International Journal of Engineering & Technology, 7 (1.1) (2018) 303-305

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Dos flooding attack control in information-centric networks

Srinivasa Rao T [1] *, Harsha G [2], Kiran V [2], Hemanth Kumar K [2]

[1] *Assoc. Professor, Koneru Lakshmiah Educational Foundation*
[2] *Student, Koneru Lakshmiah Educational Foundation*
**Corresponding author E-mail: tsrinivas@kluniversity.in*

Abstract

ICN (Information-centric networking) is a modern networking standard that mainly works only on the content extraction from a network without taking into case about the storage location or how the content is represented. In ICN providing security for the content is more important. Here we don't concentrate on protecting path. In order to fulfil the security goals in the new standard, it is very decisive to have a clear complete comprehension about ICN attacks and their brief allocation and the solutions. In this paper we in brief explain the attacks which effect the ICN network and other related attacks which have an impact on ICN. Attacks in ICN are divided to four categories, routing attacks, Naming attacks, Caching attacks, and other various related attacks. There are lot of solutions which are accessible. The main moto in ICN is to protect data which is very hard to achieve. So we develop a dynamic host based IP address scheme including certain snort rules which detect attacker and distinguish them in the clients and secure server from resource exhaustion. Our main center we deal with is on availability, and privacy.

Keywords: *Information Centric Networks; Dos Attack; Flooding Attack; Snort Rules; Dynamic IP.*

1. Introduction

According to the research by cisco from the year 2017-2021 it is said that the network traffic over the years keep on increasing year by year. In year 2017 the total Exabyte's per month on all internet, managed IP, mobile data is of 277 Exabyte's. It is said that in the year of 2021 is 3337 Exabyte's [2]. Which means the traffic will tremendously keep on increasing month by month. So the threats over the internet gets simultaneously increases. We need to build a better network architecture so that we will be able to provide both effective information retrieval and also better security. As the present internet is becoming inadequate with lot of traffic to access data for the future eras, so we need to immediately develop a new network architecture [1]. ICN is one of the best choice for the past existing host centric network architecture. Information centric networks mainly focuses as the information as center. In order to retrieve these goals, Information centric networks depends on in-network caching, name-based routing technique and location independent naming [5].

In information centric networks the data can't be directly retrieved by the client. The sender who wanted the information to be shared posts an advertisement to say, that it has some content to be shared. The receiver who wants to access the data needed to subscribe the message [2]. Then the ICN network ensures ab secure path which can be used for delivery by the sender to receiver so that the available content is reached securely. The main important thing is that the sender and receiver doesn't know each other since the network is location independent naming.

The main advantage is that the security model in the ICN where in ICN architecture the security importance changes from securing the path to securing the content which is available to all the ICN nodes. As new, techniques have been created with the creation of the new architecture [9]. This attacks have a lot of impact on the ICN architecture. The security in ICN is ta internal part of the network. The most important advantage in ICN is this. In this we enormously study about the dos attacks with their proposed solutions. We also classify the attacks and their relation with the network attributes and the new security requirements [7].

2. ICN attacks

We discus about naming attacks, caching attacks, routing attacks and now we divide then into different categories depending on the type of attack [7]..

2.1. ICN

Information centric network is a new way of networking which is ready to substitute the host centric due to large increase in traffic. The host centric also produced security problems. Information centric networks mainly focuses on the data [3]. It doesn't protect path. In information centric networks each routers has caching capacity which are connected to each other. Every router stores the data which the client has searched on the web. If the user wanted to access the same data once more the cached data from the router is fetched. If many clients are connected to the single network and two or more clients wanted to gain data about the same service then no different requests are created at that time [4]. The request which is made by the user 1 is cached by web and that request is forwarded to the other client. This reduces the traffic. In the old host centric architecture for every new user a new request is created by which it will be hard for the network to handle all the requests [4-5]. When this happens the resource is exhausted due to total use of threshold of the network. So, ICN is able to provide solutions to all these problems.

Copyright © 2018 Srinivasa Rao T et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2.2. Network steps

Step1: Sender announces a data message to the network.
Step2: Receiver i sends a subscription with content name message to the ICN network.
Step3: The network creates a delivery path from the Source to the receiver
Step4: Receiver j sends a subscription message for the similar content.
Step5: The ICN network delivers the data from the least routed path to client from the Information centric networks n node caching.

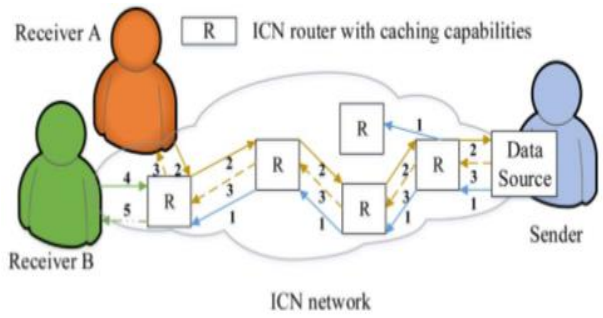


Fig. 2.1: Eslam G. Abdallah. Architecture Diagram of ICN. 2015.

3. Flooding based dos attack

An IP network is network which used internet protocol for communication between two computers connected to a network. The threat in the IP network is shown by the flooding-based attack [8]. In information centric network a client will become attacker when he intentionally or by ease to retrieve data sends a large number of requests that collapse the network [9]. By this type of attack the network comes into a trance where it will be unable to handle the total number of requests the attack which we have seen is flooding attack.
The main problem in ICN is that there is no limit for the number of user so, any number of clients can send any number of requests so for this we need to develop a technique to limit the number of requests or to sort the requests and save the network from crashing [3]. What actually happens is the attacker overloads the network and makes it unavailable for the other uses who wanted to retrieve the sane data.

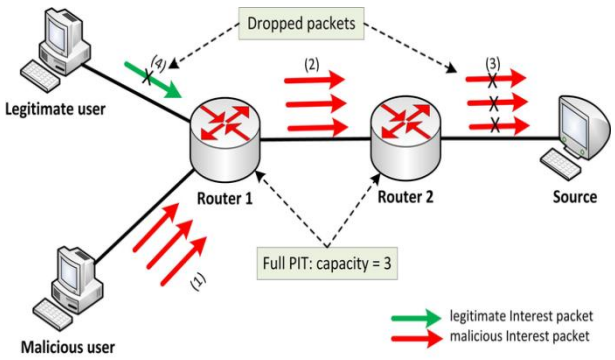


Fig. 3: Https://Www.Researchgate.Net/Figure/Interest-Flooding-Attack-On-NDN_302878160.14 November 2013, Brooklyn, NY, USA.

If the attacker need to send many packets he need to use some software. We use Network Packet Builder software which allows the attacker to produce a lot of IP addresses which doesn't exist at all and these addresses send requests which can't be answered by the server [6].
This command of Frame-ip Packet Generator allows sending flood traffic at a vast intensity packet rate:

>frame-ip –interface 2 –sending_mode 3 –loops 0 –wait 0 –IP_type 6 –InternetProtocol_source r –InternetProtocol_destination 192.168.51.1

So, in order to find a security solution we use a dynamic IP addresses scheme for the server hosts such that whenever a user requests the data the IP of the server keep on changing by this we will be able to stop the attacker from choosing a particular server and we even use snort rules in between [1] .This compares the number of requests with the threshold of the network node. When the threshold reaches the maximum value the server stops receiving the data and make the client with same requests as the attacker. Them the network stops the client and sends an ERROR 508 message to him [5]. By this way of dynamic IP method and snort rules we will be able to overcome the flooding attack.

4. Existing solution

The existing solutions for information centric networks are we put a limit to the number of clients. But, in information centric networks we cannot put a limit to the number of clients because the network is content centric [1]. If it is a host centric network we can put a limit to the number of clients. So we need to develop a new solution for ICN network.

5. Proposed solution

Snort is a very good intrusion detection and eradication system. Snort is most commonly used as a tool to teach many areas of network security. Snort makes use of these rules as attack signature. This always allow to find all the attacks such, as Dos attacks and heavy network traffic [2]. These rules used by Snort are simple and lightweight. The language which is used is flexible and powerful. These rules are divided into two sections.
These logical sections are:

1) Rule header
2) Rule option.

Now, we develop a certain rule such, that it will stop the connection to the attacker and send him an message that (SERVER LOST). This is the snort rules [4].

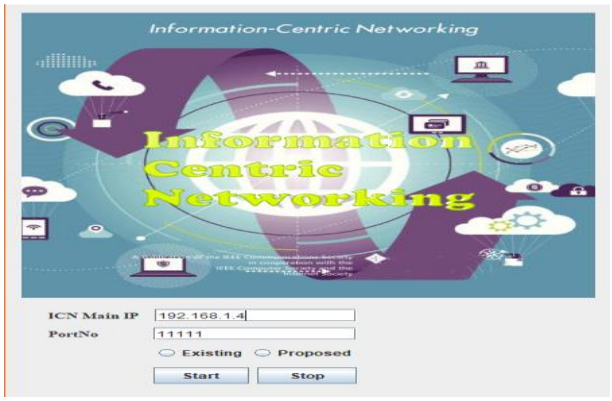
Alert XXX any1.1 any1.2 -> 192.168.51.1 any 2.2

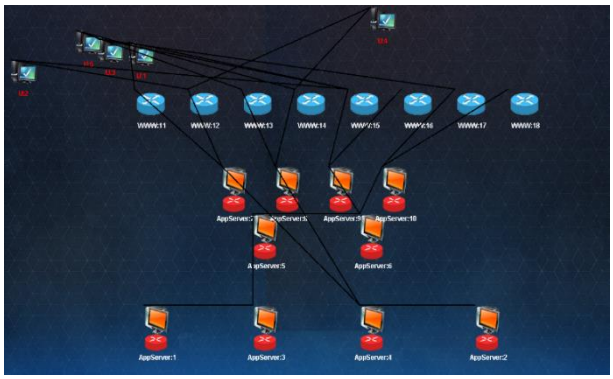
(message:" SERVER LOST and time frame seconds NUM"; threshold: high threshold, count 20, seconds >20)

1) XXX:-TCP or UDP.
2) 1.1:- source address.
3) 1.2:- source port.
4) 2.1:- receiver address.
5) 2 .2:- receiver port.
6) But now, we find that our server is safe and for the attacker his server will be lost leaving him a message SERVER LOST with the time of frames per seconds [9].

6. Outputs

6.1. The architecture 0f the both proposed and existing solutions





6.2. Number of servers and www with multiple users we created



6.3. The attack code generator which will flood servers

7. Algorithm

Step-1: Start
Step-2: Server started successfully.
Step-3: Running and listening on port: 11111
Step-4: Deploy ICN
Step-5: No of clients are activated
Step-6: Snort rule-1, Initialize all the IP address & port numbers
Step-7: The threshold value of the requested client is below 10 sec. If the requesting period of the user to the server is more than 10 attack is consider as low level attack
Step-8: The threshold value of the requested client is below 20 sec. If the requesting period of the user to the server is more than 20 attack is consider as high level attack.
Step-9: Launch all the servers
Step: 10 launch all the Users
Step: 11 Perform device actions by every user.
Step: 12 If (t<10)
Consider as User
Else
Consider as Attacker
Display the attacking time in seconds.
Step: 13 Exit

8. Conclusion

In this paper, the proposed frame work may raise many solutions to the problems faced by the ICN clients. With this development of snort rule by using the threshold value we are able to main a good bandwidth where this is easily applied in the ICN network. But if we take the scenario of the static IP addresses where the attacker will be able to make use of this IP and send continuous requests. We proved that we can maintain a traffic limit by using snort and dynamic IP. The problem is that it is only applicable to a single network.
We need to develop a solution such that we are able to solve traffic in multi ICN networks. This raised new questions because internet is not a small network it is vast boundary of different devices working at a time in a single or multiple network

References

[1] Detection of DDOS Attacks Using Snort Detection NagoorMeerasaheb Lanke#1, CH. Raja Jacob#2 #1CSE Dept., Nova College of Engineering & Technology, Vegavaram,JangareddyGudem , #2CSE Dept., M-Tech, CSE, Nova Nova College of Engineering & Technology, Vegavaram, JangareddyGudem.
[2] Using Network Packet Generators and Snort Rules for Teaching Denial of Service Attacks Dr. ZouheirTrabelsi United Arab Emirates University P.O Box 17551, Al Ain, UAE 3-7135570, 00971 Trabelsi@uaeu.ac.ae LatifaAlketbi United Arab Emirates University P.O Box 89289, Al Ain, UAE 50-1822636, 00971 200812217@uaeu.ac.ae.
[3] A Survey of Security Attacks in Information-Centric Networking Eslam G. AbdAllah, Student Member, IEEE, Hossam S. Hassanein, Senior Member, IEEE, and Mohammad Zulkernine, Senior Member, IEEE.
[4] A Survey of Information-Centric Networking Research George Xylomenos, Christopher N. Ververidis, Vasilios A. Siris, Nikos Fotiou, Christos Tsilopoulos, XenofonVasilakos, Konstantinos V. Katsaros, and George C. Polyzos.
[5] Security Aspects of the Information Centric Networks Model amahfouth99@gmail.com Computer Information System Al Quds Open Univeristy.
[6] www.snort.org
[7] A. Sardana, R. Joshi, and T. hoon Kim, “Deciding optimal entropic thresholds to calibrate the detection mechanism for variable rate DDoS attacks in ISP domain,” in Proc. ISA, Apr. 2008, pp. 270–275. [13] I. B.Mopari, S. G. Pukale, and M. L.
[8] Dhore, “Detection of DDoS attack and defense against IP spoofing,” in Proc. ACM ICAC3, 2009, pp.489–493. [14] Jéerôme François, IssamAib, RaoufBoutaba,” FireCol.
[9] A Collaborative Protection Network for the Detection of Flooding DDoS Attacks”, IEEE 2012 Transaction on Networking, Volume: PP, Issue: 99.