MITIGATE CONTENT POISONING ATTACK IN NDN BY NAMESPACE AUTHORIZATION

Pengfei Yue and Bin Pang

Department of Computer Inner Mongolia University Hohhot, China

ABSTRACT

The Named Data Networking (NDN) immunes to most of the attacks which exist in today's Internet. However, this newborn network architecture may still subject to Distributed Denial of Service (DDOS) attacks if less evaluation is paid. In this paper, we firstly give a survey of the state of art works on the mitigations of the Content Poisoning Attack (CPA) in NDN and discuss their limitations as well. After this, we give out our mitigation and the results from simulations show that with the implementation of our mitigation, the Interest Satisfaction Rate (ISR) of all Consumers maintains a highly acceptable rate even when network is under CPA.

KEYWORDS

The Named Data networking (NDN), Denial of service attack (Dos), Content Poisoning Attack (CPA)

1. INTRODUCTION

Named Data Networking (NDN) [1] is a newly proposed network architecture that aimed to solve the problems exist in today's Internet. NDN changes the Internet paradigm from address-based to data-based and Routers choose to cache the incoming Contents for further requests to make the Content distribution more efficient.

There are two kinds of packets in NDN. An Interest is a request sent by a node, named Consumer, to retrieve resources from the network. Any node in the network has or caches the resources replies the Interest with one or some Contents and this node becomes the Producer of this/these Content consequently. Comparing with the remedy like security solutions, e.g. IP-Sec, DNSSEC, in TCP/IP based network architecture, the security is considered at the early beginning of its design. However, there are some DDos attacks [2], e.g. Interest Flooding Attack (IFA), Content Poisoning Attack (CPA), which may still damage the NDN.

There is an area in the Interest to store the public key or digest of penitential Producer of Content, any immediate node in the network can choose to verify the signature of Content passing by but with lots of difficulties:

First, the computation overhead of signature verifying. Even though the hardware becomes more powerful than ever before, it is hard to achieve thousands of signature verifications at line-speed.

Second, there is no unified authentication system is NDN at this stage, as a result, it may be hard for immediate nodes to retrieve proper keys from the network.

Natarajan Meghanathan et al. (Eds) : CSITEC, CMCA, SP, NECOM, ADCO - 2019
pp. 105-115, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.91109

Third, even though the Consumers can retrieve the public keys of Content Producers from a network with a lot of effort, this kind of network traffic should not be neglected in a network with a large number of nodes.
As a result, malicious nodes can pretend to be any Producers and reply Interests with Contents which may contain fake signatures. The works on Content Poisoning Attack (CPA) which are based on probability check on passing Contents or based Consumers feedbacks all have their limitations. They cannot root out the CPA in NDN with little effort and confidently, since they cannot judge a Content is malicious when it does not pass their checking.

We believe a solution that gives every node in the network the right to verify the validations of passing Contents with less overhead is significant. In this paper, we propose mitigation on the CPA and show its performance by simulations.

The rest of the paper is organized as follows. We analyse the state of art work on the Content Poisoning attack in NDN and give a survey in section two. In section three, we make an analyse on CPA and propose our solution. The simulation and result are shown in section four. We summarize and discuss our future work in section five.

2. CONTENT POISONING ATTACK AND SURVEY

2.1. Content Poisoning Attack in NDN

In NDN, we say that a Content satisfies An Interest means the name prefix in this Content matches the name prefix in Interest and with legitimate signature and useful payload. In CPA, an attacker replies some or all incoming Interests with fake Contents which can be Contents of invalid signatures or useless payload. This can prevent the legitimate Consumer to retrieval Contents and seclude legitimate Contents. Theoretically, in NDN every node can verify the arriving Contents of its own accord, however, the verification is impractical.

In Figure 1, Consumer nodes, which are denoted as C1 and C2, want to retrieve resources from Producer P1 or P2 under the namespace /CS or /BIO, and then they send out Interests. Nodes R1, R2, and R3 are normal nodes and perform as routers for other nodes. If there is no malicious node in this network, the left half of Figure 1, most of the Interests can travel to the right destination and bring Contents back to Consumers. However, if there is a malicious node, which is denoted as M, in this network, it can intercept all Interests and as easy as to reply to them with fake Contents.

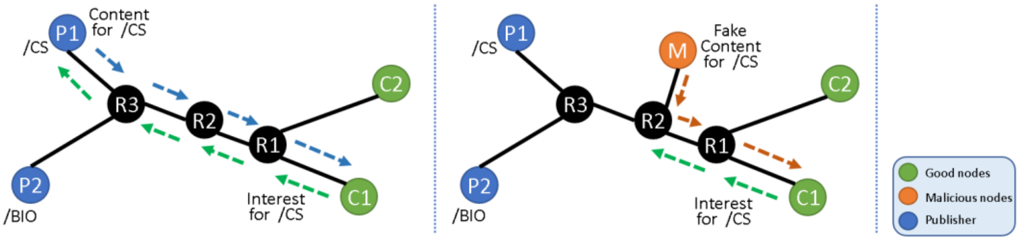

Figure 1. Content Poisoning Attack

The Attacker behaves like a BlackHole in the network, which is depicted in Figure 2 and swallows all incoming Interest. All incoming Interests cannot be satisfied, and it is hard for legitimate nodes to target malicious nodes in the network. For example, node C1 verifies and drops all fake Contents after receiving them. C1 may send warnings to neighbours or other nodes in the network. But these nodes, which have received warnings, face the problem that whether to trust or not because there is no suitable authentication system in the network.

One possible solution is to use the public key infrastructure (PKI), but since NDN is an address-free network architecture, different applications may use different trust authorities. It is hard or even impractical for a Router to retrieve certifications from a lot of trust authorities to verify all passing Contents which arrive at wire-speed.

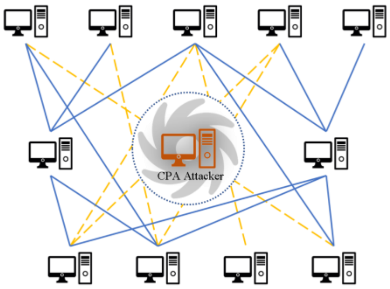

Figure 2. CPA - A BlackHole in the network

2.2. Survey on the mitigations on Content Poisoning Attack

2.2.1. Mitigations based on Probability Check

The authors in [3] proposed a mechanism, named CCNCheck, for intermediate Routers to probabilistically check the signatures of Contents. When an Interest arrives, an intermediate Router will check its cache first. If found, the cached Content will be checked and then returned, otherwise, the Interest will be forwarded according to the forwarding strategy. When a Content arrives, it is checked based on a given probability as well.

In their successive work [4], different probabilities are assigned on core Routers and border Routers. The probabilities on border Routers change dynamically according to the results of signature verifications.

2.2.2. Mitigations based on Consumer Feedback

One solution is based on explicit Consumer feedbacks. The author in [5] used a heavy report from Consumers and goes one step further by giving out two forwarding strategies to discover alternative paths to valid Contents. The heavy report is in the format of Interest which contains the whole fake Content and relevant verification key. Indeed, heavy-weight can bring enough information to upstream nodes, but over-head as well.

While another solution is based on implicit Consumer feedbacks. In NDN, if the returned Content is not the one the Consumer needs, it will be discarded and a new Interest which excludes this Content will be sent out. The proposed scheme in [6] makes use of the exclude information of every Interest to calculate the ranks of all cached Contents. To get the rank, the number of exclusions on Contents, the time distribution of exclusions and excluding Interfaces ratio are recorded and calculated to make the results more precise.

In [7], the Reputation Values (RVs) of Routers' are calculated based on the results of signature verification. Interests are forwarded according to the RVs which means that more Interests will be forwarded to routers with higher RV. RVs follows the liner increasing and exponential decreasing. The most significant part is that its authors believe that Routers may be compromised as well

2.2.3. Others

In [8], the author proposes mitigation called Interest-Key Binding (IKB) rule, that is an Interest must reflect the public key of the Producer. The Producers need to put their public keys or certificates in the KeyLocator field of the Content. The Routers hash the KeyLocator fields of each incoming Content and check if the result matches the PPKD of the PIT entries. If there is no match, the relevant Contents will be dropped, otherwise, they will be cached and forwarded. For a Consumer, it needs to obtain and validate the Producer's public Key in advance. The author proposes three schemes to solve the bootstrap of trust management which is crucial in fetching the public key. The edge Routers do the IKB algorithm and the other Routers do this probabilistically to alleviate the burden of hash computation.

In [9], only the Interests that are satisfied with the cached Contents and verified. The authors propose a modified cache replacement algorithm, called Segmented Least Recently Used (SLRU), and SLRU is used to make sure that the popular Contents remain in Cache longer.

The author in [10] makes use of the Principal Components Analysis (PCA) as a tool to get the major metrics of 18 metrics in NDN Forward Daemon (NFD) to mitigate both Interest Flooding Attack (IFA) and CPA. The Bayesian Network is introduced to correlate the metrics. The authors believe there can mitigate other Attacks since they get enough information from the forwarding. Their mitigation is evaluated with a small topology which consists of only 3 Routers and four hosts. There is only one path between the Consumer and Producer, whether their mitigation can achieve the same benefit in real topology remains uncertain.

In conclusion, the mitigation based on probability check is blunt, since a large probability brings big computation, while smaller one may weak its effort. Nodes which decide to check need to retrieve the proper keys from the network. All nodes on the forwarding path are required to have the knowledge of the security hierarchies of all Contents they decide to verify. While the mitigations based on Consumer feedbacks are not secure because the network should not put their trust on the Consumers which are easier to be compromised. The limitations on signature verification are apparent and urgent to be solved, there needs a light-weight and secure solution to make the nodes in the network to know the validation of Contents.

3. CONTENT POISONING MITIGATION

For the designer of the next-generation network, it is hard to and should not decide to let the network put heavy trust on the Consumers or to let the Routers to do a lot of work which cannot get a definite result. We believe it is the Consumer and Producer 's responsibility to make their Interests and Content verifiable through a solution designed at the very beginning of network designing. By letting the Producer register to the management node first to get the authorization and Consumer to retrieve this authorization by requesting the key&name hash before sending Interests. Every node in the entire network can verify the incoming Contents freely and get definite results.

3.1. General Principle

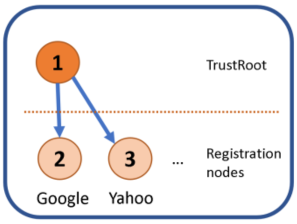

Figure 3. Authentication Hierarchy

The principle of our mitigation is simple and straight-forward: If one node wants to publish Contents as a Producer, it needs to register first.

The whole structure of our mitigation is hierarchical and consists of TrustRoot and Registration Nodes (RegNodes). In Figure 3, the TrustRoot, which is the ultimate root of all trust hierarchies and denoted as 1, delegates some Registration nodes, which are denoted as 2 and 3. The main role of RegNodes is to manage of the registration and retrieve the key&name Hash of some namespaces and to communicate with TrustRoot to get the its authorizations. In Figure 3, RegNode 2 manages namespace /Google while RegNode 3 manages namespace /Yahoo. This delegation of namespaces can be exclusively or not, for example, in a small network, the manager can set one RegNode to manage all namespace it has. A simple process is like this:

1. Each Producer (node which has Contents under one or some namespaces) is required to register to the RegNode to get a binding of its public key and namespace (key&name Hash).

2. Before requesting Contents, Consumer needs to retrieve this binding from a proper RegNode or from the TrustRoot.

3. After received the key&name Hash, Consumer sends out Interest with key&name Hash for Contents. Intermediate Routers on the forwarding path record the key&name Hash in their PITs.

4. Producers or intermediate Routers which have the requested resources in the network return Contents with key&name Hash.

5. Any Router (on the Content returning path) can check the validation of Content of its own accord.

3.2. The Whole Structure and Authentication Procedure

To implement our mitigation, some modifications in the Interest and Content are needed. The key&name Hash is the hash of the Producer’s public key connected with its authorized namespace, and it is stored in a fixed area of Interest and Content (Figure 4). Consumer needs to get the binding first and Producers to register before publishing Contents. All intermediate Routers in the network just need to retrieve the public keys of TrustRoot and do some hash computations and matchings only when they decide to check the passing Contents.

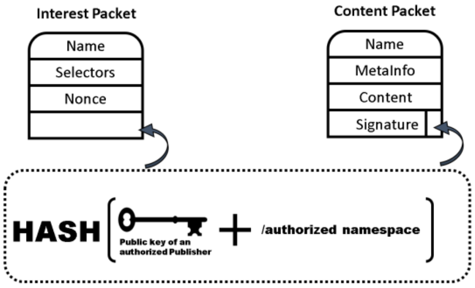

Figure 4. The key&name Hash in Interest and Content

To be specific, we use Figure 5 to illustrate this procedure in more detail:

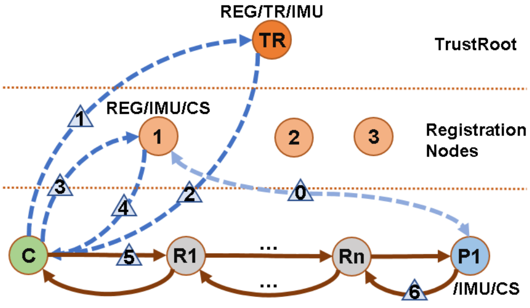

Figure 5. Register and Authentication Procedure

When node C retrieve Contents from Producer P1 under the namespace /IMU/CS. In this network, Registration node 1 manage the namespaces /IMU/CS. Before sending out Interest with name /IMU/CS, node C should do the following steps:

Step 0. P1: register itself to a proper registration node and get the binding (the key&name Hash).
Step 1. C: send a request to the TrustRoot node TR for the location of Registration node (REG/IMU/CS).
Step 2. TrustRoot: reply (node 1).
Step 3. C: send a request to node 1 for the key&name Hash binding.
Step 4. Node 1: reply with the key&name Hash for P1 which is the authorized Producer.
Step 5. C: send out the Interest (with key&name Hash) for /IMU/CS.
Step 6. P1: reply with Content (with key&name Hash).

Usually, the Trust Root may choose to delegate the Registration nodes of each namespace according to its connectivity. In our simulation, this is deliberately set to let our scheme more concise. We do the basic implementation of our scheme in this paper and leave the delegation of Registration nodes to our future work.

3.3. The Mitigation of CPA

After accomplishing all steps above, Contents with key&name Hash bindings are forwarded back to the Consumers. Each node on the forwarding path can verify every passing Content freely. If a Content does not pass the verification, it is simply dropped. Although the overhead of our mitigation mainly lies in the hash computations, mitigation with fewer computations should always be a favourite choice. We let every intermediate Router verifies the incoming Contents based on the usages of PITs.

To be more specific, intermediate Router chooses to verify the incoming Content if the number of in-records of a matching PIT entry of relevant Interests for a namespace exceeds half of the number of all in-records of PIT entries. This is based on the following analysis:

First, to those Interest for certain Contents, more in-records in one PIT entry of intermediate Routers means that the Contents have a large probability to be popular ones.

Second, if one Content is poisoned by an Attacker, Consumer will re-transmit Interest after the failure of signature verification. The re-transmitted Interests will raise the number of in-records in certain PIT entries.

4. SIMULATIONS

We use NDNSim [11], which is a module in a commonly used the network simulator, called Network Simulator (NS) in network research area to test our mitigation on CPA.

When under attack by CPA Attacker, Consumers may retrieve a number of fake Contents and some or all Interests that sent previously cannot be satisfied. We believe that the Interest Satisfaction Rate (ISR) is the prime metric to show the damage of CPA. The ISR defines as follows:

$$ISR = \frac{\text{all received Legitimate Contents per second}}{\text{all Interest sent per second}} \tag{1}$$

When the network is under attack, it will carry more traffics since more re-transmitions occurs. If the total overpass the network capacity, some packets may be dropped no mater they are legitimate or not. In order to reach a clear observation, besides the ISR, we also record the Legitimate Content Rate (LCR) of all Consumers at the same time. The LCR is defined as follows:

$$LCR = \frac{\text{all received Legitimate Contents per second}}{\text{all Contents received per second}} \tag{2}$$

Some parameters in this and next scenario are shown in Table 1.

Table 1. Simulation Parameters in complex scenario

Rate of Interest	5 per second	Distribution of Interests	exaptational
Size of Content	1024KB	Number of Consumers	30
Bandwidth	100MBps	Number of Producers	1
Size of Cache	100 entries	Number of Attacker	1
Payload of Content	1024KB	Simulation time	500s
Forwarding	multicast		

4.1. Scenario “Attacker near Consumers”

We make two scenarios based on the topology (Figure 6) from Rocketfuel [12], which consists more than 100 nodes, and we make a small modification by deleting some irrelevant isolated nodes and links in order to do our simulation. We set different locations of the Attacker in order to see their effects on our mitigation.

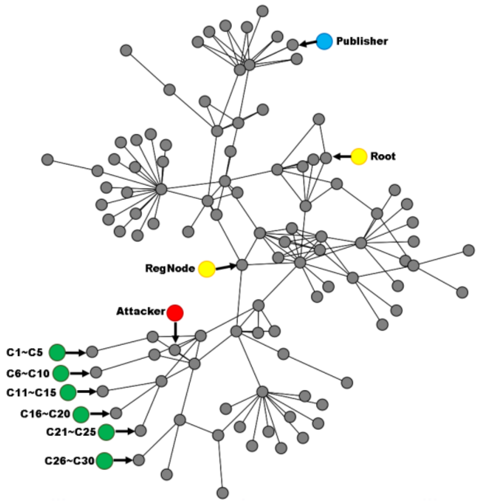

Figure 6. “Attacker near Consumers” Scenario

In Figure 6, the 30 newly added Consumers, which are denoted as green, are divided into 6 groups and connected to 6 edge routers and Consumers in the same group send Interests under the same name prefix. At the same time, the only one Producer satisfies these Interests with legitimate Contents. The Attacker, which is denoted as a red node, is located near Consumers and response all incoming Interests with fake Contents. The purple nodes are the registration node and the blue one is the Producer. The whole scenario is divided into 3 phases: there are only legitimate Consumers and Producers in the first phase. In the second phase, the Attacker is added and attacks the network. Our mitigation is added and mitigates the attack in the third phase. The results from the simulation are shown in Figure 7.

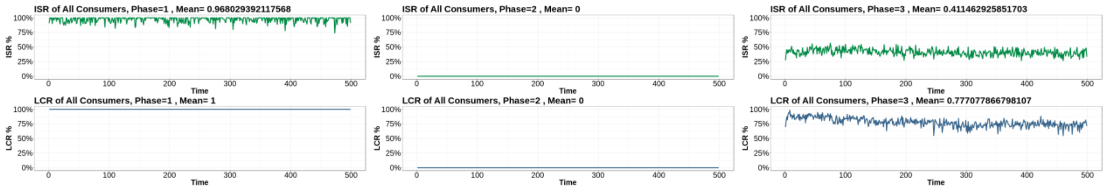

Figure 7. Results of the “Attacker near Consumers” Scenario

The ISRs and LCRs of this scenario are illustrated in Figure 7. Nearly all Interests can be satisfied in the first phase, and all Contents that Consumers received are legitimate. When Attacker acts, none of 30 Consumers can get legitimate Contents in the second phase. In the third phase, with our mitigation, an average of 41% Interests that Consumers sent can bring and about 78% Contents that Consumers received are legitimate.

4.2. Scenario “Attacker near the Producer”

Like the prior scenario, there are 3 phases and the Attacker is located near the Producer (Figure 8) in order to make a comparison and the only difference is the location of the Attacker. The ISRs and LCRs of all phases are illustrated in Figure 9.

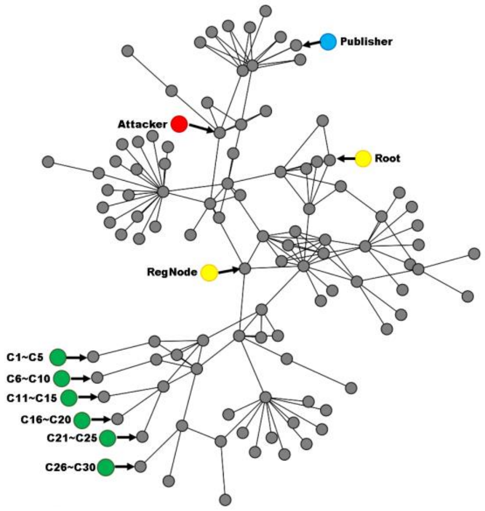

Figure 8. “Attacker near Producer” Scenario

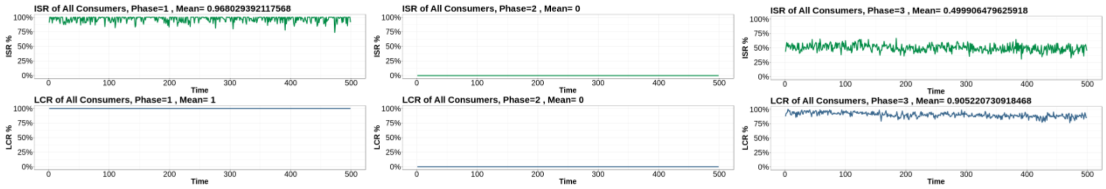

Figure 9. Results of the “Attacker near Producer” Scenario

In Figure 9, comparing with the prior scenario, there is a distinct difference in the third phase which is the scenario of the network under attack and with our mitigation. In this phase, the Consumers can retrieve an average rate of 50% legitimate Contents even when the attacker acts, and among all received Contents, 91% are legitimate. This observation verifies that no matter where the Attacker is located, our mitigation can bring the ISR and LCR back to acceptable levels.

4.3. The Overhead of Our Mitigation

At the current stage, the verification is based on the number of recordings in PIT entries, and the overhead should not be neglected.

At the Consumer side, its experiences heavily depend on the ISR, LCR and how long its Interest can be satisfied. In the network domain, the last metric above is the delay of the Interest which is the time elapsed from the Interest sent out to the legitimate Content returned. Although we believe our mitigation brings back legitimate Contents with less computation and more efficiently, the Delay between Interest and Content should not beyond our consideration since users cannot tolerate a large Delay especially in real-time situations.

We get the delays of Consumer Interests in both scenarios the same network topology and the results are illustrated in Figure 10. In Figure 10, the upper-left is the delay of the first phase of both scenarios, and the upper-right is the delay of the second phase of both. The bottom-left is the delay of the scenario “Attacker near Consumers”, while the bottom-right is the delay of the scenario “Attacker near Producer”.

In the first, that is the network without Attack or mitigation, Consumers experience an average of 8ms delay of their Interests. In the second phase, this delay soars to infinity which corresponding to the results of ISR and LCR, since all Interests are intercepted by Attacker. In the third phase, the delays achieve an average of 91ms and 55ms respectively in the scenario “Attacker near Consumers” and scenario “Attacker near Producer”.

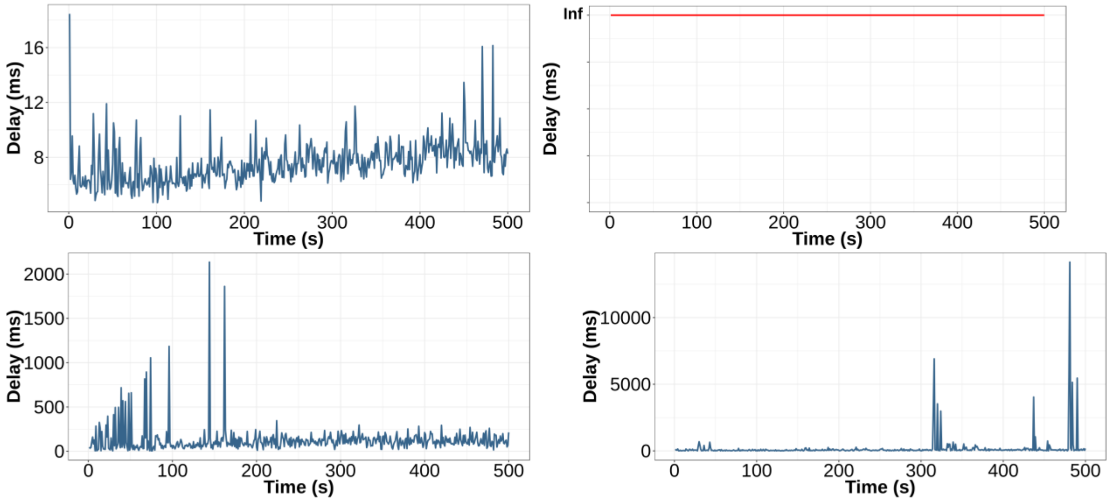

Figure 10. Delays of both scenarios

4.4. The Conclusion of Simulations

From the results in both previous scenarios, we can easily make a conclusion, that is CPA acts as a Black Hole in the network, and when only one Attacker attacks, all Interests can be intercepted. After the implementation of our mitigation, both ISR and LCR of Consumer can raise to certain acceptable levels. We do not make more scenarios with more Attackers in the network since the damage of only one is significant.

When our mitigation is implemented in the third phases of all scenarios, it can mitigate the CPA no matter where the Attacker is located, since all intermediate Routers are able to know if the incoming Content is legitimate or not by verification the key&name Hash. By the observation of Consumer Interest delays of our mitigation, we can conclude that our mitigation is effective and efficient.

5. Conclusion and Discussion

The current Internet architecture has brought a lot of benefits to the whole world, and many security problems spring out since it lacks the considerations of security at the beginning of its design. As a clean state design, the NDN is born with security considerations and more sophisticated in content distribution which consist of the majority of network traffic nowadays. However, like CPA, some kinds of DDOS attacks can still bring damages in NDN. In this paper, a secure solution is proposed and evaluated by simulations.

With simulations of scenarios with a real network topology. By evaluating the ISRs, LCRs, and delays, we found that our mitigation can let the Interests to bring an acceptable rate of Contents back to Consumers with a small delay.

Although our mitigation is designed with less computation consumption, it is not so smart since the verification is based on a fixed parameter of the PIT entry occupation at the current stage. We suppose to replace this by making the parameter changes dynamically to reduce the computations further in our future work.

REFERENCES

[1] Named Data Networking (NDN), Retr. January 2013. <http://named-data.net>.

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

[3] Ribeiro I, Rocha A, Albuquerque C, et al. On the possibility of mitigating content pollution in content-centric networking[C]//Local Computer Networks (LCN), 2014 IEEE 39th Conference on. IEEE, 2014

[4] I. Ribeiro, A. Rocha, C. Albuquerque and F. Guimarães, "Content pollution mitigation for Content-Centric Networking," 2016 7th International Conference on the Network of the Future (NOF), Buzios, 2016

[5] DiBenedetto S, Papadopoulos C. Mitigating poisoned content with forwarding strategy[C]//Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on. IEEE, 2016

[6] Ghali C, Tsudik G, Uzun E. Needle in a haystack: Mitigating content poisoning in named-data networking[C]//Proceedings of NDSS Workshop on Security of Emerging Networking Technologies (SENT). 2014.

[7] Wu D, Xu Z, Chen B, et al. What If Routers Are Malicious? Mitigating Content Poisoning Attack in NDN[C]//Trustcom/BigDataSE/I SPA, 2016 IEEE. IEEE, 2016.

[8] Ghali C, Tsudik G, Uzun E. Network-layer trust in named-data networking[J]. ACM SIGCOMM Computer Communication Review, 2014

[9] Kim D, Nam S, Bi J, et al. Efficient content verification in named data networking[C]//Proceedings of the 2nd International Conference on Information-Centric Networking. ACM, 2015

[10] Nguyen T, Mai H L, Doyen G, et al. A Security Monitoring Plane for Named Data Networking Deployment[J]. IEEE Communications Magazine, 2018, 56(11): 88-94.

[11] Alexander Afanasyev, Ilya Moiseenko, and et al. ndnsim: Ndn simulator for ns-3. Technical report, UCLA, 2012

[12] N. Spring, R. Mahajan, and D. Wetherall, “Measuring ISP topologies with rocketfuel,” in ACM SIGCOMM, 2002

AUTHORS

PENGFEI YUE is a PhD student in the college of Computer in the Inner Mongolia University, China.He visited the NDN Net Lab in the University of Memphis in 2016. His research includes next generation network, network security, and VANET.