Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 10, October -2017

ANOMALY BASED DETECTION OF VIOLATIONS IN WEB APPLICATIONS

Nivetha.D[1], Swetha sri.P[2],Rampriya.R[3]

[1]*Computer science and engineering, CK college of engineering and technology*
[2]*Computer science and engineering, CK college of engineering and technology*
[3]*Computer science and engineering, CK college of engineering and technology*

Abstract — *Denial of Service is the technique that is used for de-phasing the server architecture. The server is being compromised and it is detached from normal use when Denial of service is executed so that normal users could not make use of the service provided by the server. Many techniques were introduced in order to avoid this DOS attacks but it contains its own flaws. Here we propose a new scheme that avoids both Denial of Service and Distributed Denial of Service attacks. This scheme includes scanning of the packets flow along the network and also maintains a black list of misuser's.*

Keywords-*Intrusion detection , Claim, carry and check, Denial of service, Flood attack, Network traffic attack.*

I. INTRODUCTION

1.1 Network Security:

IDS are besides other protective measures such as virtual private networks, authentication mechanisms, or encryption techniques very important to guarantee information security. They help to defend against the various threats to which networks and hosts are exposed to by detecting the actions of attackers or attack tools in a network or host-based manner with misuse or anomaly detection techniques. At present, most IDS are quite reliable in detecting suspicious actions by evaluating TCP/IP connections or log files, for instance. Once an ID'S finds a suspicious action, it immediately creates an alert which contains information about the source, target, and estimated type of the attack (e.g., Server abash, ICMP scanning or denial of service).The intrusive actions caused by a single attack instance which is the occurrence of an attack of a particular type that has been launched by a specific attacker at a certain point in time are often spread over many network connections or log file entries, a single attack instance often results in hundreds or even thousands of alerts. IDS usually focus on detecting attack types, but not on distinguishing between different attack instances. In addition, even low rates of false alerts could easily result in a high total number of false alerts if thousands of network packets or log file entries are inspected .The IDS creates many alerts at a low level of abstraction as a consequence. So it is extremely difficult for a human security expert to inspect this flood of alerts, and decisions that follow from single alerts might be wrong with a relatively high probability. In our opinion, a ―perfect IDS should be situation-aware in the sense that at any point in time it should ―know what is going on in its environment regarding attack instances (of various types) and attackers. We make an important step toward this goal by introducing and evaluating a new technique for alert aggregation. Alerts may originate from low-level IDS[5] such as those mentioned instances (of various types) and attackers. , we make an important step toward this goal by introducing and evaluating a new technique for alert aggregation.

II. LITERATURE SURVEY:

Aqeel Sahi [1] proposed a new classifier system for detecting and preventing DDoS TCP flood attacks (CS_DDoS) in public clouds. The proposed CS_DDoS system offers a solution to securing stored records by classifying the incoming packets and making a decision based on the classification results.

Qinghua Li[2], proposed a distributed scheme to detect if a node has violated its rate limits. It provide rigorous analysis on the probability of detection, and evaluate the effectiveness and efficiency of our scheme with extensive trace- driven simulations.

Q. Li and G. Cao[3], proposed a distributed scheme to detect packet dropping in DTNs. In our scheme , a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet.

Y. Ren, M.C. Chuah[7], proposed various methods that have been developed to detect wormhole attacks. However, most of them cannot work efficiently in DTNs[9].

III.DETECTION OF VIOLATION

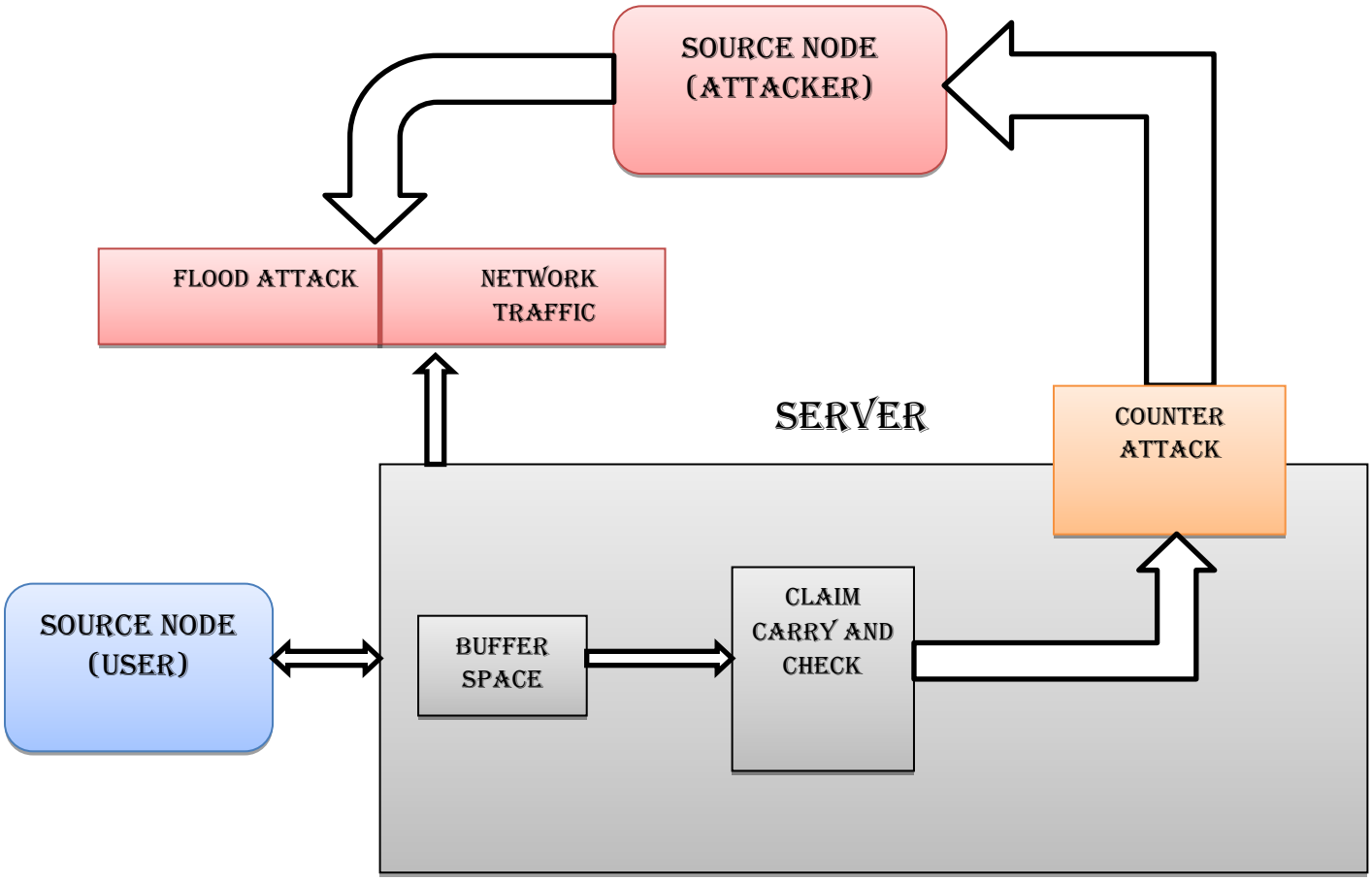

Fig 1: Architecture of detection of violation

The figure1 illustrates the architecture of the proposed system. There are two types of attack. The attacks are detected by claim carry and check algorithm.

Table1.Notations

SYMBOL	DEFINITIONS
ICMP	Internet Control Message Protocol
TCP/IP	Transfer Control Protocol /Internet Protocol
DDOS	Distribution Denial Of service
IDS	Intrusion Detection System
LAN	Local Area Network
DOS	Denial Of Service
JCAP	Java Packet Capture(Tool)
MAC	Medium Access Controller
DNS	Domain Name System

3.1 DOS ATTACK:

A denial of service attack [4] is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system. A denial of service attack is an effort to make one or more computer systems unavailable. It is typically targeted at web servers, but it can also be used on mail servers, name servers, and any other type of computer system. Denial of service (DoS) attacks may be initiated from a single machine, but they typically use many computers to carry out an attack. Since most servers have firewalls and other security software installed, it is easy to

lock out individual systems. Therefore, distributed denial of service (DDoS) attacks[4] are often used to coordinate multiple systems in a simultaneous attack.

A distributed denial of service attack intimate all coordinated systems to send a stream of requests to a specific server at the same time. These requests may be a simple ping or a more complex series of packets. If the server cannot respond to the large number of simultaneous requests, incoming requests will eventually become queued. This backlog of requests may result in a slow response time or a of service attack has succeeded.

We simulate two types of attacks, they are

- Flood attack.
- Network traffic attack.

Algorithm:

Step 1: Start
Step 2: Attacker sends many packets to the server.
Step 3: Packets are sent in two form of attack they are flood attack and network traffic attack.
Step 4: In food attack there are two types they are packet flood attack and replica flood attack.
Step 5: Packet flood attack is used to send many packets to the server.
Step 6: Replica flood attack is used to send copy of packets to the server.
Step 7: Network traffic attack is an indirect attack which sends continuous request of status to the server and keeps the server busy.
Step 8: Stop.

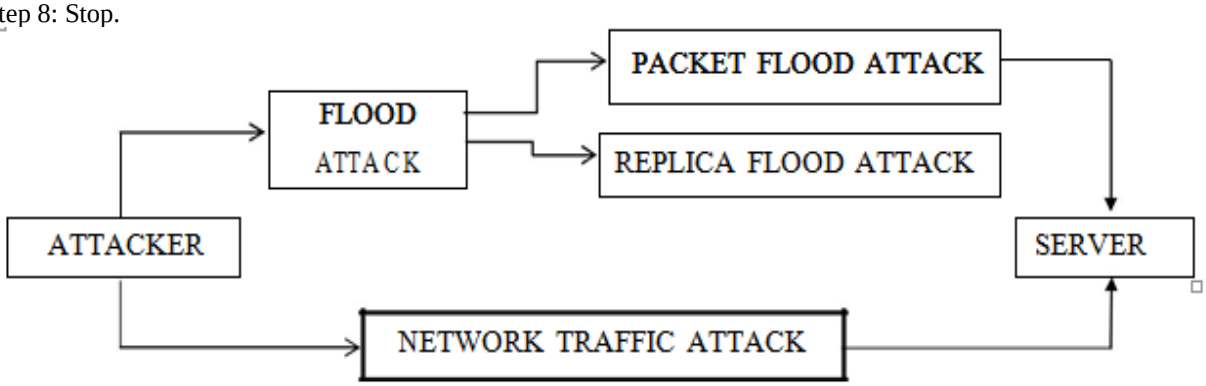

Fig 2: Flow Diagram For Dos Attack

3.2 CLAIM CARRY AND CHECK DETECTION:

To detect the attackers that violate their rate limit L, we must count the number of unique packets that each node as a source has generated and sent to the network in the current interval. However, since the node may send its packets to any node it contacts at any time and place, no other node can monitor all of its sending activities. To address this challenge, our idea is to let the node itself count the number of unique packets that it, as a source, has sent out, and claim the up-to-date packet count (together with a little auxiliary information such as its ID and a timestamp) in each packet sent out. The node‘s rate limit certificate is also attached to the packet, such that other nodes receiving the packet can learn its authorized rate limit L. If an attacker is flooding more packets than its rate limit, it has to dishonestly claim a count smaller than the real value in the flooded packet, since the real value is larger than its rate limit and thus a clear indicator of attack. The claimed count must have been used before by the attacker in another claim, which is guaranteed by the pigeonhole principle, and these two claims are inconsistent. Server check the violated packets in transferred data by sending the source node. If server find the violated packets then it will be detected by using CLAIM CARRY AND CHECK algorithm.

Algorithm:

Step 1: Start.
Step 2: Packets are sent from the source node.
Step 3: Each node itself counts the number of unique packets and claim the Count to the destination node.
Step 4: Destination node carry the claim and check for the rate limitation if the limit is violated meta-alert is generated.
Step 5: Analyze each alert from each cluster to find the source IP of the attack.
Step 6: If two alerts are from the same source falling in the same cluster then aggregate them into one.
Step 7: Else, form a separate aggregate for each alert.
Step 8: Repeat the steps 5 and 6 until all the alerts are analyzed.
Step 9: Stop.

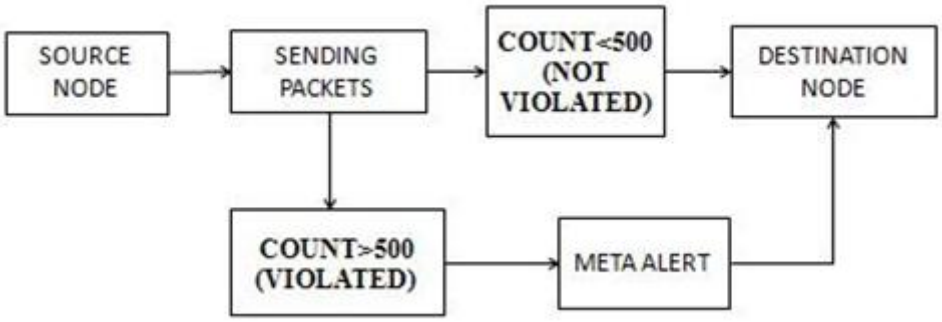

Fig.3 Flow Diagram for Claim Carry And Check

3.3 PACKET STATISTICAL REPORT:

The various layers are analyzed. In this, attackers send the packets through transport layer and network layer. In transport layer, Transmission Control Protocol (TCP), which uses a set of rules to exchange messages with other Internet points at the information packet level. We are using Network layer to transfer variable length data sequences from a source to a destination host via one or more networks to maintain quality of services. packet processing refers to the wide variety of algorithms that are applied to a packet of data or information as it moves through the various network elements of a communications network. Within any network enabled device (e.g. router, switch, network element or terminal such as a computer or smartphone) it is the packet processing subsystem that manages the traversal of the multi-layered network or protocol stack from the lower, physical and network layers all the way through to the application layer The internetworking protocol developed to support the network, called ARPA net,[6] was called TCP or Transmission Control Program. As research and development progressed and the size of the network grew, it was determined that the internetworking design that was being used was becoming unwieldy and it did not exactly follow the layered approach of the OSI Model. This led to the splitting of the original TCP and the creation of the TCP/IP[8] architecture - TCP now standing for Transmission Control Protocol and IP standing for Internet Protocol.

The transport layer is responsible for delivering data to the appropriate application process on the host computers. This involves statistical multiplexing of data from different application processes, i.e. forming data packets, and adding source and destination port numbers in the header of each transport-layer data packet. Together with the source and destination IP address, the port numbers constitutes a network socket, i.e. an identification address of the process-to-process communication. In the OSI model, this function is supported by the session layer. Finally, some transport-layer protocols, for example TCP, but not UDP, provide end-to-end reliable communication, i.e. error recovery by means of error detecting code and automatic repeat request (ARQ) protocol. The ARQ protocol also provides flow control, which may be combined with congestion avoidance.

UDP is a very simple protocol, and does not provide virtual circuits, non-reliable communication, delegating these functions to the application program. UDP packets are called data grams , rather than segments. TCP is used for many protocols, including HTTP web browsing and email transfer. UDP may be used for multicasting and broadcasting, since retransmissions are not possible to a large amount of hosts. UDP typically gives higher throughput and shorter latency, and is therefore often used for real-time multimedia communication where packet loss occasionally can be accepted, for example IP-TV and IP-telephony, and for online computer games.

Algorithm:

Step 1: Start.
Step 2: Analyzing the various layers.
Step 3: Sending the packets through network layer and transport layer.
Step 4: Transmission control protocol, which uses a set of rules to exchange messages.
Step 5: TCP provide end to end reliable communication.
Step 6: Network layer to transfer variable length data sequences from a source to destination.
Step 7: Stop.

3.4 COUNTER ATTACK:

The IDS[10] system running in the victim system collects the type of alert according to the type of attack that is undergone by the victim system and group them into the meta-alert system. Server performs the counter attack to the attacker. Server find the attacker by using IP and MAC address. A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. In IP networks, the MAC address of an interface can be queried given the IP address using the Address Resolution Protocol (ARP) for Internet Protocol Version 4 (IPv4) or the Neighbor Discovery Protocol (NDP) for IPv6. In this

way, ARP or NDP is used to translate IP addresses (OSI layer 3) into Ethernet MAC addresses (OSI layer 2). On broadcast networks, such as Ethernet, the MAC address uniquely identifies each node on that segment and allows frames to be marked for specific hosts. It thus forms the basis of most of the link layer (OSI Layer 2) networking upon which upper layer protocols rely to produce complex, functioning networks.

MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sub layer of the OSI reference model.MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address (BIA). It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. A network node may have multiple NICs and each must have one unique MAC address per NIC. Then server attack the attacker server so, attacker server getting slow or some performance issue. So, attacker could not able to send the packets.

Algorithm:

Step 1: Start.
Step 2: Performing counter attack to the attack.
Step 3: Server find the attacker by using IP address.
Step 4: Attacker server getting slow or performance issues.
Step 5: Attacker could not be able to send the packets.
Step 6: Attacker server will be restarted.
Step 7: Stop.

IV. RESULTS AND DISCUSSION

In this paper, we presented a practical solution to use supervised network in anomaly intrusion detection system. The system is able to employ dynamically and supervise network traffic for classifying and separating normal traffic from the attack traffic DoS. The proposed system was used for training and testing Data in intrusion detection system. Efficiency in Anomaly Network Intrusion Detection System Based on CLAIM CARRY AND CHECK. were able to recognize attack traffic and normal one. This is best suited to increase their high speed and fast detection rates as compared with other learning techniques and also improves the accuracy of detecting DoS.

The screenshots taken during the execution of the program is as follows.

Fig.4 DoS Attack

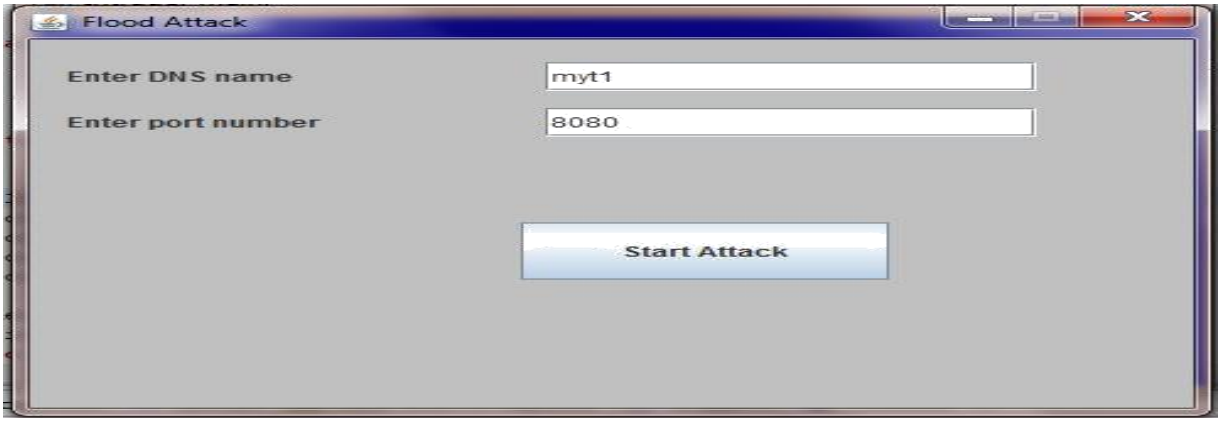

Fig.5 Flood Attack

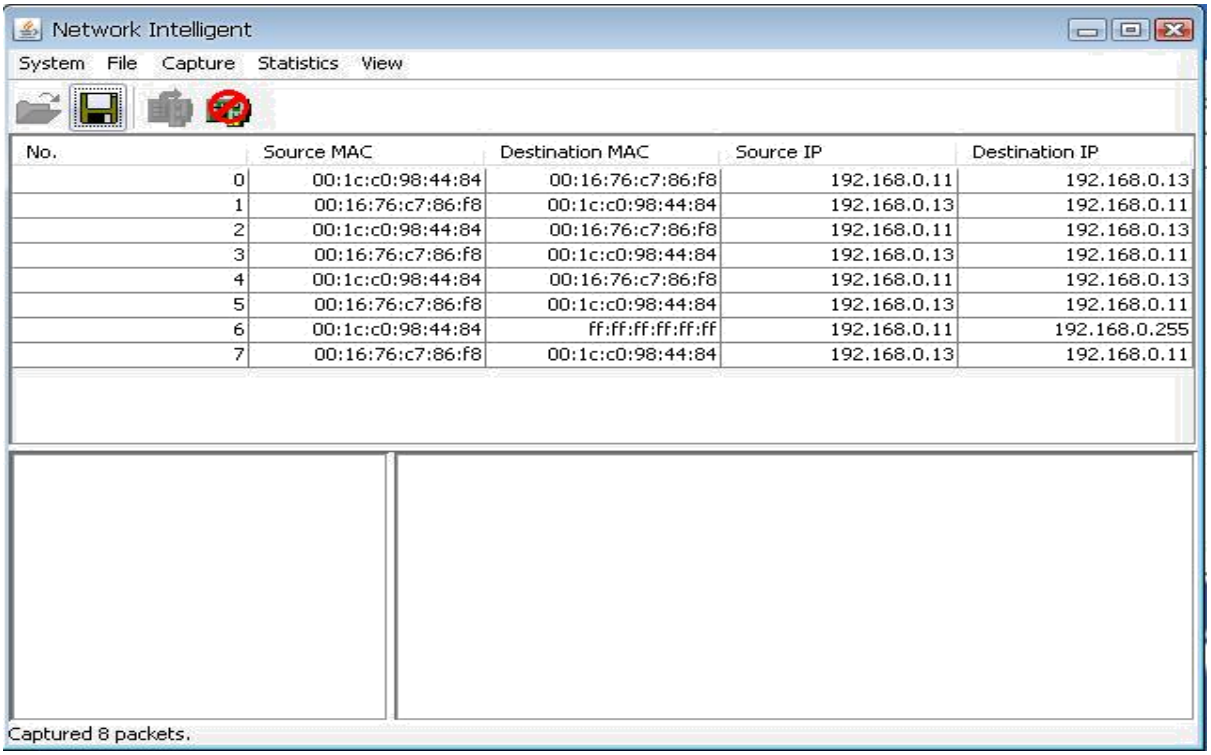

Fig.6 Detection of Flood Attack

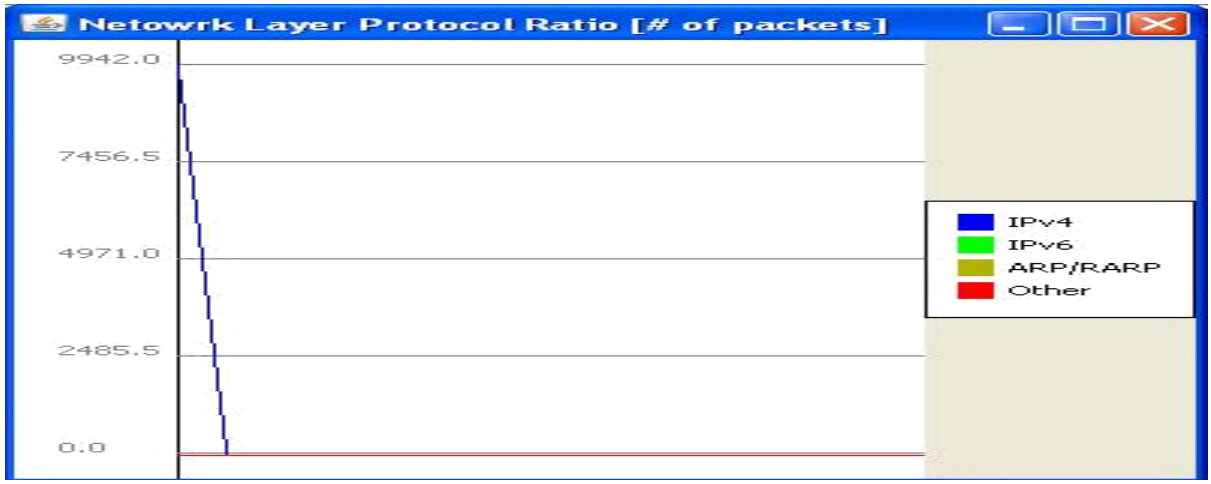

Fig.7 Statistical report of network layer

V. CONCLUSION

In this project, we employed rate limiting to mitigate flood attacks and proposed a scheme which exploits claim-carry-and-check to probabilistically detect the violation of rate limit. Our scheme uses efficient constructions to keep the computation, communication and storage cost low. We analyzed the lower bound and upper bound of detection probability. In the future, we will develop techniques for interestingness- based communication strategies for distributed IDS. These IDS will be based on organic computing principles. In addition, we will investigate how human domain knowledge can be used to improve the detection processes further. We will also apply our techniques to benchmark data that fuse information from heterogeneous sources (e.g., combining host and network-based detection).

REFERENCES

[1] Aqeel Sahi; David Lai; Yan Li; Mohammed Diykh,,"An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment,"Vol.5,pp. 6036 – 6048,April 2017.
[2] Quinghua Li, "To lie or to comply: defending Against Flood attacks in disruption tolerant networks,"IEEE Transactions on dependable and secure computing, vol 10, No. 3,pp.168-182, June 2013.
[3] Q.Li, W.Gao ,S.Zhu,and G. Cao,",A Routing Protocol for socially Selfish Delay Tolerant Networks‖,"Ad Hoc Networks, vol.10, No.8,pp.1619-1632, November 2012.
[4] K. Narasimha Mallikarjunan, ",A survey of distributed denial of service attack,**"**International Conference on Intelligent Systems and Control (ISCO),2016
[5] Jiong Zhang and Mohammad Zulkernine, "Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection", IEEE International Conference on Communications, 2006.
[6] P.Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, andC.Diot,"Packet Switched Networks and Human Mobility in Conference Environments,"Proceeding of ACM SIGCOMM, May 2005.
[7] Yanzhi Ren, "Detecting blackhole attacks in Disruption-Tolerant Networks through packet exchange recording", IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks,pp.1-6,June 2010.
[8] T. Socolofsky, C. Kale: "A TCP/IP Tutorial", RFC 1180, Spider Systems Limited, January 1991.
[9] A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, "Low cost Communication for Rural Internet Kiosks Using Mechanical Backhaul," Proc. ACM Mobicom, 2006.
[10] A. Valdes and K. Skinner, ",Probabilistic Alert Correlation, Recent Advances in Intrusion Detection‖, W. Lee, L. Me, and A.Wespi, eds pp. 54-68, Springer, June 2001.

