/Rewarding mechanism-based Interest Flooding Attack mitigation strategy in NDN

Xin Zhang, Ru Li*
Department of Computer Science
Inner Mongolia University
Hohhot, China
{cszhangxin & csliru}@imu.edu.cn

***Abstract*—Named Data Networking (NDN) is one of the next generation network architectures, the consumer requests the data by sending an Interest packet and the network responds to each request uniquely, effectively avoiding many Distributed Denial of Service (DDoS) attacks under the traditional architecture. However, there is a new type of attack in NDN - Interest Flooding Attack (IFA), in which malicious consumers send a lot of requests for non-existent data, causing the network to fail to serve legitimate consumers. How to accurately identify malicious consumers to fight IFA becomes an urgent problem to be solved. Therefore, this paper proposes a Charging/Rewarding mechanism based on Hidden Markov Model (HMM) to fight IFA. This method is based on the external characteristic parameters of the consumers to establish HMM and then identify malicious consumer. The Hidden Markov Model is established by the Baum-Welch algorithm. The forward algorithm is used to compute the probability of the observed external characteristic parameters sequence appears in the given model, and the Viterbi algorithm is used to predict the state of the consumer. In order to limit the malicious consumer and stimulate the legitimate consumer, the edge router will charge consumers when providing forward service and reward legitimate consumers. Finally, the effectiveness of the countermeasure is verified through experiment. The experimental results show that the countermeasure can increase the consumer Interest packet satisfaction ratio by 85.9% and 88.6% at tree and net-like topology respectively.**

Keywords—Named Data Networking, Interest Flooding Attack, Hidden Markov Model

I. INTRODUCTION

The TCP/IP-based network architecture was designed to address resource sharing. Nowadays, the demand of users for the Internet is content distribution, however, the traditional Internet can't meet this new demand. Therefore, Information Centric Networking (ICN)[1] was proposed. ICN increases the efficiency of content distribution by in-network cache, and the consumer only needs to know the content of the request instead of where the data is. Named Data Networking (NDN)[2] is an instantiation of ICN. In NDN, there are two kinds of packets: Interest packet and Data packet, and each node in NDN maintains a Pending Interest Table (PIT). The PIT stores the interest name and corresponding incoming interface. However, the PIT stores all pending interest names that have not yet been satisfied until a timeout, the malicious consumer can send a number of Interest packets to overflow the PIT in routers resulting in a new type of Distributed Denial of Service (DDoS) attack, called Interest Flooding Attack (IFA)[3]. How to accurately identify malicious consumers to fight IFA becomes an urgent problem to be solved.

Although several countermeasures have been proposed for IFA, the proposed countermeasures does not consider the economic incentive of NDN. If there is no cost, the malicious consumer can utilize the forward service provided by routers to launch attack[4]. Therefore, this paper proposes an IFA countermeasure based on Charging/Rewarding mechanism. The edge router charges consumer when providing forward service. In order to limit the malicious Interest packets and stimulate the legitimate Interest packets, the legitimate consumer should be rewarded.

The NDN edge router determines whether to reward consumer according to their states. If the state of the consumer is legitimate, then reward. The state of the consumer cannot be directly obtained, but the external characteristic parameter of consumer can be directly obtained. Because the Interest packet satisfaction ratio of legitimate consumer and malicious consumer is different, this paper uses consumer Interest packet satisfaction ratio to represent consumer external characteristic parameter. The consumer Interest packet satisfaction ratio is a proportion of the number of retrieved Data packets to the number of Interest packets forwarded for each router interface connecting to the consumer. To obtain the consumer state by consumer Interest packet satisfaction ratio, a model should be established between the consumer Interest packet satisfaction ratio and the consumer state. The actual traffic entering the network represents the consumer traffic. The HMM is a doubly stochastic process with an hidden stochastic process and observable stochastic process. The hidden stochastic process can only be observed through observable stochastic process that produce the sequence of observed symbols[5]. In this paper, HMM is used to predict the consumer state periodically. The HMM contains two states: a hidden state that cannot be directly obtained and an observable state that can be directly obtained. The consumer state corresponds to hidden state, and the consumer Interest packet satisfaction ratio observed corresponds to observable state. Therefore, the relationship between the consumer Interest packet satisfaction ratio and the consumer state can be established by the HMM.

Therefore, this paper proposes a Charging/Rewarding mechanism based on HMM to fight the IFA. The contributions of this paper are summarized as follows:

- This paper proposes an algorithm to detect the malicious consumer based on HMM which was never used before by other proposed solutions.
- This paper proposes an IFA countermeasure based on Charging/Rewarding mechanism. In Charging phase, NDN edge router charges consumer when providing

This work is supported by the National Natural Science Foundation of China under Grant No. 61363079 and the Enhancing Comprehensive Strength Foundation of Inner Mongolia University (No. 10000-16010109-24). *Corresponding Author.

forward service. In Rewarding phase, NDN edge router rewards consumer when the consumer is predicted to be legitimate by HMM.

The rest of this paper is structured as follows: the second part focuses on the related work; the third part on the design of the countermeasure; the fourth part on the evaluation of countermeasure. Finally, the conclusion and future work in the fifth part.

II. RELATED WORK

This section focus on the IFA solutions recently proposed. In 2013, the authors give three countermeasures (Token Bucket, satisfaction-based accept and satisfaction-based push back) to defend IFA[6]. In 2015, Tan N. Nguyen et al. proposed an IFA detection method based on Hypothesis Testing[7]. In 2016, Yonghui Xin et al. proposed an IFA detection and mitigation strategy based on cumulative entropy and relative entropy theory, they used entropy to discover the traffic abnormality. When an IFA is started, the calculated entropy will suffer obvious change[8]. Vetri Selvi et al. developed a Game Theory Model for the IFA[9]. Aubrey Alston et al. proposed in-packet cryptographic mechanism to fight IFA[10]. Ryoki Shinohara et al. proposed an IFA mitigation strategy based on router interface reputation value and PIT statistics[11]. In 2017, Naveen Kumar et al. applied different machine learning techniques to detect IFA, they selected some features for the detection of IFA[12]. In 2018, Ting Zhi et al. proposed an IFA detection mechanism based on Gini impurity, they use the Gini impurity to measure the dispersity of the requested Interest names. When an IFA is started, the Gini impurity will exceed the normal range[13]. Yoshimichi Nakatsuka et al. proposed an detection and mitigation method based on mean and variance using stored hop counts[14]. Gang Liu et al. designed a lightweight m-list table-based IFA detection mechanism, the m-list table used to record malicious Interest packet[15].

NDN leverages the capabilities of cache to increase data acquisition efficiency while reducing transmission overhead. However, each node is selfish and will not contribute its own resource to cache Data packet if it does not gain profit. Some work have explored the incentive mechanism for caching in NDN[16]-[21]. The nodes should get rewards by caching Data packet. In the same way, when the incentive mechanism is used to mitigate the IFA, the edge router will charge consumer when providing forward service, and the edge router will reward legitimate consumer.

In 2017, Licheng Wang et al. proposed an IFA countermeasure based on payment mechanism. At first, the consumer has a certain amount of virtual money. When the consumer sends the Interest packet, it must pay a certain amount of virtual money to the transiting router. They suppose each consumer can earn virtual money by providing forward service, looking up Interests for others and publishing content[22]. In the view of this paper, in order to limit the malicious consumer and stimulate the legitimate consumer, this paper proposes an IFA countermeasure based on Charging/Rewarding mechanism. The edge router charges consumer and then judges the consumer is legitimate or not. If the consumer is predicted to be legitimate by the HMM, then reward it.

III. DESIGN DETAILS

A. Assumptions

- Suppose that edge routers are trusted authorities in NDN and play the role of central banks for issuing a certain amount of virtual money to each consumer at the beginning.
- Each interface of edge router has a counter to count the number of virtual money of consumer that connected to interface. At time t, the consumer connects to interface j of edge router i, the number of its virtual money is denoted as $V_{ij}(t)$.

B. Charging/Rewarding mechanism

The IFA countermeasures consists of two phases: Charging phase and Rewarding phase. In Charging phase: the edge router charges consumer. In Rewarding phase: in order to stimulate the legitimate consumer, if the consumer is legitimate, reward the legitimate consumer. In the Charging phase, when the interface j of router i receives an Interest packet at time t, the charges are an amount of money that consumer have to pay for forward service. The Price function determines the charges. Because the malicious consumer send a number of Interest packets to overflow the PIT in routers, the more PIT entry come from the interface, the higher the price. The charges are denoted as $C_{ij}(t)$:

$$C_{ij}(t) = Price(PIT_{ij}(t)) \tag{1}$$

In (1), $Price$ is the Price function, $PIT_{ij}(t)$ is the number of PIT entries from the interface j of router i at time t.

The router i decides whether to forward the Interest packets received from the interface j by comparing the value of $V_{ij}(t)$ and $C_{ij}(t)$. If $V_{ij}(t) \geq C_{ij}(t)$, the interface j forwards the received Interest packet and the number of virtual money of interface j are updated by $V_{ij}^{'}(t) = V_{ij}(t) - C_{ij}(t)$. Otherwise, the Interest packet is dropped.

In the Rewarding phase, the interface j of router i uses HMM to predict the state of consumer connecting with interface j and judges whether to reward based on the predicted state. If the consumer connecting to the interface is legitimate, then will reward it, and the virtual money number of the interface j are updated by $V_{ij}^{''}(t) = V_{ij}^{'}(t) + C_{ij}(t)$.

C. Charging phase

Using Charging mechanism to mitigate IFA, the edge router charges consumer when providing forward service. If the charge is successful, the edge router forwards the received Interest packet. Gradually, the number of consumer virtual money is on the decrease, the probability of forwarding Interest packets by the edge router becomes smaller and smaller, and the consumer Interest packets will be limited.

Mankins et al. used dynamic resource pricing model to mitigate DDoS attacks under TCP/IP architecture and tested four kinds of Price functions[23], and Licheng Wang et al. used these Price functions to mitigate IFA in NDN, the four kinds of Price functions are shown below[22]:

Constant function ($p = k$) : the price p is set to a constant k .

Linear function ($p = kc$) : the price p is proportional to the variable c . In this paper, the value of variable c is the number of PIT entries from the interface.

Asymptotic function ($p = kB/(B-c)$) : the price p is raised asymptotically to the variable c . c is the number of PIT entries from the interface, B is the max number of PIT entries from the interface.

Exponential function ($p = \alpha e^{\beta c}$) : the price p is raised exponentially to the variable c . c is the number of PIT entries from the interface.

The growth trend of the four kinds of Price functions are different. Because the constant function charge is fixed and there is no change trend, this paper only considers Linear function, Asymptotic function and Exponential function. The comparison of three kinds of Price functions are shown in Fig. 1.

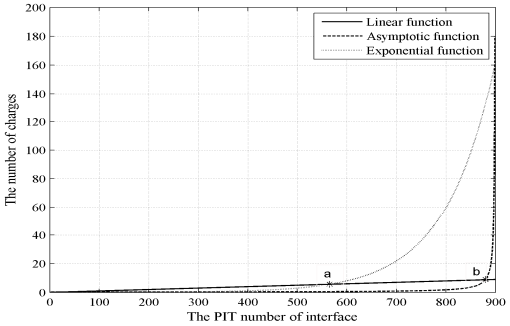


Fig. 1. Comparison of Price function.

It can be found from the graph that the Asymptotic function value is the smallest when the number of PIT entries from a interface is between 0 and a , the Linear function value is in the middle when the number of PIT entries from a interface is between a and b , and the Exponential function value is the largest when the number of PIT entries from a interface is larger than b . When the number of PIT entries from a interface is very small, it is impossible to judge whether it is an interface connects with malicious consumer or legitimate consumer. Because forwarding Interest packets consumes the virtual money. In order to stimulate the legitimate Interest packet, the charges should be small, so the Price function with the smallest function value should be used; When the number of PIT entries from a interface is large, it may be an interface connects with malicious consumer and use the Price function with the largest function value, the malicious Interest packet can be limited quickly.

D. Rewarding phase

In the Charging phase, because of sending Interest packets consumes virtual money, the number of virtual money for the legitimate consumer will become less and less gradually. In order to stimulate the legitimate consumer, the edge router should reward the legitimate consumer.

In the Rewarding phase, the state of the consumer is regarded as hidden state, and the consumer Interest packet satisfaction ratio observed is taken as an observation value to establish the HMM. HMM is determined by initial probability vector π , state transition probability matrix A and observation probability matrix B .

The A defines the hidden states transition probability, the B defines the probability of the hidden state produce observable state.

The HMM can be represented by three tuples.

$$\lambda = (A, B, \pi) \tag{2}$$

The two state Hidden Markov Model established is shown in the Fig. 2.

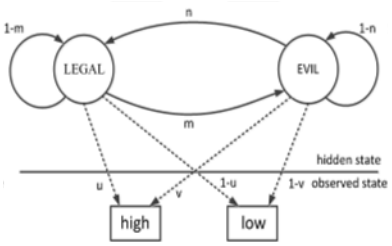


Fig. 2. Two state hidden Markov model.

The motivation of two state Hidden Markov Model is that the state *LEGAL* produces low Interest packet satisfaction ratio with a small probability, the state *EVIL* produces high Interest packet satisfaction ratio with a small probability.

E. Hidden Markov Model

1) Hidden state set Q

In the actual network environment, there are two types of consumer: legitimate consumer and malicious consumer, *LEGAL* state on behalf of the consumer state is legitimate, *EVIL* state on behalf of the consumer state is malicious. The hidden state set $Q = (LEGAL, EVIL)$. The hidden state sequence is $I = (i_1, i_2, ..., i_T)$.

2) Observation state set V

In the actual network environment, the state of the consumer is unknown, and the state of the consumer can only be judged by the observed state. In this paper, the Interest packet satisfaction ratio of the consumer is taken as the external characteristic parameter of the consumer, and the observed external characteristic parameters are divided into two types: state high and low. The observation state set is $V = \{high, low\}$. The converted observation sequence is $O = (o_1, o_2, ..., o_T)$, the conversion method is as follows:

Tan N. Nguyen et al. modeled and analyzed the change of consumer Interest packet satisfaction ratio of each interface of the NDN router[7]: when an IFA starts, the expectation of consumer Interest packet satisfaction ratio is

$$E(Satisfaction(t)) = \frac{(1-P_t)i_t^*}{i_t^* + N_a} \quad (3)$$

In (3), N_a is the number of malicious consumer Interest packets, i_t^* is the number of legitimate consumer Interest packets. At instant t, all Interest packets have the same probability of not being resolved, denoted as P_t.

$$o_{t'} = \begin{cases} high & Satisfaction(t') \geq \dfrac{(1-P_t)i_t^*}{i_t^* + N_a} \\ low & Satisfaction(t') < \dfrac{(1-P_t)i_t^*}{i_t^* + N_a} \end{cases} \quad (4)$$

In (4), $Satisfaction(t')$ is consumer Interest packet satisfaction ratio at time t'.

3) HMM parameter training

According to the state space of the obtained HMM and former observation sequence, the parameters of the Hidden Markov Model $\lambda = (A, B, \pi)$ can be trained. Since the training data only contains the observation sequence $O = (o_1, o_2, ..., o_T)$ and there is no corresponding hidden state sequence $I = (i_1, i_2, ..., i_T)$. The Baum-Welch algorithm is an unsupervised learning algorithm, the parameters of the HMM are trained by using the Baum-Welch algorithm. The training process can refer to reference [5]. After training, the HMM parameters can be obtained.

4) HMM external characteristic parameters compute

After obtaining the model $\lambda = (A, B, \pi)$, given the observation sequence O, the forward algorithm is used to compute the probability of the observed sequence appearing in the model $\lambda = (A, B, \pi)$.

5) HMM state prediction

Given the model $\lambda = (A, B, \pi)$ and the former observation sequence O, this paper use the Viterbi algorithm to find the most likely corresponding state sequence.

F. HMM based IFA Countermeasures

The overall architecture of the countermeasure is shown in Fig. 3. In the Charging phase, the edge router charges consumer according to the Price function. If the number of virtual money of the consumer is more than or equal to the charges, the edge router forwards the Interest packets; Otherwise, the Interest packets are dropped; In the rewarding phase, the edge router uses HMM to predict the state of the consumer connecting with the interface. If the consumer state predicted to be legitimate, then rewards it.

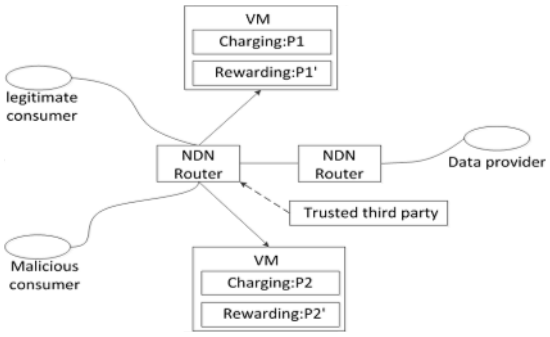


Fig. 3. Countermeasure architecture.

IV. EVALUATION

A. Experiment scenario and setting of simulation parameters

The HMM software used to implement this countermeasure has been implemented by Kanungo [24]. To verify the validity of the countermeasure, an Interest Flooding Attack and countermeasures are implemented in Ndnsim simulation environment and tested in tree topology and net-like topology respectively. The topology is shown in Fig. 4 and Fig. 5, and the topology parameters are shown in TABLE I and TABLE II.

TABLE I. TREE TOPOLOGY PARAMETER

Name	Parameter
NDN router	7
Legitimate node	7
Malicious node	5
Data provider	1

TABLE II. NET-LIKE TOPOLOGY PARAMETER

Name	Parameter
NDN router	90
Legitimate node	47
Malicious node	25
Data provider	1

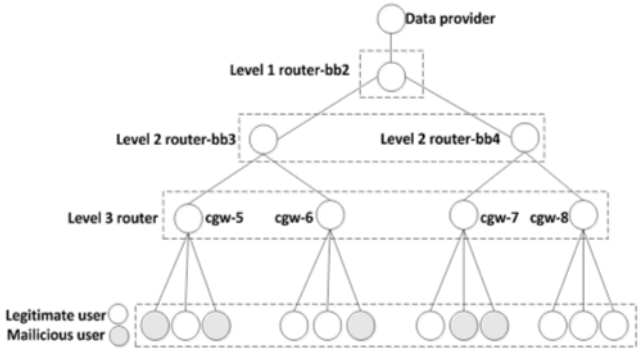


Fig. 4. Tree topology.

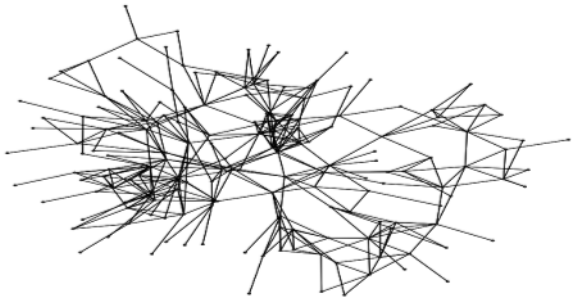


Fig. 5. Net-like topology.

The detailed simulation parameters are shown in TABLE III.

TABLE III. EXPERIMENT PARAMETER

Name	Parameter
Network simulation environment	ns-3.24
NDN simulation environment	ndnSIM
simulation topology	tree topology and net-like topology
Attack start time	10[s]
Interest packet lifetime	1[s]
PIT size	1000
Simulation time	50[s]

B. Simulation results

This paper measures the Interest packet satisfaction ratio of legitimate consumer, PIT size and compare results with: (i) Token Bucket (TB), (ii) Satisfaction-based Accept (SA) , (iii) Satisfaction-based Pushback (SP) [6].

1) Tree topology countermeasure effectiveness

Under tree topology, the countermeasure effectiveness is shown in Fig. 6.

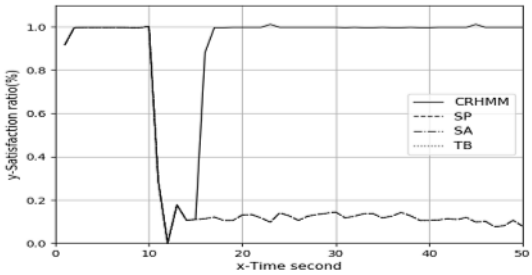
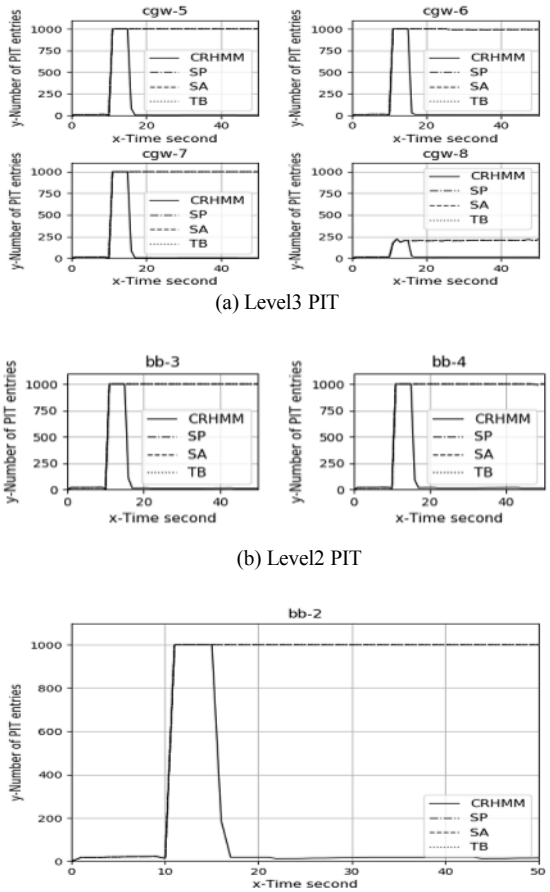


Fig. 6. Tree topology countermeasure effectiveness.

Fig. 6 plot the Interest packet satisfaction ratio mitigation effectiveness of TB, SA, SP and the countermeasures this paper proposed (CRHMM) at tree topology. It can be seen that the consumer Interest packet satisfaction ratio drops rapidly when the malicious consumer starts IFA at time 10.0. The countermeasure effectiveness of TB, SA, SP disappears under high attack rate at tree topology. With the countermeasures this paper proposed, the consumer Interest packet satisfaction ratio improves significantly, about 85.9%.

The PIT change of Level 3 router, Level 2 router and Level 1 router are shown respectively in Fig. 7.



(a) Level3 PIT

(b) Level2 PIT

(c) Level1 PIT

Fig. 7. PIT size comparison.

In Fig. 7, the PIT size mitigation effectiveness of TB, SA, SP disappears under high attack rate at tree topology. In Fig. 7(a), the consumer connected to the router cgw-8 are all legitimate consumer, so the number of PIT entries in the router cgw-8 will not rise to 1000; The number of the malicious consumer connected to the router cgw-5 and cgw-7 are two, and the number of the malicious consumer connected to the router cgw-6 is one, so the number of PIT entries of routers cgw-5 and cgw-7 descends less than router cgw-6. In Fig. 7(b)(c), the number of PIT entries in the router begin to decrease with the countermeasures this paper proposed, and finally returns to normal.

2) Net-like topology countermeasure effectiveness

Under net-like topology, the countermeasure effectiveness is shown in Fig. 8.

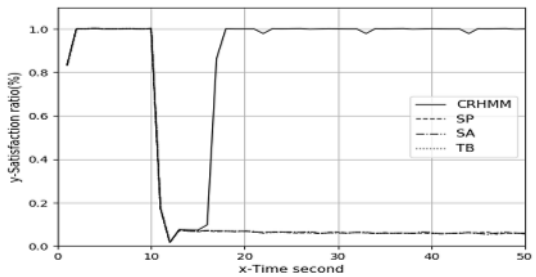


Fig. 8. Net-like topology countermeasure effectiveness

Fig. 8 plot the Interest packet satisfaction ratio mitigation effectiveness of TB, SA, SP and the countermeasures this paper proposed (CRHMM) at net-like topology. It can be seen that the consumer Interest packet satisfaction ratio drops rapidly when the malicious consumer starts IFA at time 10.0. The countermeasure effectiveness of TB, SA, SP disappears under high attack rate at net-like topology. With the countermeasures this paper proposed, the consumer Interest packet satisfaction ratio improves significantly, about 88.6%.

The PIT change of a router along the route is shown in Fig. 9.

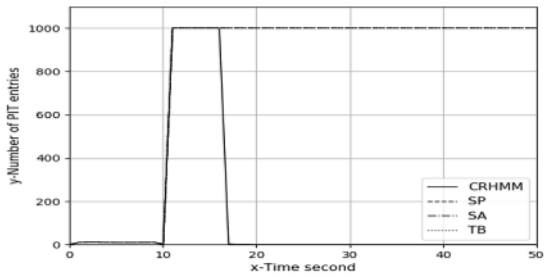


Fig. 9. PIT size comparison..

In Fig. 9, the PIT size mitigation effectiveness of TB, SA, SP disappears under high attack rate at net-like topology. When the malicious consumer starts IFA at time 10.0, the number of PIT entries increases rapidly, reaching the maximum value of PIT. With the countermeasures this paper proposed(CRHMM), the number of PIT entries decreases until reaching the normal value.

V. Conclusion and Future Work

In this paper, a HMM for the prediction of consumer state has been proposed by using its Interest packet satisfaction ratio. Moreover, this paper proposes a Charging/Rewarding mechanism based on HMM to fight IFA, and the countermeasure only run on edge router. Simulation results show that the countermeasure this paper proposed can effectively mitigate IFA and stimulate legitimate consumer. In future work, we plan to develop an more suitable prediction algorithm for external characteristic parameter and consider a more realistic attack model.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant No. 61363079 and the Enhancing Comprehensive Strength Foundation of Inner Mongolia University (No. 10000-16010109-24).

References

[1] Xylomenos G, Ververidis C N, Siris V A, et al. A survey of information-centric networking research[J]. IEEE Communications Surveys and Tutorials, 2014, 16(2): 1024-1049.

[2] Zhang L, Afanasyev A, Burke J, et al. Named data networking[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 66-73.

[3] Gasti P, Tsudik G, Uzun E, et al. DoS and DDoS in named data networking[C]//Computer Communications and Networks (ICCCN), 2013 22nd International Conference on. IEEE, 2013: 1-7.

[4] Li F, Wu J. Frame: An innovative incentive scheme in vehicular networks[C]//Communications, 2009. ICC'09. IEEE International Conference on. IEEE, 2009: 1-6.

[5] Rabiner L R, Juang B H. An introduction to hidden Markov models[J]. ieee assp magazine, 1986, 3(1): 4-16.

[6] Afanasyev A, Mahadevan P, Moiseenko I, et al. Interest flooding attack and countermeasures in Named Data Networking[C]//IFIP Networking Conference, 2013. IEEE, 2013: 1-9.

[7] Nguyen T N, Cogranne R, Doyen G, et al. Detection of interest flooding attacks in named data networking using hypothesis testing[C]//Information Forensics and Security (WIFS), 2015 IEEE International Workshop on. IEEE, 2015: 1-6.

[8] Xin Y, Li Y, Wang W, et al. A novel interest flooding attacks detection and countermeasure scheme in ndn[C]//Global Communications Conference (GLOBECOM), 2016 IEEE. IEEE, 2016: 1-7.

[9] Selvi V, Shebin R. Game theory based mitigation of Interest flooding in Named Data Network[C]//Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on. IEEE, 2016: 685-689.

[10] Alston A, Refaei T. Neutralizing interest flooding attacks in Named Data Networks using cryptographic route tokens[C]//Network Computing and Applications (NCA), 2016 IEEE 15th International Symposium on. IEEE, 2016: 85-88.

[11] Shinohara R, Kamimoto T, Sato K, et al. Cache control method mitigating packet concentration of router caused by interest flooding attack[C]//Trustcom/BigDataSE/ISPA, 2016 IEEE. IEEE, 2016: 324-331.

[12] Kumar N, Singh A K, Srivastava S. Evaluating machine learning algorithms for detection of interest flooding attack in named data networking[C]//Proceedings of the 10th International Conference on Security of Information and Networks. ACM, 2017: 299-302.

[13] Zhi T, Luo H, Liu Y. A Gini Impurity-Based Interest Flooding Attack Defence Mechanism in NDN[J]. IEEE Communications Letters, 2018, 22(3): 538-541.

[14] Nakatsuka Y, Wijekoon J L, Nishi H. FROG: A Packet Hop Count based DDoS Countermeasure in NDN[C]//2018 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2018: 00492-00497.

[15] Liu G, Quan W, Cheng N, et al. Accuracy or delay? A game in detecting interest flooding attacks[J]. Internet Technology Letters, 2018, 1(2): e31.

[16] Xu Y, Li Y, Ci S, et al. Distributed Caching via Rewarding: An Incentive Caching Model for ICN[C]//GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017: 1-6.

[17] Xu J, Xue K, Cao C, et al. Incentive cooperative caching for localized information-centric networks[C]//Wireless Communications and Signal Processing (WCSP), 2017 9th International Conference on. IEEE, 2017: 1-6.

[18] Agyapong P K, Sirbu M. Economic incentives in information-centric networking: Implications for protocol design and public policy[J]. IEEE Communications Magazine, 2012, 50(12).

[19] Ndikumana A, Tran N H, Ho T M, et al. Joint incentive mechanism for paid content caching and price based cache replacement policy in named data networking[J]. IEEE Access, 2018, 6: 33702-33717.

[20] Hajimirsadeghi M, Mandayam N B, Reznik A. Joint caching and pricing strategies for information centric networks[C]//Global Communications Conference (GLOBECOM), 2015 IEEE. IEEE, 2015: 1-6.

[21] Pham T M, Fdida S, Antoniadis P. Pricing in information-centric network interconnection[C]//IFIP Networking Conference, 2013. IEEE, 2013: 1-9.

[22] Wang L, Pan Y, Dong M, et al. Economic Levers for Mitigating Interest Flooding Attack in Named Data Networking[J]. Mathematical Problems in Engineering, 2017, 2017.

[23] Mankins D, Krishnan R, Boyd C, et al. Mitigating distributed denial of service attacks with dynamic resource pricing[C]//Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual. IEEE, 2001: 411-421.

[24] Kanungo T. UMDHMM: Hidden Markov model toolkit[J]. Extended Finite State Models of Language, 1999.