International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

A Novel Method For DDoS Attack Prevention In Wireless Network Using QoS Oriented Distributed Routing Protocol(QOD)

A. Nandhini[1], N. Senthilkumaran[2]

[1]Researscholar, M.Phil Computer Science, Vellalar College for women, Erode12
[2]Director, Department of Computer Applications, Vellalar College for Women, Tamilnadu, India.

Abstract - *A Distributed Denial-of-Service (DDoS) is an attack in which attackers generate a huge amount of message to victims by compromised computers (zombies) with the aim of attacker denying normal service or mortifying of the quality of services. The flood of incoming messages to the target system basically forces it to shut down, thus denying service to the system to legitimate users. The IP traceback mechanism is one of the techniques in which is used to identify the attacked source packet from DDoS attack in wireless network. In this work IP traceback mechanism for DDoS attack based on entropy variations between normal and DDoS attack traffic, which is fundamentally different from commonly used packet marking techniques. In this paper, QoS-Oriented Distributed routing protocol (QOD) is proposed to enhance the QoS support capability of wireless network. QOD protocol consist of Neighbour node selection, packet schedule, a mobility-based packet resizing, Traffic redundant elimination and data redundancy elimination algorithms. The neighbour node selection algorithm is used to reduce the transmission delay between the source and the destination node. The packet loss process reduces by using packet schedule algorithm. Packet resizing based on mobility of nodes to reduce the transmission time and packet loss .Traffic redundant elimination algorithm to increase the transmission throughput based on packet forwarding and packet scheduling. A data redundancy elimination algorithm is used to remove the redundant data for further improves the transmission QoS.*

***Key Words*: Distributed Denial-of-Service, QOD, Wireless Network, TRE, LSF.**

1. INTRODUCTION

Wireless network is an interconnection of many systems capable of providing service to mobile users within an exacting geographic region. In wireless network, data are carried by radio wave from one node to another node. Wireless security is the avoidance of unauthorized access and damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).WEP is a security protocol for Wi-Fi networks which is protocol add security to a wireless network by encrypting the data.WPA is a security protocol designed to create secure wireless (Wi-Fi) networks. It handles security keys and the way users are authorized which is similar to the WEP protocol but it provided improvement in the way.

A wireless attack is a malicious action beside wireless system information or wireless networks. The following needs to be considered in security components are Confidentiality, Integrity and Availability. Confidentiality means the non-authenticated person does not look at the data. Integrity is provided security to the data which is receiver does not modify that data after received by sender. Availability aims to create confident that information is readily available to authorized users.

A distributed denial-of-service attack (DDoS attack) tries to make a computer resource unavailable to its intended users. DDoS attacks aim at exhausting the victim's resources, such as network bandwidth, computing power and operating system data structures. The attackers first established a network of computers for launch a DDoS attack which is used to generate the huge volume of traffic needed to deny services to legitimate users of the victim.

Attackers discover vulnerable hosts on the network to create this attack network. The vulnerable hosts are those either running no antivirus or out of date antivirus software and those that have not been correctly patched. These are exploited for use the vulnerability to gain access to this host by the attacker. In compromised hosts of the attack network, attacker is to be installing new program. These attack tools running on attack host are known as zombies, and they can be used to carry out any attack under the control of the attacker [16].

There are two categories of DDoS attack, usual DDoS attacks and Distributed Reflection Denial-of-Service (DRDoS) attacks. The master computer orders the zombies run the attack tools to send huge volume of packets to the victim for exhaust the victim's resource in usual DDoS attack. The master zombies to send a flow of packet with victim IP address by that lead the slave zombies which is called reflectors. Then the reflectors send to the victim a huge volume of traffic as a reply to its refrain for the opening of a new connection. In this paper discussed about prevention of the DDoS attack.

The main objective of the research is,

- Reduce the transmission time & delay and packet loss using QoS-Oriented Distributed routing protocol (QOD)
- Identifying the attacked source packet based on entropy variation in DDoS attack by using IP traceback algorithm.
- To improve the overall system performance

A Distribute Denial of Service (DDoS) attack happens when a service that would usually work becomes busy. There are many reasons for unavailability which it's usually refers to infrastructure that cannot handle suitable for capacity overload. A large number of systems maliciously attacking one target which result are DDoS attack. This is often finished by a botnet where many devices are automatic to request a service at exactly the same time.

By using different techniques, local flow monitoring [16] and IP traceback algorithm and QoS-oriented distributed routing protocol (QOD) is detect and prevent the DDos attack in wireless network. IP traceback schemes are considered successful if they can identify the zombies from which the DDoS attack packets entered the node.by using entropy variation [5].QOD is the first work for QoS routing in wireless networks. This thesis work makes five contributions.

- QoS-guaranteed neighbor selection method. This method selects eligible neighbors and employs deadline-driven scheduling mechanism to guarantee QoS routing.

- Distributed packet scheduling method. In this method schedules the packet routing after qualified neighbors are identified. To forwarders with higher queuing delays, it assigns previous generated packets, while assigns more recently generated packets for forwarders with lower queuing delays to reduce total transmission delay.

- Mobility-based segment resizing method. The source node adaptively resizes the each packet in its packet flow for each neighbor node according to the neighbor's mobility. In order to raise the scheduling possibility of the packets from the source node.

- Soft-deadline based forwarding scheduling method. In this method, first an intermediate node forwards the packet with the least time that's allowed to wait before being forwarded out to reach equality in packet forwarding.

- Data redundancy elimination based transmission method. This method eliminates the redundant data to improve the QoS of the packet transmission. The APs and mobile nodes can overhear and cache packets for appropriate to the distribution feature of the wireless networks

II.LITERATURE REVIEW

Akash Mittal et al., [6] had studied different types of DDoS techniques. Internet is the foremost intermediate for communication which is used by number of users across the network. At the same time, its commercial character is causing increase exposure to enhance cybercrimes and there has been a vast increase in the number of DDoS (distributed denial of service attack) attacks on the internet over the earlier period decade. In this paper basically summarizing different techniques of DDoS such as Bloom Filter, Trace Back method, Independent Component Analysis and TCP Flow Analysis.

Yoohwan Kim et al., [2] had discussed about protect against ddos attack based on Statistics-Based Packet Filtering Scheme. This scheme support automated online attack characterization and discarding the affected packet, when score of packet is computed based on statistical processing. This paper describes the design and estimate of automated attack characterizations, selective packet discarding, and an overload control process. Design of packet score has suitable for a large volume attack and it does not work well with low-volume attacks.

Tao Peng et al., [4] presented a survey of denial of service attacks and the methods that have been proposed for defense against these attacks. In this survey, it analyzed the design decisions in the Internet that have created the potential for denial of service attacks. They reviewed the state-of-art mechanisms for defending against denial of service attacks and compare the strengths and weaknesses of other network model. The most effective DoS defense scheme is to detect and block attack traffic close to the source. However, the implementation cost for this scheme is high, due to the difficulty in discriminating between legitimate and malicious traffic at its source.

Lukasz Apiecionek et al., [5] described quality of service could be used as a protection tool against DDoS attack. The QoS method has to remove traffic from the queue by using Random Early Detection (RED) with special condition. The QoS Fair Queue method is used for the standard operation of the device and transmits packets to the receiver. Correct connection history is gathered based on the Fair Queue method. When a DDoS attack is detected, the packets are transmitted to a special data stream recognition module and it compares them with the correct connection history database. The QoS method concept of eliminating DDoS attacks with information which proves that using this concept is possible in the real environment.

N. Syed Siraj et al., [1] described Detection of Denial of Service Attack in Wireless Network using Dominance based Rough Set. Denial-of-service (DoS) attack is aim to block the services of victim system either temporarily or permanently by sending huge amount of garbage traffic data in various types of protocols. Maintenance of uninterrupted service system is technically difficult as well as economically costly. In general, probabilistic packet marking (PPM) and deterministic packet marking (DPM) is used to identify DoS attacks. But it is observed that, data available in the wireless network information system contains uncertainties. Therefore, an effort has been made to detect DoS attack using dominance based rough set.

III. METHODOLOGY

IP-traceback and QOD algorithms are used to prevent the DDoS attack in wireless network environment. The attacked source IP-address is captured by using IP-traceback

algorithm and QOD protocol to enhance the quality of support capability and transforms the packet routing to a resource scheduling problem in wireless network.

3.1 IP TRACE BACK ALGORITHM

1. initialize the local threshold parameter, C, □, and sampling interval □T;
2. identify flows, f1, f2, …., fn, and set count number of each flow to zero, x1 = x2 = … = xn = 0;
3. Define attack flows, f = <u, v>, i =1, 2,…,n, u□□ U, and sort the attack flows in descent order, and we have f'1, f'2, …, fn'.
4. for i=1 to n

{

Calculate H (F\f'$_i$,)

If (| H(F) – C | > d) then append the responding upstream router of f'$_I$, to set A

Else break;End if; End for;

3.2 QOD PROTOCOL MODEL

The attacked packets deleted from IP traceback method and remaining original packets are transferred to client by using QoS Distribution routing protocol (QOD). The main of the QOD is to reduce transmission time and increase the network capacity. This protocol is checking Quality of packets from the SN node. In QOD if source node is not within the transmission range of the access point, the source node has to choose the nearby neighbor nodes where the transmission path should be QoS guarantee. There may be "n" number of neighbor nodes between source and destination. The QoS service through the implementation of techniques as follows.

A. QoS-guaranteed neighbor selection

In this step, an intermediated node assigns the higher priority with closest deadline and forwarded the higher priority packet first. It use $s_p(i)$ to denote the size of the packet steam from node n_i and w_i to denote the bandwidth of node and T to denote the packet arrival interval from node n_i and it set threshold value. The QoS of the packet through node $n_i$can be satisfied if

$$\frac{S_p(1)}{T_a(1)} + \frac{S_p(j)}{T_A(j)} + \frac{S_p(j)}{T_A(j)} + \cdots + \frac{S_p(m)}{T_A(m)} \leq W_i \qquad (1)$$

In QOD, an intermediated node with space utility less than threshold replies the source node after receiving a forward request from a SN node. The SN node calculates queuing delay based on replies from neighbor node and makes confirm if the path satisfies QoS deadline. Otherwise, the SN node rejects the neighbor node and chooses another path. The work load allocation can be made for QoS deadline satisfied nodes.

B. Distributed packet scheduling

After qualified neighbors are identified and perform packet schedules packet routing. It assigns earlier generated packets to forwarders with higher queuing delays, while assigns more recently generated packets to forwarders with lower queuing delays to reduce total transmission delay and reduce the stream transmission time. This algorithm assigns before generated packet to forwards with higher queuing delays and scheduling feasibility, while assigns more recently generated packets to forwarders with lower queuing delays and scheduling so that the transmission delay of the entire packet stream can be reduced.

It use t to denote the time when a packet is generated and use T_{QoS} requirement and w_S and w_i denote the bandwidth of a source node and an intermediate node. The transmission delay between SN to intermediated node is denote by $\mathbf{T_{s\rightarrow I} = s_p/w(s)}$ and $\mathbf{T_{I\rightarrow D} = s_p/w(I).}$ The packet queuing time denote by T_w and the packet queuing time of n. The source node needs to calculate T_w of each intermediate node to select intermediate nodes that can send its packets by the deadline that's satisfied $\mathbf{T_w < T_{QoS} - Ts\rightarrow I - T_I\rightarrow D.}$

After receiving the reply messages from neighbor nodes that includes the scheduling information of all flows in their queues. The SN node calculates the T_w of its packets in each intermediate node and then chooses the intermediate node n that satisfies $\mathbf{T_w < T_{QoS} - Ts\rightarrow I - T_I\rightarrow D.T.}$

C. Mobility-based segment

In wireless network, the transmission link between two nodes is frequently broken down. The delay generated in the packet re transmission degrades the QoS of transmission of a packet flow. The source node resizes each packet in packet stream for each neighbor node rendering to the neighbor's mobility in order to increase the scheduling feasibility of the packets from the source node. The basic idea is larger-size packets are assigned to lower-mobility intermediate nodes. The smaller-size packets are assigned to higher-mobility intermediate nodes, which increases the QoS-guaranteed packet transmissions. When the mobility of a node rises, the size of a packet Sp send to its neighbor nodes i reduction as following

$$\mathbf{Sp\ (new) = \gamma / v_i\ (Sp\ (unit))} \qquad (2)$$

Where γ is a scaling parameter, v_i denotes the relative mobility speed of the source node and neighbor node and Sp (unit) = 1kb.

D. Soft-deadline based forwarding scheduling

In packet forwarding scheduling, use the soft-deadline application for achieves fairness. The Least slack first scheduling (LSF) algorithm can use through forward node. The packet of slack time can be calculated by Dp– t – c Where, *Dp*- The packet delay, *t* - The current time of the

packet *c*- The remaining packet transmission time of a packet.

The slack time of each packet can be calculate by an intermediate node and forwards the minimum slack time packet. The packet could be randomly chosen if it all packets has the same slack time. It aims to make delays and the sizes of delay almost the same. In this algorithm equality in packet forwarding and scheduling can be achieved.

E. Data redundancy elimination based transmission

In this step, eliminates the redundant data to improve the QoS of the packet transmission which uses an end-to-end Traffic Redundancy Elimination (TRE) algorithm in QOD. By using TRE a chunking scheme for determine the boundary of the chunks in a data stream. The source node (SN) contain it sender data and the receiver also stores its received data. The SN node scans the content for duplicated chunks in its cache, before starting the transmission of the packets. It reduces the piece with its chunk cross, if it finds any duplicate chunk. Because it knows that server and the intermediate node receives the packet already. The node is search on local cache when server receives the chunk signature. If server store the chunk associated with signature, it sends an acknowledgement message to the sender and replies the signature the matched data chunk else server request chunk of the signature source from sender

IV. RESULTS AND DISCUSSION

The results are discussed under the performance of Distribute Denial Of services Attack prediction model. The result of proposed IP track and QOD system is discussed and compared with the routing protocol. To measure the performance of the proposed works are data services packet sending rate, Attacker ratio and Throughput evaluated. The necessary input parameters are given in Configure in file. The simulation procedure should be specific about certain parameter as mentioned below to enable table simulation and implementations.

Table 4.1 Network Parameter

PARAMETER	VALUE
Simulation tool	Java Net Bean
Simulation Time	100ms
Number of Packets	100
Routing Protocol	IP and QOD Routing protocol
Performance Metrics	Packet sending Rate, Attacker Ratio and Throughput

The Table 4.1 shows the parameters of the proposed network environment. These parameters were adhered to whole process of simulation with the Net bean framework. The Performance metrics are Packet Sending Rate, Attacker Finder and Throughput. The following Table 4.2 describes experimental result for IP Tracking Algorithm performances analysis. The table contains sources node id, Neighbor node id, packet size, speed and average of performances rate details are shown. The O (N) best case analysis (Performances rate) for proposed IP tracking system is,

Performance (IP Tracking Algorithm) Rate= [(Packet Size/Speed) *60] /100

Table 4.2 Performances Rate Analysis- IP Tracking Algorithm

S.No	Sources Node ID	Packet Size (Byte)	Speed (ms)	Performance Rate [%]
1	N1	1635	19	51.63
2	N2	593	8	44.47
3	N3	1365	18	45.5
4	N4	531	10	31.86
5	N5	658	9	43.86
6	N6	1677	23	43.74
7	N7	539	12	26.95
8	N8	1206	17	42.56
9	N9	1405	20	42.15
10	N10	649	9	43.26

The following Figure 4.1 describes experimental result for IP Tracking Algorithm performances analysis. The figure contains sources node id, Neighbor node id, packet size, speed and average of error rate details are shown.

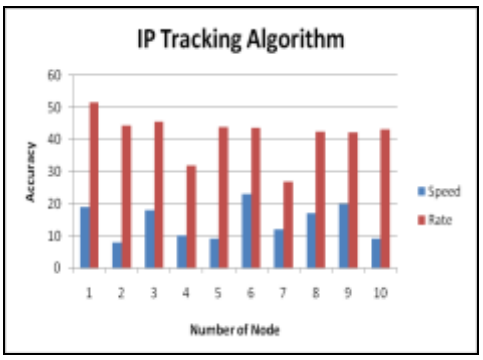

Fig 4.1 Performances Rate Analysis- IP Tracking Algorithm

The following Table 4.3 describes experimental result for QOD Routing Algorithm performances analysis. The table contains sources node id, Neighbor node id, packet size, speed and average of performances rate details are shown. The O (N) best case analysis (Performances rate) for proposed QOD Routing system is,

Performance (QOD Routing) Rate= [(Packet Size/Speed) *60] /100

Table 4.3 Performances Rate Analysis- QOD Routing Algorithm.

S.No	Sources Node ID	Destination Node ID	Packet Size (Byte)	Speed (Minutes)	Performance Rate[%]
1	N1	N3	1635	15	65.4
2	N2	N7	593	5	71.16
3	N3	N8	1365	11	74.45
4	N4	N10	531	8	39.82
5	N5	N3	658	5	48.90
6	N6	N1	1677	23	43.74
7	N7	N9	539	10	32.34
8	N8	N5	1206	14	51.68
9	N9	N4	1405	18	52.22
10	N10	N1	649	7	55.62

The following **Figure 4.2** describes experimental result for QOD Routing Algorithm performances analysis. The figure contains sources node id, Neighbor node id, packet size, speed and average of error rate details are shown

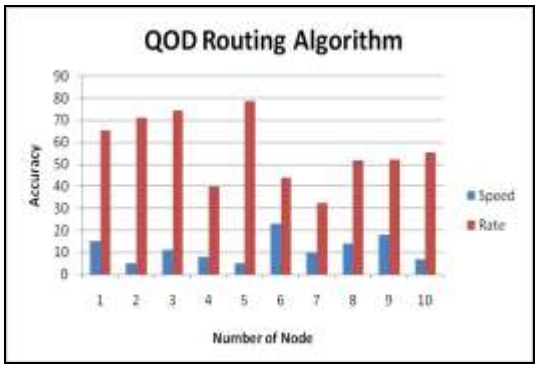

Fig 4.2 Performances Rate Analysis-QOD Routing Algorithm

The following **Table 4.2 and 4.3** describes comparison between IP-T and QOD Routing Algorithm performances analysis. The table contains sources ID, packet size and averages of performances rate details are shown. The comparison of Slice Based protocol performances rate is best for QOS-Distribute protocol.

Table 4.4 Comparison between IP-Track and QOD-Routing Model

S.NO	Sources Node ID	Packet Size (Byte)	Performance Rate[%]	
			IP-Track	QOD-Routing
1	N1	1635	51.63	65.4
2	N2	593	44.47	71.16
3	N3	1365	45.5	74.45
4	N4	531	31.86	39.82
5	N5	658	43.86	48.90
6	N6	1677	43.74	43.74
7	N7	539	26.95	32.34
8	N8	1206	42.56	51.68
9	N9	1405	42.15	52.22
10	N10	649	43.26	55.62

The following **Fig 4.1 and 4.2** describes comparison between IP and QOD Routing Algorithm performances analysis. The figure 4.3 contains sources ID, packet size and averages of performances rate details are shown. The comparison of Slice Based protocol performances rate is best for QOS-Distribute protocol

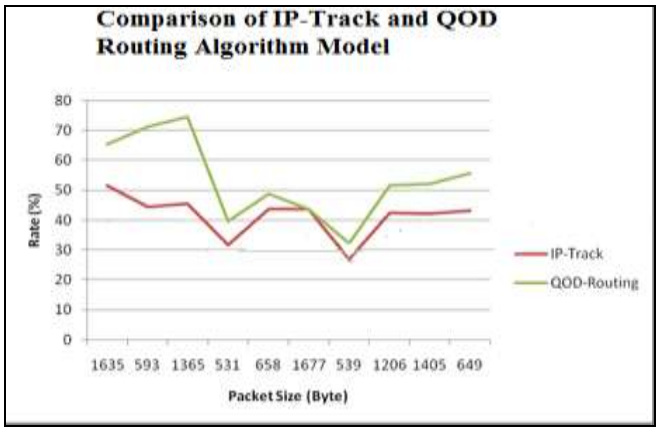

Fig 4.3 Comparison of IP -Track and QOD Routing Algorithm Model

V. CONCLUSIONS

In this paper, proposed an effective and efficient IP traceback scheme against DDoS attack based on entropy variations. It detects and store short-term information of flow entropy variations at routers. The victim using pushback tracing procedure in IP traceback algorithm for identified the DDoS attack. In this algorithm first identifies its upstream router for where attack comes from, and then submits the traceback requests to related upstream routers. The procedure continues until zombies are identified. Another method in proposed work is QOD protocol. The QOD incorporate five methods. First method, qualified neighbors chooses for

packet forwarding by using QoS guaranteed neighbor selection method. Reduce the packet transmission time by using packet scheduling method. Resize the packets and assign smaller packets with mobility through packet resizing method. The traffic redundant elimination based transmission method used for increasing the transmission throughput. Finally soft deadline based forwarding method applying some packets are not feasible in packet forwarding to achieve the equality. In this proposed work QOD can achieve high mobility flexibility, scalability and disputation reduction.

In future, by improving the performance level of DDoS attack prevention has used in different algorithm will be applied in wireless network security and proposed schema will be tested against other type of attack.

REFERENCES

1) Syed Siraj Ahmed.N and D. P. Acharjya "Detection of Denial of Service Attack in Wireless Network using Dominance based Rough Set" (JACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 12, 2015Michael T. Goodrich, "Probabilistic Packet Marking for Large-Scale IP Traceback" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. X, NO. X, JANUARY 2007.

2) Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah and H. Jonathan Chao "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 3, NO. 2, APRIL-JUNE 2006..

3) Yang Xiang, Wanlei Zhou, and MinyiGuo "Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 20, NO. 5, MAY 2009.

4) Tao Peng, Christopher Leckie, And Kotagiri Ramamohanarao "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems" ACM Computing Surveys, Vol. 39, No. 1, Article 3, Publication date: April 2007. N. Syed Siraj Ahmed and D. P. Acharjya "Detection of Denial of Service Attack in Wireless Network using Dominance based Rough Set" (JACSA) International Journal of Advanced Computer Science and Applications, Vol. 6, No. 12, 2015.

5) LuKaszApiecionek, Jacek M. Czerniak, and Wojciech T. Dobrosielsk "Quality of Service Method as DDoS protection Tool" D.Fileve et al. (eds.), Intelligent Systems' 2014, Advances in Intelligent Systems and Computing 323, Springer International Publishing Switzerland 2015

6) Akash Mittal, Prof. Ajit Kumar Shrivastava, Dr. Manish Manoria"A Review of DDOS Attack and its Countermeasures in TCP Based Networks" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011