# Intelligent Inter and Intra Network Traffic Estimation Technique for DDoS Attack Detection using Fuzzy Rule Sets for QoS Improvement

V.ShyamalaDevi[1]
Associate Professor / Department of MCA
KSRCT,Tiruchengode , Tamilnadu
*emailtoshyamala@gamil.com*

Dr. R. Umarani[2]
Professor / Department of MCA,
Saradha Womens College, Salem, Tamilnadu
*umainweb@gmail.com*

***Abstract:-*** The quality of service of any network has higher dependency at throughput, latency and service completion strategies. In modern communication systems, there are many loopholes, which could be used by some malicious users to perform various network attacks so that the performance of the network is degraded. There are many denial of service when an approach has been discussed towards the problem of network threats, but still suffers the quality of denial of service attack detection. Propose a service-constrained approach learns the network traffic in various ways like the traffic incurred within the network and that comes from external network. The method uses various features like hop count, hop details, payload, TTl, time and so on. To maintain a rule set with fuzzy value where each rule specifies the feature of genuine packet being received. The incoming packet has to meet any of the rules and the attribute of the packet has to lie between the ranges of values in the rule. The proposed method estimates the inter traffic and intra traffic through the routes of the packet being transferred to identify the genuine nature of the packet being received. In addition, the method maintains set of logs where the packet features are stored to compute the legitimate weight of each packet being received. Based on compute inter and intra traffic values the received packets trustworthy is computed to allow or deny the packet. The proposed method increases the accuracy of DDOS attack detection and helps to improve the performance of the network.

***Key words:-*** *Inter Traffic, Intra Traffic, DDoS attack, Traffic Estimation, Fuzzy Rule Sets, QoS.*

*****

## I. INTRODUCTION

The real time network has more than one entry point to reach the destination node, which is located within the network. The external nodes in order to access the service send the packets through intermediate nodes to reach some node in external network. Generally, the packets are transferred in a co-operative manner to reach its destination. What happens in the middle is, there will be some middle node that performs malicious activities like dropping, modification of the packets. Otherwise, there are some nodes, which send more number of malicious packets where there is some limit in the number of packets for each node in the network.

Denial of service attack is one when a set of node sends more number of packets towards the service point, which is greater than the allowed limit. Huge numbers of packets are sent to the destination in the intension to degrade the service. Such malicious nodes have to be detected and the packets coming from that node should be dropped. The denial of service attacks can be detected in two ways according to the payload data and the number of packets being sent. In some cases like huge network conditions, there are some service packets that have limited time to live (TTL) value but may be affected by the middle nodes, which purposively delay the packet caused by modification. In addition, the modification attack may be performed which increases the payload size and makes the packet as malicious one. To identify such malicious packets the general TTL value, payload data or the number of packets will not help efficiently.

Traffic estimation is the factor, which represents the flow of packets in the network. There are two conditions to be considered like the number of packets being received from the nodes of the own network and the number of packets being received from the nodes which are located in external network. There are stages where there exists a malicious node outside the network or the botnet controller is present outside the network; then the malicious node may delay the packet, modify the content of the packet, or purposively increase the number of packets to generate denial of service attack.

Inter traffic is the traffic measure which shows the number of packets being received through a particular node which belongs to the same network in any point of time. The same inter traffic can be inferred by counting the number of packets being received from the node of same network and pass through the same node. The intra traffic is the measure, which is computed by identifying the number of packets being received from outside network through a specific path. The inter and intra traffic factors could be used to identify the botnet or malicious nodes so that the network performance will be improved.

The traffic fuzzy rules are the patterns that represent the traffic conditions between different sources and destinations. In this, each rule has various factors like payload, number of packets, time delay, and number of hops, hop details and many more. The time variant patterns could be used to form the rule sets and the rule sets are used to perform denial of service attacks detection.

## II. RELATED WORKS

There are various researchers proposing many methodologies related to the DDoS attacks, each have their own merits and demerits and discuss few of them here.

Host Based Intrusion Detection System [1] presents intrusion detection system which informs system administrator about potential intrusion incidence in a system. The designed architecture employee's statistical method of data evaluation allows detection based on the knowledge of user activity deviation in the computer system from learned profile representing standard user behavior.

Network Intrusion Detection System [2] embedded a NIDS in a smart-sensor-inspired device under a service-oriented architecture (SOA) approach. Use of this embedded NIDS can enables to operate independently as an anomaly-based NIDS, or integrated transparently in a Distributed Intrusion Detection System (DIDS). It combines the advantages of the smart sensor approach and the subsequent offering of the NIDS functionality as a service with the SOA use to achieve their integration with other DIDS components. It also addresses the construction of a physical sensor prototype. This prototype was used to carry out the tests that have demonstrated the proposal's validity, providing detection.

An Activity Pattern Based Wireless Intrusion Detection System [3] is designed for wireless network. It exploits pattern recognition techniques to model the usage patterns of authenticated users and uses it to detect intrusions in wireless networks. User activity is monitored and their discriminative features are extracted to identify intrusions in wireless networks. The detection module uses PCA technique to accumulate interested statistical variables and compares them with the thresholds derived from user's activities data. When the variables exceed the estimated thresholds, an alarm is raised to alert about a possible intrusion in the network. The novelty of the proposed system lies in its light-weight design, which requires less processing and memory resources and it can be used in real-time environment.

EAACK [4] proposes and implements a new intrusion-detection system named Enhanced Adaptive Acknowledgments (EAACK) specially designed for MANETs. EAACK consists of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, a 2-b packet header is included in EAACK.

ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack [9], presents a comprehensive study to show the danger of Botnet-based DDoS attacks on application layer, especially on the Web server and the increased incidents of such attacks that have evidently increased recently. This provides better understanding of the problem, current solution space, and future research scope to defend against such attacks efficiently. In particular, it proposes to use Matching Pursuit and Orthogonal Matching Pursuit algorithms. The major contribution of the paper is the proposition of 1D KSVD algorithm as well as its tree based structure representation (clusters), which can be successfully applied to DDoS attacks and network anomaly detection.

Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art [11], presents a comprehensive study to show the danger of Botnet-based DDoS attacks on application layer, especially on the Web server and the increased incidents of such attacks that has evidently increased recently. Botnet-based DDoS attacks incidents and revenue losses of different scenario. This provides better understanding of the problem, current solution space, and future research scope to defend against such attacks efficiently. Analyzing Feasibility for Deploying Very Fast Decision Tree for DDoS Attack Detection in Cloud-Assisted WBAN [12], proposes classifying data mining techniques which uses Very Fast Decision Tree (VFDT) and considered as the most promising solution for real-time data mining of high speed and non- stationary data streams gathered from WBAN sensors and therefore is selected, studied and explored for efficiently analyzing and detecting DDoS attack in cloud-assisted WBAN environment.

A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment [15], proposes a method of integration between HTTP GET flooding among Distributed Denial-of-Service attacks and Map Reduce processing for fast attack detection in a cloud computing environment. In addition, experiments on the processing time were conducted to compare the performance with a pattern detection of the attack features using Snort detection based on HTTP packet patterns and log data from a Web server. The experimental results show that the proposed method is better than Snort detection because the processing time of the former is shorter with increasing congestion.

Having explored all the intrusion detection methods and finding out that none of them has discussed the reactive intrusion detection, this research proposes a Novel Network Forensics analysis for the mitigation of DDoS attacks which is based on reactive one.

## III. PROPOSED METHOD

The proposed method has various stages namely inter traffic estimation, intra traffic estimation, DDoS Detection. To each of them is discussed detail in this section. In Feature Extraction stage, the packet features are extracted from the packet received. Extract the features namely Source ip, Source port, Destination ip, Destination port, Pay load size, TTL value, Hop count, Host names, Time received. Extracted features are converted into a feature vector or rule that is used to perform traffic approximation in the later stage.

### Algorithm

```
Input:  Captured Packet Pt.

Output: Rule Ri.

Step1: Extract Source Ip Sip = P t(Source Address).

Step2: Extract source port Sport = Pt (Sport).

Step3: Extract Destination IP DIP = Pt (Dest Address).

Step4: Extract Destination Port Dport = Pt (Dport).

Step5: Extract Host names Hnames = Pt (Host Names).
```

Step6: Compute Hop Count H-count = size of (H-names).

Step7: Extract Ttl value TTL = Pt(TTL).

Step8: Compute Payload = Pt(Size(Payload)).

Step9: Generate Rule Ri = {Sip, Sport,Dip, Dport, HCount,Hnames,TTl,Payload, Time}.

Step10:stop.

### A) Intra Traffic Estimation

At this stage, from the extracted features, the set of host names, which are located inside the network were identified. Once the list of nodes belonging to the same has been identified, then, from the traffic log available the average traffic is computed in the route. The average delay and average payload are being computed. Similarly the average hop count being incurred is estimated for the same route to reach the destination. Using these, the intra traffic factor for the route to reach the destination is estimated.

**Algorithm**

Input: Traffic Log Tl, Rule Ri.

Output: Intra Traffic Factor ITF.

Step1: Read packet feature Pf.

Step2: Identify the list of hops belongs to the same network.

Intra neighbor IN = $\int_{i=1}^{size(Hnames)} \sum Node \in HN$ //HN-Home network

Step3: compute average payload in the route IN.

Average Payload Apl = $\int_{i=1}^{size(Tl)} \frac{\sum Tl(i) \in IN}{no\ of\ traces}$

Step4: compute average hop count.

Ahc = $\int_{i=1}^{size(Tl)} \frac{\sum Hc(Tl(i) \in IN)}{Number\ of\ traces}$

Step5: compute average delay

ADl = $\int_{i=1}^{size(Tl)} \frac{\sum(Tl(i) \in IN).delay}{no\ of\ traces}$

Step6: compute ITF = $\frac{Apl \times Ahc}{no\ of\ common\ hops} \times ADL$

Step7: stop.

### B) Inter Traffic Estimation

Inter traffic estimation is the process of computing the traffic factor which incurred outside the network. For the packet being received and extracted feature identified, the set of host name is located outside the network. Once the host names are identified, then the inter traffic factor is computed using the common hops and the average payload and the average hop count are also computed. All measures used to compute the inter traffic factor will be used to compute the trustworthy of the packet being received.

**Algorithm**

Input: Traffic log Tl, Packet Feature F.

Output: ITTF.

Step1: start

Step2: Read packet feature F.\

Step3: Identify the list of hops belongs to other network.

Inter neighbor ItN = $\int_{i=1}^{size(Hnames)} \sum Node \in HN$ //HN-Home network

Step4: compute average payload in the route ItN.

Average Payload Apl = $\int_{i=1}^{size(Tl)} \frac{\sum Tl(i) \in ItN}{no\ of\ traces}$

Step5: compute average hop count.

Ahc = $\int_{i=1}^{size(Tl)} \frac{\sum Hc(Tl(i) \in ItN)}{Number\ of\ traces}$

Step6: compute average delay

IADl = $\int_{i=1}^{size(Tl)} \frac{\sum(Tl(i) \in ItN).delay}{no\ of\ traces}$

Step7: compute ITTF = $\frac{Apl \times Ahc}{no\ of\ common\ hops} \times IADL$

Step8: stop.

### C) Rule Set Generation

The fuzzy rule sets are generated using the traffic traces available in the node where the intrusion detection is performed or in the cluster head. First, the set of traces generated through the hops is identified and separated logs are used to generate the rules. The rule has various attributes like source address, source port, destination address, destination port, host names, hop counts, payload, TTL value, time. From the extracted results, the rule is computed with tolerance values or range values for each attribute specified above. The generated rule will be used to perform intrusion detection in the later stage.

**Algorithm**

```
Input: Packet Trace Tl, packet vector Pv.

Output: Rule Ri.

Step1: start

Step2: for each log l from Tl        Identify similar route like host names from Pv.

Similar route packets SRP= $\int_{i=1}^{size(Tl)} \sum Tl(i).Hostnames \in Pv.Hostnames$
                                                        End.

Step3: for each log from SRP

Compute average payload APL= $\int_{i=1}^{size(SRP)} \frac{\sum SRP(i).payload}{Size(SRP)}$

Compute average hop count

AHC = $\int_{i=1}^{size(SRP)} \frac{\sum SRP(i).hopcount}{Size(SRP)}$

Compute average TTL Attl = $\int_{i=1}^{size(SRP)} \frac{\sum SRP(i)TTL}{Size(SRP)}$

Compute average intra traffic factor AITF= $\int_{i=1}^{size(SRP)} \frac{\sum IntraTraffiFactor(SRP(i))}{size(SRP)}$

Compute average inter traffic factor AItTF= $\int_{i=1}^{size(SRP)} \frac{\sum InterTraffiFactor(SRP(i))}{size(SRP)}$

Compute common host names CHN= $\int_{I=1}^{SRP(i)} (SRP(i) \cup CHN) \cap Pv.Hnames$

        End.

Step4: generate the rule Ri={APL,AHC,TTL,AITF,AItTF,CHN}

Step5: stop.
```

**D) DDoS Detection**

The Denial of service attack is being detected by using all the above-discussed functionalities like Intra traffic inference, Inter traffic inference, and Rule generation. Whenever a new packet is being received, the feature extraction phase is performed. Once the path being identified, the presence of the path in the malicious log is identified to verify whether the packet is genuine or malicious. If there is no entry present in the malicious log, then for the host names or the path of the packet is being traversed to generate the rule. The rule generation process internally computes the inter traffic estimation and intra traffic estimation values which represent the general traffic pattern or possible delay factors within the network or outside the network. There are situation where the botnet or malicious nodes may be present outside the network or inside the network. By computing inter and intra traffic estimations the malicious node and its locations can be identified easily. In this approach from the generated rule, and using the feature vector the inter and intra traffic estimation values can be computed. Using all these, if the packets inter and intra traffic values lie within the tolerance values, the packet will be allowed; otherwise it will be denied and generate a malicious log.

**Algorithm**

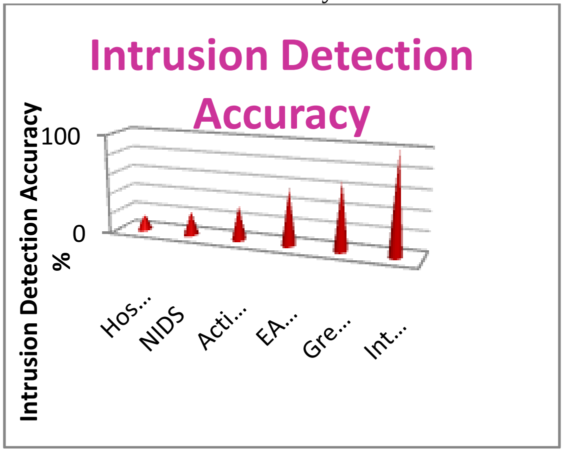
```
Input: Packet Feature Pv, Malicious Trace Mt.

Output: Boolean

Step1: start

Step2: Read packet feature Pv.

Step3: Read Malicious trace Mt.

Step4: Identify source and destination addresses from Pv.

                SAddr = Pv(Saddress).

                DAddr = Pv(Daddress).

                Sport = Pv(Sport).

                Dport = Pv(Dport).

Step5: for each log from Mt

                Perform equivalence operation.

 lag= $\int_{i=1}^{size(Mt)} (Mt(i).Saddr == Pv.Saddr \&\& Mt(i).Sport = Pv.Sport \&\& Mt(i).Daddr == Pv.Daddr \&\& Mt(i).Dport == Pv.Dport, Mt(i).Hnames == Pv.Hnames) 1,0$
        End

Step6: if Flag = =1 then

                Drop packet

        Else

                Compute Inter traffic Estimation ITF = Inter traffic estimation(Pv).

                Compute Intra Traffic Estimation InTF = intra traffic Estimation (Pv).

                Generate Rule Ri = RuleGeneration(Pv).
        If Ri.ITF>ITF && Ri.InTF>InTF then
            Allow packet.
    Else
        Generate malicious log in Mt.
    End
    End
Step7: stop.
```

From the above discussion, it is clear that the incoming packets is being extracted for its features and then inter traffic and intra traffic estimations are performed. Then rule generation is performed using the feature vector. Finally, by using all the measures computed, the packet is identified as malicious or genuine one.

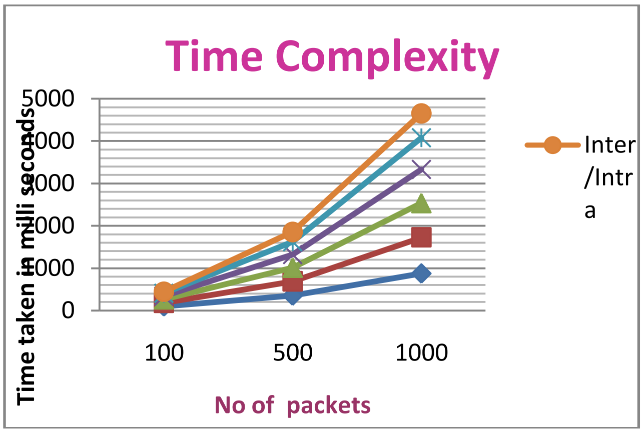
## IV. RESULT AND DISCUSSION

The proposed inter/intra traffic estimation technique for denial of service attack detection has produced good results. Unlike other intrusion detection system, have used the common hop addresses present in the traversal path of the packet. Because whenever the malicious packet reaches the service port it follows the various malicious nodes. The source of the malicious packet could not be identified but still we can identify the malicious node which are supporting the malicious nodes or attacking nodes. By identifying the supporting nodes we can reduce the frequency of attacks generated.

The graph1 shows the result of the intrusion detection performed by the proposed method where the measure is computed by capturing 500 packets. The graph shows the frequency of detection of malicious packet. It is very clear that the proposed system identifies the more malicious packet compare to other host based and activity pattern based intrusion detection systems.

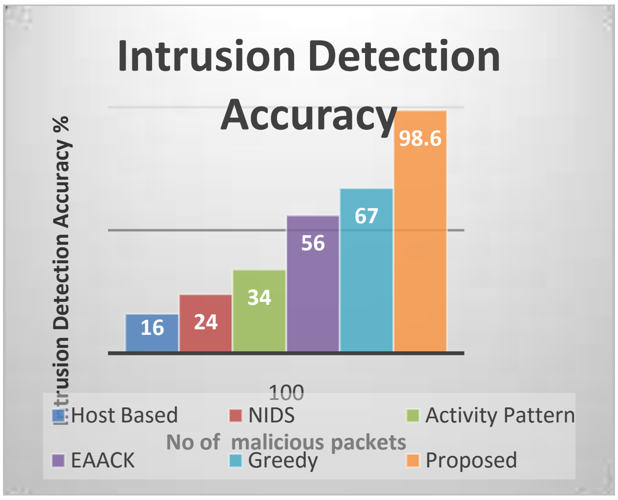


**Graph1: shows the frequency of detection of malicious packet**



**Graph2: shows the time complexity of the proposed system.**

The graph2 shows the time complexity of the proposed system compare to other methodologies. It shows clearly that the proposed system takes only little time compare to other methods for different number of packets.



**Graph3: Comparison of intrusion detection accuracy.**

The graph3 shows the comparison of DDoS attack detection accuracy and it shows clearly that the proposed approach has produced efficient result and produces more accurate results.

## V. CONCLUSION

Proposed an Inter/Intra network traffic estimation technique to perform denial of service attack detection to improve the performance of the network. The incoming packet features are extracted and with the help of malicious history the packet initially tested for malicious one. If it is malicious the packet will be dropped otherwise to compute the inter traffic estimation and intra traffic estimation and generate the rule. From generated rule, to identify the packets trustworthy. The proposed approach has produced efficient results in both DDoS detection accuracy and time complexity as well.

## REFERENCES

[1] Vokorokos, L. Host Based Intrusion Detection System, Intelligent Engineering Systems (INES), **Page(s):** 43 – 47, 2010

[2] Maciá-Pérez, F Network Intrusion Detection System Embedded on a Smart Sensor, Industrial Electronics, IEEE Transactions on Volume:58 , Issue: 3 Page(s): 722 – 732, 2012.

[3] Haldar, N.A.H An Activity Pattern Based Wireless Intrusion Detection System Information Technology: page(s): 846 – 847, 2012

[4] Elhadi M. Shakshuki , EAACK—A Secure Intrusion-Detection System for MANETs, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013 1089

[5] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[6] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey," in Proc. 2nd Int. Meeting ACCT, Rohtak, Haryana, India, 2012, pp. 535–541

[7] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[8] B. B. Gupta, R. C. Joshi, ManojMisra, "ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack," International Journal of Network Security (IJNS), vol. 14, no. 1, pp. 36-45, 2012.

[9] B. B. Gupta, R. C. Joshi, ManojMisra, "ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack," International Journal of Network Security (IJNS), vol. 14, no. 1, pp. 36-45, 2012.

[10] Tomasz Andrysiak, kaszSaganowski, MichałChoraś, DDoS Attacks Detection by Means of Greedy Algorithms, Image Processing and Communications Challenges 4, Advances in Intelligent Systems and Computing Volume 184, 2013, pp 303-310

[11] EsraaAlomari, elvakumarManickam, B B Gupta, Shankar Karuppayah and RafeefAlfaris. Article: Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art. International Journal of Computer Applications 49(7):24-32, July 2012.

[12] RabiaLatif, HaiderAbbas, Saïd Assar, SeemabLatif, Analyzing Feasibility for Deploying Very Fast Decision Tree for DDoS Attack Detection in Cloud-Assisted WBAN, Springer, Intelligent Computing theory, vol 8588, pp 507-519, 2014.

[13] Katkamwar, N.S., Puranik, A.G., Deshpande, P.: Securing Cloud Servers against Flooding Based DDoS Attacks. International Journal of Application or Innovation in Engineering & Management (IJAIEM) 1(3) (November 2012)

[14] JunhoChoi, Chang Ko, Pankoo Kim, A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment, Springer, Soft computing, Volume 18, Issue 9, pp 1697-1703, 2014.