Two State Intrusion Detection System Against DDos Attack in Wireless Network

[1]Pintu Vasani, [2]Parikh Dhaval
[1]M.E Student, [2]Head of Department (LDCE-CSE)
L.D. College of Engineering, Ahmedabad, India.
[1]Pintu_417@yahoo.in, [2]Parikh.da@ldce.in

***Abstract* - With the emergence of global connectivity with expansion of computer network during the past decade, security threats in network have become a crucial issue for computer systems. Now a day, it is very important to retain a high level security to ensure safe and trusted communication for information exchange across the network and wireless network has become an exciting and important technology because of the rapid proliferation of wireless device [1]. The traditional way of protecting network with firewalls and encryption software is no longer sufficient and effective for these features. In this author suggested Flow-based intrusion detection system (IDS). There are many security attacks in wireless network and DDos is one of them. In this thesis I am going to use flow-based mechanism in wireless system because in early cases IDS is used to check the payload data which is very time consuming process. Now a days it is not possible because the speed of the internet is too high. The goal of this thesis is to detect the malicious activity as fast as possible with minimum number of false alarm and maximum accuracy.**

***Keyword* - Intrusion detection system, DDos attack, Flow-based, High Speed, wireless network**

I. INTRODUCTION

Network Intrusion detection is the process of monitoring and analyzing events that occur in a computer or networked computer system to detect the behavior of the users that conflict with the intended use of the system. In Wireless network each device is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless networks face today is security, because no central controller exists. To solve the security problem we need an IDS. Which can be categorized into two models: Signature-based IDS and anomaly-based IDS[2]. In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base of the IDS if any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory. To solve this problem anomaly based IDS[2] is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. There are many security attacks in wireless network and DDos(Distributed denial of service) is one of them. Our main aim is seeing the effect of DDos in routing load, packet drop rate, end to end delay. There are many types of DDos attacks in wireless network like TCP flooding, UDP flooding etc. [3]. We overcome this problem through Flow-based Intrusion detection system. Which is continuously check the flow of the network and alarm according threshold value[4]. Place point of view Intrusion detection system is mainly two type: Host-based detection and Network-based detection. In Host-based IDS is reside on host computer and detect the malicious activity on host computer only. Where, In Network –based IDS is on network and analyze the network performance [5] and network-based IDS is performing two types : Packet-based detection and Flow-based detection. In Packet-based NIDSs has to analyze the whole payload content beside headers. It is very time consuming process so when one packet is analyze, so many other packets are arrived and dropped so benign packet may not reach to destination and legitimate user getting problem. In flow NIDSs, rather than looking at all packets going through a network link, it looks at aggregated information of related packets of network traffic in the form of flow, so the amount of data to be analyzed is reduced[6][7].

II. RELATED WORK

Prajeet Sharma et al [2] have proposed a scheme to find DDos attack through intrusion detection system based on parameter like protocol, packet type, time of packet send and receive and threshold value of the packet. Husain. Shahnawaz et al [8] have developed system based on initial trust on neighbor node and based on trust it count the value of trust on over total node in network and pass the packet which is arrived from trusted node only other packet are generated alarm for malicious activity. Anna Sperotto et al [4] have proposed flow-based method for intrusion detection system. In which based on threshold value of flow and generate alarm. Hashem Mohammed Alaidaros et al [7] have proposed hybrid scheme of packet-based and flow-based method to find intrusion in system. Anna Sperotto and Gregor Schaffrath et al [6] have proposed in “The overview of Ip flow-based intrusion detection system” research paper that “A flow is defined as a set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties.” Martuza Ahmed et al [9] have given packet-based scheme. In which it check each and every packet passing through node having IDS. Myung-Sup Kim et al [10] have some survey of network traffic and how to detect abnormal traffic and define various attack types based on packet header information.

III. INTRUSION DETECTION SYSTEM

Let we see intrusion detection system according to KrUgel et al. [11], "intrusion detection is the process of identifying and responding to malicious activities targeted at computing and network resources". In intrusion detection system is categorized in two model: Signature-based IDS and Anomaly-based IDS as we discuss in above section.

An IDS aims to discriminate between intrusion attempts and normal activities. In doing so, however, an IDS can introduce classification mistakes, usually known as false positives, false negatives, true negative and true positive. There is a natural trade-off between detecting all malicious events (at the expense of raising alarms too often, i.e., having high false positives), and missing anomalies (i.e., having high false negatives, but not issuing many false alarms), sometime anomalies are there but not detected (i.e., true negative). Which component of the trade-off is more important is a case specific decision, and ideally, we would want to optimize both components. We might want to identify all malicious attempts, because this would make our network safer. However, this would be of no use if the number of alerts would overload.

There are two types of network-based intrusion detection system: Packet-based IDS and Flow-based IDS. Packet-based, also named "traditional NIDS", has to inspect the whole payload content beside headers. In flow-based NIDS, rather than looking at all packets going through a network link, it looks at aggregated information of related packets of network traffic in the form of flow, so the amount of data to be analyzed is reduced.

An efficient NIDSs has two features[12] :

[A] High accuracy (low false alarms)

[B]High performance (high speed of auditing)

Packet-based Intrusion Detection System

In packet-based, also named "Deep Packet Inspection" (DPI), the combination of header and payload scan determines whether a packet is an intrusion or not. Incoming packets are scanned and every single rule of the database is checked against it as shown in figure 1. The database rules include thousands of signatures and patterns of attacks [7].

The main advantage of packet-based approach is that all common kinds of known attacks and intrusions practically can be detected if the data source deliver entire network packet for analysis. It gives "True Positive alarm" in most of the cases.

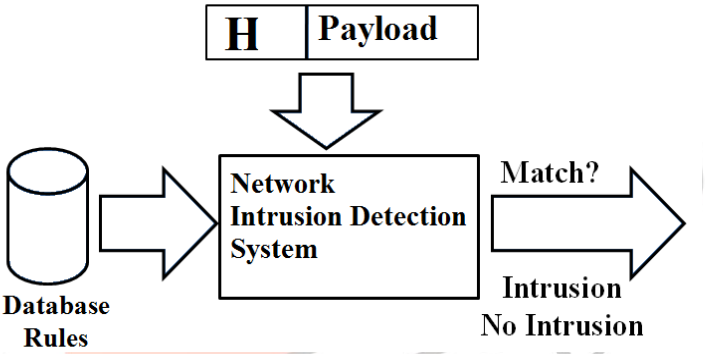

Figure 1. Packet-based IDS, adopted from[7]

Since the whole payload in every single incoming packet must be analyzed, packet-based NIDSs must have high processing throughput so that they will be really fast and will not be the bottleneck for the network[7]. In other words, systems that are capable of monitoring every packet on a high-speed network are very expensive and high resource consumption. Moreover, a drop of packets will occur if the NIDSs speed is not high enough to let the analysis process be done[7]. To overcome this problem Flow-based IDS is suggested for fast internet speed and solve above problem.

Flow-based Intrusion Detection System

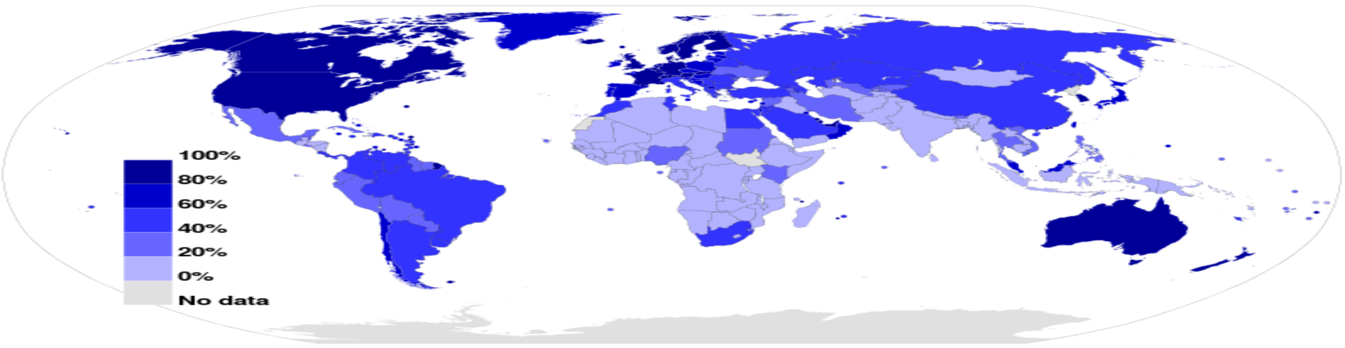

Figure 2 Percentage of Internet users in 2012 (source: Wikipedia)

The spread of 1-10 Gbps technology has in recent years paved the way to a flourishing landscape of new, high bandwidth Internet services. At the same time, we have also observed increasingly frequent and widely diversified attacks. To this threat, the research community has answered with a growing interest in intrusion detection, aiming to timely detect intruders and prevent damage. We believe that the detection problem is a key component in the field of intrusion detection. Our studies, however, made us realize that additional research is needed, in particular focusing on validation and automatic tuning of Intrusion Detection Systems (IDSs)[4].

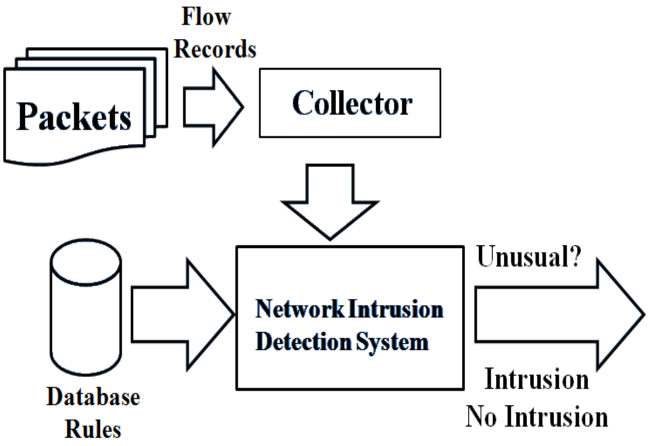

Figure 3. Flow-based IDS, adopted from[7]

Flow-based has an overall lower amount of data to be processed by NIDSs, therefore it is the logical choice for high speed networks but it suffers from producing high false alarms(There is no attack but detected i.e., False Positive).

Packet-based IDS is suffer from high data comparison and drop packet in network but this technique is give accurate anomaly detection (True positive alarm). when Flow-based IDS is suffer from high false alarm in network(False positive alarm) but it is work on high speed network without dropping packet. So, finally overcome both the problem I suggested one another proposed model which solve both the problem describe above.

IV. PROPOSED SCHEME

Flow based is only check the header portion of the packet. It is not given sufficient information about packet so it generate many false alarm in benign packet. Every time server wants to check whether any malicious activity is going on or not.

So, I am going to use flow-based Intrusion detection system against DDOS attack in wireless network. Mostly DDOS attacks are detected based on header information like IP address of source and destination, port number of source and destination, packet type and protocol type etc. I am using extra parameter like packet rate, arrival time of packet, number hop count and flow size.

Flow-based Intrusion detection system flowchart:
Step 1: If inflow is less than threshold value than no intrusion is found otherwise goto step2.
Step 2: Capture all packet.
Step 3: To capture Ip address, Port address and protocol type from packet and compare with set information if it exist then successful intrusion detected else step4.

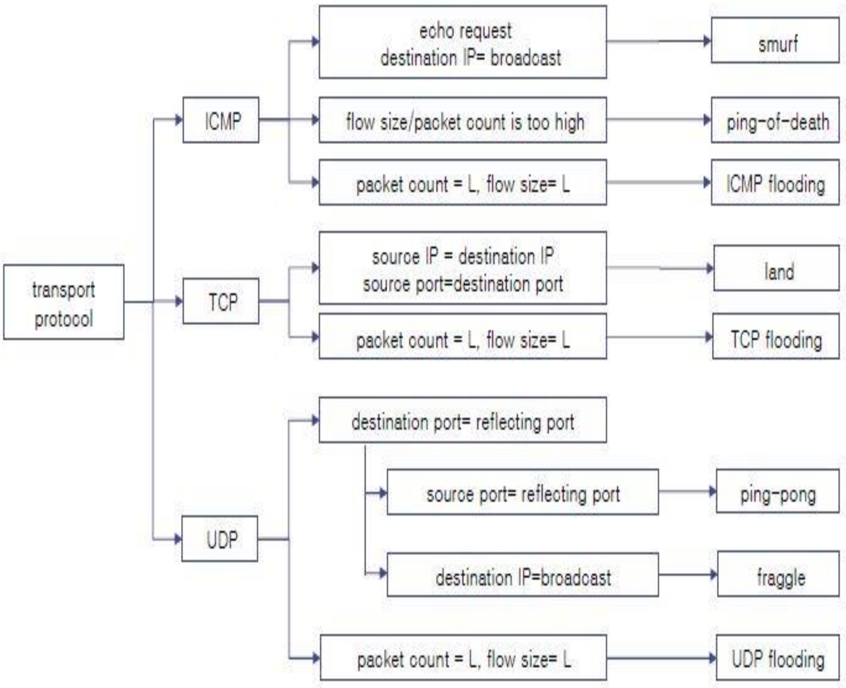
transport
protocol
ICMP
TCP
UDP
echo request
destination IP= broadcast
smurf
flow size/packet count is too high
ping-of-death
packet count = L, flow size= L
ICMP flooding
source IP = destination IP
source port=destination port
land
packet count = L, flow size= L
TCP flooding
destination port= reflecting port
source port= reflecting port
ping-pong
destination IP=broadcast
fraggle
packet count = L, flow size= L
UDP flooding

Figure 4. Flow Header Detection Sequence[10].

Step 4: Check flow record is exist. If yes then simply put in corresponding flow else create new flow and put packet in that flow.
Step 5: Making flow record extract information from each flow and compare with dataset

Step 6: If it is matched with dataset then successfully intrusion detected and update the dataset database else no intrusion is detected.

FlowDiagram: Proposed Schem:

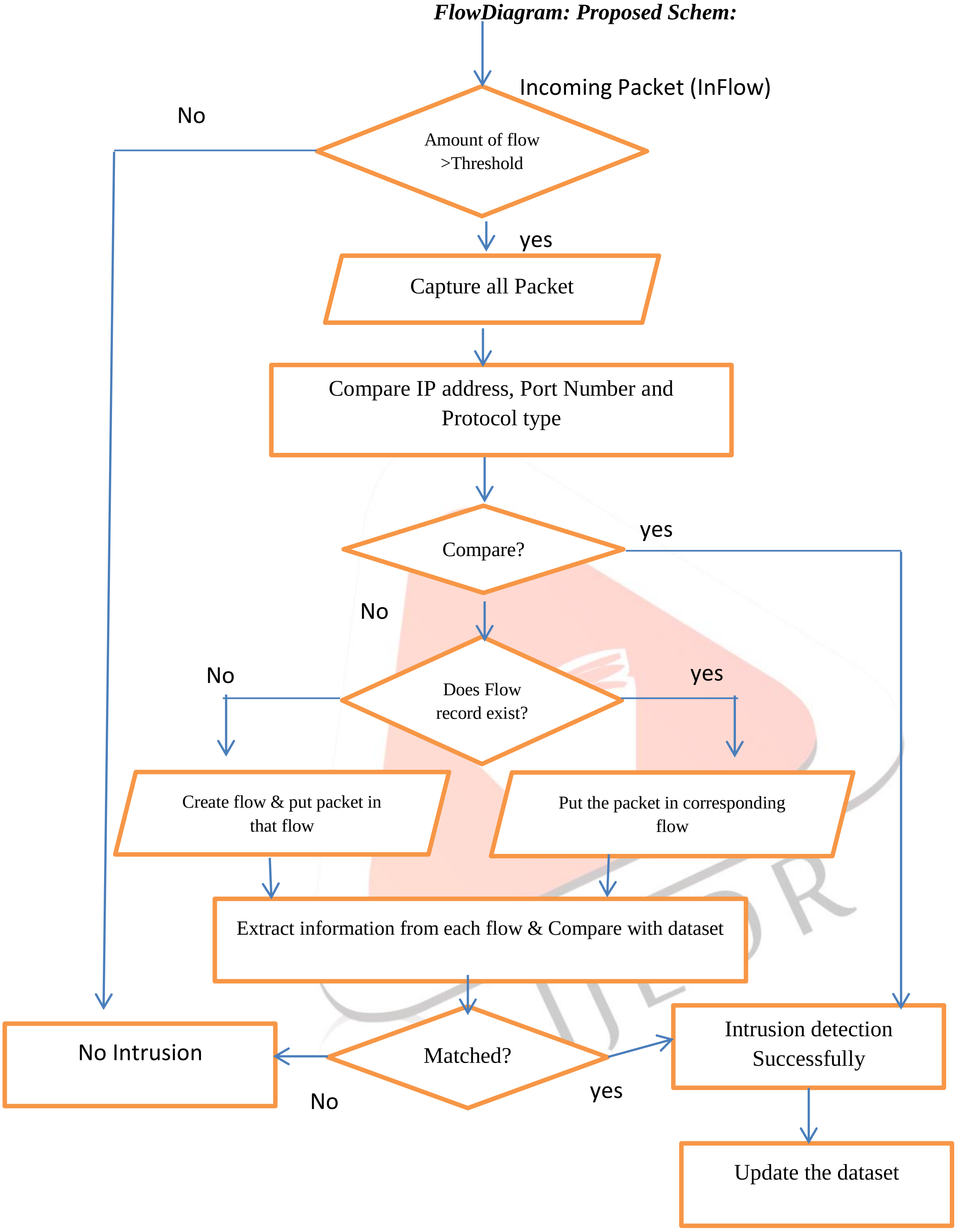
Incoming Packet (InFlow)
No
Amount of flow >Threshold
yes
Capture all Packet
Compare IP address, Port Number and Protocol type
Compare?
yes
No
No
Does Flow record exist?
yes
Create flow & put packet in that flow
Put the packet in corresponding flow
Extract information from each flow & Compare with dataset
No Intrusion
Matched?
Intrusion detection Successfully
No
yes
Update the dataset

Figure 5. Proposed scheme

V. CONCLUSION

This paper presents an overview of how the performance and detection accuracy of the payload-based, flow-based NIDSs are affected by the threats and attacks within the high-speed networks environment. It also gives overview of DDOS attack and solution of DDOS attack through flow-based method with adding some extra parameter but In flow-based IDS is also facing problem of the high false alarm. I will suggest one system in which it is first check inflow of the network and made comparison and take some parameter of the header without worrying of payload data and find DDOS attack more accurately and then It compare some extra parameter which are reside in dataset. Comparison made then Intrusion detection successfully and update dataset with new anomaly.

REFERENCES

[1] Yi-an Huang and Wenke Lee et al. “A Cooperative Intrusion Detection System for Ad Hoc Networks” Information Assurance and Security (IAS), 2011.

[2] Sharma, Prajeet, Niresh Sharma, and Rajdeep Singh. "A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network." International Journal of Computer Applications 41.21 (2012): 16-21.

[3] Jun, Jae-Hyun, Hyunju Oh, and Sung-Ho Kim. "DDoS flooding attack detection through a step-by-step investigation." Networked Embedded Systems for Enterprise Applications (NESEA), 2011 IEEE 2nd International Conference on. IEEE, 2011.

[4] Sperotto, Anna, and Aiko Pras. "Flow-based intrusion detection." Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on. IEEE, 2011.

[5] Lecture Notes for Internet Security “Intrusion detection system :Literature surveys”. Fall 2006, Syracuse University.

[6] Sperotto, Anna, et al. "An overview of IP flow-based intrusion detection." Communications Surveys & Tutorials, IEEE 12.3 (2010): 343-356.

[7] Alaidaros, Hashem Mohammed, Massudi Mahmuddin, and Ali Al Mazari. "From Packet-based Towards Hybrid Packet-based and Flow-based Monitoring for Efficient Intrusion Detection: An overview." (2012).

[8] Shahnawaz, Husain, R. C. Joshi, and S. C. Gupta. "Design of Detection Engine for Wormhole Attack in Adhoc Network Environment." International Journal of Engineering and Technology (2012).

[9] Ahmed, Martuza, et al. "PIDS: A packet based approach to network intrusion detection and prevention." Information Management and Engineering, 2009. ICIME'09. International Conference on. IEEE, 2009.

[10] Kim, Myung-Sup, et al. "A flow-based method for abnormal network traffic detection." Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP. Vol. 1. IEEE, 2004.

[11] Adrian stoica, Jeong Jin Kang, Sabah Mohammed, Ronnie D. Caytiles et al “Information science and technology” proceedings international conference ISSN 2287-1233, IST 2012,shanghai china, april 2012

[12] Hervé, Marc, Andreas et al. “Towards a taxonomy of intrusion-detection systems.” The International Journal of Computer and Telecommunications Networking (1999).