Novel Approach for Avoiding DDOS Attacks Using Dynamic Path Identifiers

SATRAM GAYATRI DEVI [#1] & L. SOWJANYA [#2] & D.D.D.SURIBABU [#3]

[#1] MCA Student, Master of Computer Applications, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#3] Head & Associate Professor, Dept of CSE, D.N.R. College of Engineering, Bhimavaram, AP, India.

Received: January 16, 2019 Accepted: February 20, 2019

ABSTRACT: *Now a days there is a huge demand and interest in using path identifiers (PIDs) for data communication .These PIDs act as a inter-domain routing objects to avoid distributed denial-of service (DDoS) flooding attacks. As we all know that path identifier is designed earlier, those are static in nature and hence it is very easy for the attackers to create any attack on a fixed path. To address this issue, in this present application we try to design and implement a novel path identifiers for data communication like dynamic D-PID, a framework that uses PIDs negotiated between neighboring domains as inter-domain routing objects. In DPID, the PID of an inter-domain path connecting two domains is kept secret and changes dynamically. We simulated our application using socket programming language along with java network package to verify the effectiveness and cost. The results from both simulations and experiments show that D-PID can effectively prevent DDoS attacks.*

Key Words*: Denial of Service, Inter Domain Packet, Socket Programming, Secret Key, Dynamic Path Identifier.*

I. Introduction

Currently almost all parts of the world are concentrating more and more on their security levels. As there was a tremendous increase of electronic devices almost each and every user try to store, retrieve, access the data to and fro via electronic devices. As the security plays a very important role even though there was a lot of hackers or intruders who try to hack or attack the sensitive data of others during data transmission. In recent days security plays a very vital role in each and every organization like banking, hotels, shopping malls, Hospitals, Schools and so on. As security plays a very prominent role a lot of users try to access the contents illegally and they want to misuse the content during transmission [1].

Generally attacks are classified into two types based on their functionality

1. Physical Attack
2. Non-Physical Attack

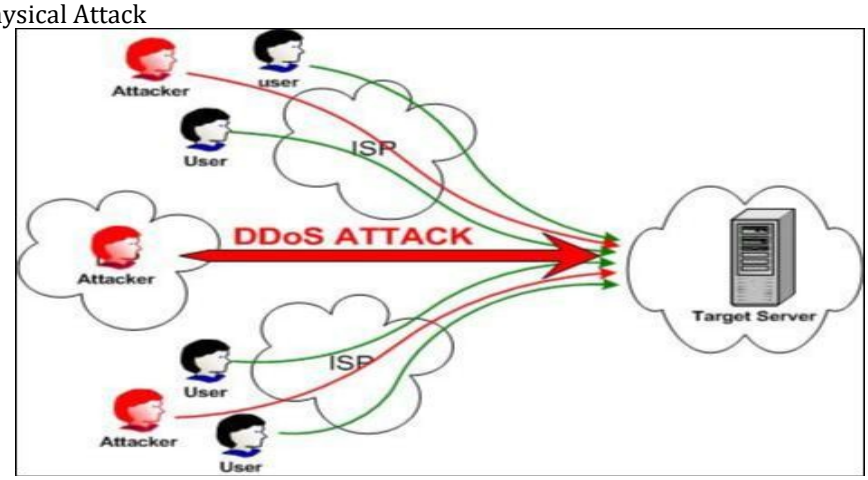

Figure 1. Denotes the Typical Architecture of a Denial of Service Attack on a Target Server

The attack which is been attempted by an intruder and in turn misuse the content or damage the content physically from its original content is known as physical attack. In this physical attack the data will not be transferred from valid source to valid destination, even some times with an attacked content [2]. On the

other side if an attack occurs just in order to make delay during data transfer, without changing the original content is known as non-physical attacks. In this category the data will not be changed or damaged but just the data will be sending or received to and from the source and destination with some delay. Generally identifying the non-physical attack is very difficult for the network admin as the hacker can create delay either from source node or destination node or at router level. Hence it is very crucial task for the network admin to identify the non physical attacker [3].

From the above figure 1, we can clearly identify that the dos attack which is created on a distributed network is termed as a distributed denial of service attack and in turn they will try to deny the access of valid user from the target server. These DDOS attackers always try to deny the access of authorized users from the target server. As we all know that more delay always leads to loss, so if a DOS attacker who wish to create some disturbance in transmission of data to and from the target server, then it will be leads to data loss.

II. Related Work

In this section we mainly discuss about the related work that was carried out inorder to find out the proposed dos attack detection on a network.

Dos Attack Detection on a Network

Generally the DOS attack can be occurred either at network end or either at host end. So the system should identify the attack accurately from any level [4], [5]. Generally when coming to the network based attacks detection, it is again classified into 2 main sub categories like:

1 Misuse Based Detection System
2 Anomaly Based Detection System

Generally the misuse-based detection systems will identify the network attacks by monitoring all the network activities and it looks for any matches that found with existing attacks
that occurs in the same system. In spite of having high detection rates to known attacks and low false positive rates, misuse-based detection systems are easily known and hacked by any new attacks and even variants of the existing attacks. Along with this it is also a complicated task to maintain the signatures database updated in the network.

On the other hand the anomaly based detection systems are proposed in which the network is monitored continuously and if it found any node significantly deviate from the legitimate traffic as a suspicious objects, anomaly based detection system try to identify the attacks. By doing this the user can able to detect zero-day intrusions that exploits previous unknown system vulnerabilities [6], [7].

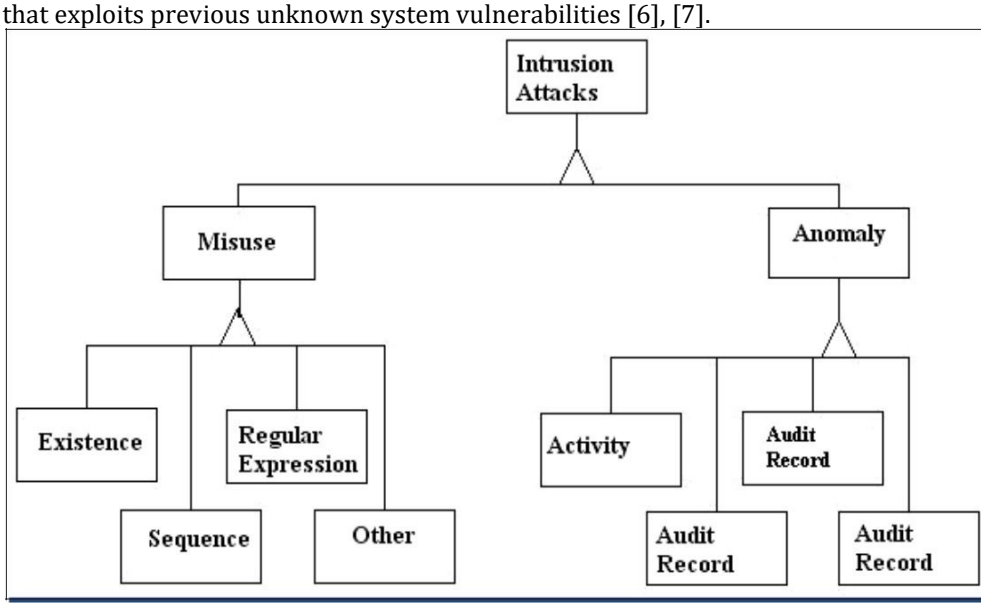

Figure 2. Denotes the Architecture of a Network Based Detection Systems

From the above figure 2, we can clearly get an idea about the architecture of network based detection systems. Generally the network based detection systems is classified into two categories like misuse based and anomaly based and which in turn sub-divided into various other types based on the type of functionality.

III. Proposed Dynamic Path Identifier to Avoid the Denial of Service Attacks

In this section we will mainly discuss about the proposed DPID for avoiding the DOS attacks. Now let us discuss about this proposed model in detail as follows:

Preliminary Knowledge

In the proposed system, the system proposes the D-PID design by addressing the following challenges. First, how and how often should PIDs change while respecting local policies of autonomous systems (ASes)? To address this challenge, D-PID lets neighboring domains negotiate the PIDs for their inter-domain paths based on their local policies. Here the two neighbors try to choose a unique ID which shouldn't be effected with flooding attacks or DOS attack[8].

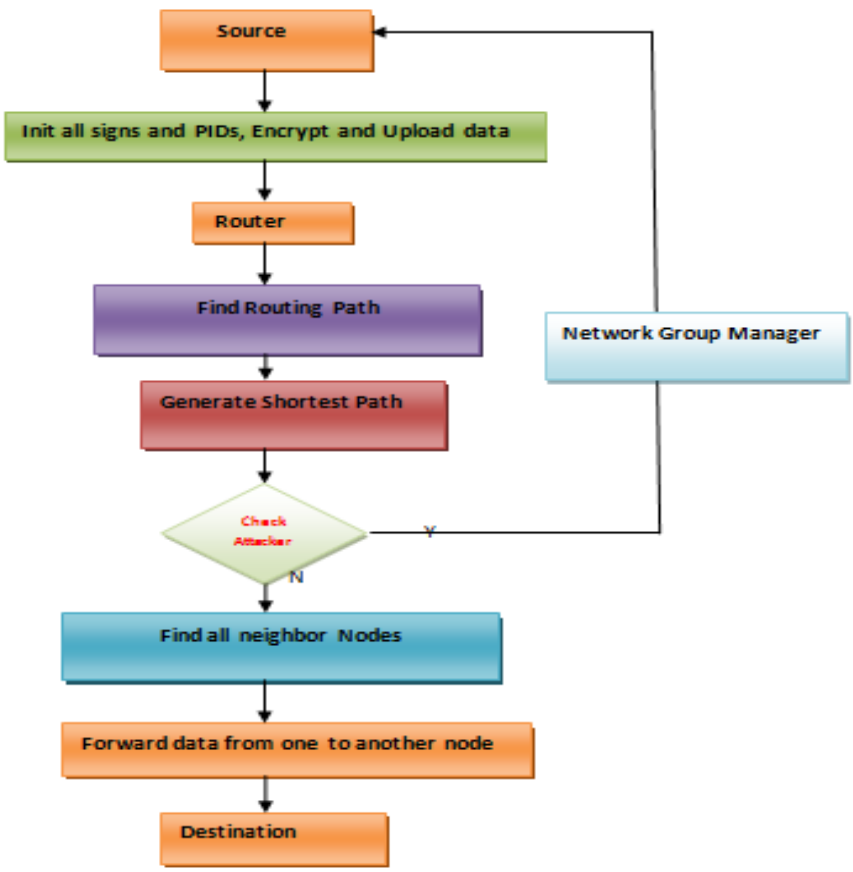

Figure 3. Represents Proposed Architecture of DPID over DDOS Flooding Attacks

Advantages of Using D-PID

1. Distributed denial-of-service (DDoS) attacks to avoid attackers
2. More security due to path identifiers are dynamic in nature(D-PIDs).
3. IT is dynamic in nature so there is no scope of data loss if any doS attacks occur during transmission
4. In this proposed approach we can achieve high level of accuracy in sending the packets to the destination node[9].
5. It is efficient and practical method for packet delivery.

From the above figure 3,we can clearly able to identify the architecture flow of our proposed approach DPID in order to avoid the DDOS Flooding attack [10]over wireless sensor network.

IV. Conclusion

In this paper, we for the first time design and implement a novel path identifiers for data communication like dynamic D-PID, a framework that uses PIDs negotiated between neighboring domains as inter-domain routing objects. In DPID, the PID of an inter-domain path connecting two domains is kept secret and changes dynamically. We simulated our application using socket programming language along with java network package to verify the effectiveness and cost. The results from both simulations and experiments show that D-PID can effectively prevent DDoS attacks.

V. References

1. "Understanding Denial-of-Service Attacks". *US-CERT. 6 February 2013*. Retrieved 26 May 2016.
2. TFreak, 2003. www.phreak.org/archives/exploits/denial/smurf.c
3. The Philosophy of Anonymous "Radicalphilosophy.com. 2010-12-17. Retrieved 2013-09-10.
4. U. D. Khartad and R. K. Krishna, "Route Request Flooding Attack Using Trust Based Security Scheme in Manet," International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Vol. 1, No. 4, 2012, p. 27.
5. K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, "DDoS attack detection method using luster analysis," Expert Systems with Applications, vol. 34, no. 3, pp. 1659-1665, 2008.
6. R. Guo, G. R. Chang, R. D. Hou, Y. H. Qin, B. J. Sun, A. Liu, Y. Jia and D. Peng, "Research on Counter Bandwidth Depletion DDoS Attacks Based on Genetic Algorithm.
7. Fed CIRC, "Defense Tactics for Distributed Denial of Service Attacks," Federal Computer Incident Response Center, Washington DC, 2000.
8. H.-J. Kim, R. B. Chitti and J. S. Song, "Handling Malicious Flooding Attacks through Enhancement of Packet Processing Technique in Mobile Ad Hoc Networks," Journal of Information Processing Systems, Vol. 7, No. 1, 2011, pp. 137-150.
9. *The Philosophy of Anonymous " Radicalphilosophy.com. 2010-12-17. Retrieved 2013-09-10.*
10. R.B.Chiti, "Defense Tactics for Distributed Denial of Service Attacks," Federal Computer Incident Response Center, Washington DC, 2000.