International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Exclusion of Denial of Service Attack using Graph Theory in MANETS

Preeti[1], Anuradha T[2]

[1]*PG Student, Department of CSE, PDA College of Engineering, Kalaburagi, Karnataka, India.*
preetipsg100@gmail.com
[2]*Assistant Professor, Department of CSE, PDA College of Engineering, Kalaburagi, Karnataka, India.*

Abstract -*Mobile ad hoc networks (MANET) are wireless, multi-hop, infrastructure less collection of self organizing mobile devices that form a temporary cooperative network without any base station. Sending packets from one device to another is done via chain of intermediate nodes. Because of dynamic topology node can enter or leave network at any time, during this, malicious node can enter and harm the network. The main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be insecure to various attacks such as Denial of service (DoS)attack .One of the major DoS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. Different solutions have been proposed to eliminate the dos attack, however, these solutions often compromise routing efficiency or network overhead. Here a novel method has been focused on detection and prevention of DoS attack using trust based mechanism which is based on the graph theory, where the trust value is obtained based on the behaviors and activity information of each node to secure the routing protocol because it has a better performance rather than cryptography method. Results show that secured transmission is done in the nodes by overcoming the DoS attack, where the data travels in the honest route by mitigating the DoS attack.*

***Key Words*: DoS, Graph theory, MANEts, OLSR, Trust mechanism.**

1. INTRODUCTION

Mobile ad hoc Network (MANET) is a group of mobile devices capable of communicating wirelessly with each other without using a predefined infrastructure or centralized authority. These nodes are not dependent and they act as both host and as well as router to send the data. Every node in MAENT has to maintain the communication range. Due to mobility of nodes topology changes rapidly with varying time. Due to the dynamic topology the malicious nodes can enter with the honest nodes and degrade the network performance in the form of attack. In this paper, the avoidance of Denial of Service (DoS) attack in the MANETs is proposed.

1.1 Graph theory

Graph theory used to model pair wise relations between neighboring nodes. A graph theory in this context is made up of nodes which are connected by edges that are link between nodes. Graph is an ordered pair G = (V, E) consisting a set of nodes 'V' together with a set of edges 'E'. V is a set formed with a relation of incidence that associates with each edge of two vertices. Many real world situations can handily be represented by convey of a diagram consisting of a set of points together with lines joining certain pairs of these points. For example, the points could represent people, with lines joining pairs of friends; or the points might be communication centers, with lines representing communication links.

1.2 Denial of service (DoS)

In this type of attack, an attacker attempts to prevent the legitimate and authorized users from the services offered by the network. The node isolation is type of dos attack.

Node isolation attack In this attack, an attacker exploits the fact that the victim prefers a minimal MPR (Multi Point Relay) set in order to hide the existence of the victim in the network. The attacker, which must be located within broadcast distance of the victim, advertises a fake HELLO message claiming to be in close proximity to all of the victim's two-hop neighbors. In addition, a fictitious node is advertised, giving the attacker an advantage over other possible legitimate candidates for MPR selection. Knowledge of the victim's two-hop neighbors is readily available by analyzing TC (Topology Control) messages of the victim's one-hop neighbors, a list of which can be constructed directly from the HELLO message broadcast by the victim himself. MPR selection rule would cause the victim to exclusively select the attacker as its MPR, as it is the minimal set that allows for coverage of all of the victim's two-hop neighbors (including the fictitious node).DOS is now straightforward. The attacker can isolate the victim simply by not including the victim in its TC message. In essence, the attacker refrains from notifying the network that the victim can be reached through it, and because no other node advertises a path to the victim, it is isolated. Other nodes, not seeing link information to the victim, would conclude that it has left the network, and remove its address from their routing tables. Although nodes one-hop and two-hops from

the victim would continue to exchange information with it, they will not propagate that information further as they were not designated as its MPR.

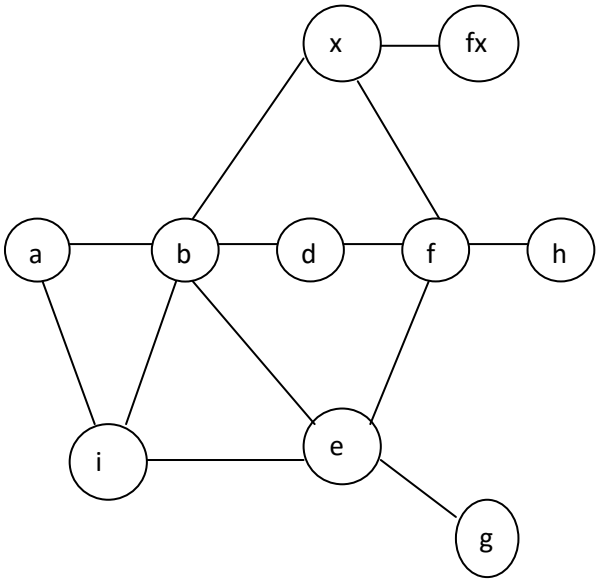

Fig-1 Example of a node isolation attack: node x claims to know every two-hop neighbor of b, as well as Fx, a non-existent node.

The node isolation attack is illustrated by Fig. 1. Assume all nodes within broadcast distance have an edge connecting them, that node x is the attacker, that Fx is a fictitious node, and that node b is the victim. The cloud in the figure represents the rest of the network. OLSR rules state that x should have advertised a legitimate HELLO message containing {b; f}. Instead, it sends a fake HELLO message that contains {b; f; g; Fx}. This list contains all of b's two-hop neighbors, as well as one non-existent node, Fx. b would now innocently select x as its sole MPR, setting the ground for node isolation. By not advertising b in its TC message, x effectively isolates b from the rest of the network.

2. RELATED WORK

Many studies in DoS attack in MANET. In [1], The watchdog approach based on two Bayesian filters Bernoulli and multinomial in a complementary manner and discovers the path between source and destination by avoiding the types of attacks that causes Denial of Service. In [2], this paper has described the various techniques against the denial of service attack. In [3], introduces improvement over AMTT (Avoiding Mistaken Transmission Table). It not only identifies and distinguishes malicious node from the legal node but also reconsider it after giving adequate penalty. In [4], The reputation based system where, each node would evaluate nodes recommendation, route ID and packet drop ratio and hence detect the malicious node. In [5], A hybrid security approach by using AES (Advanced Encryption Standard with blowfish algorithm to verify the data. In [6], MCA-based (Multivariate Correlation Analysis) DoS attack detection which is powered by triangle area based MCA technique and the anomaly based technique these technique extracts the geometrical correlations hidden in individual pairs of two distinct features within each network traffic record and detect the unknown DOS attacks from the network is discussed. In [7], uses novel automatic security mechanism using Support Vector Machine (SVM) to defense against malicious attack occurring in AODV. In [8], introduces graph-based descriptor for the detection of anomalies in mobile networks, using billing-related information. The graph-based descriptor represents the total activity in the network. In [9], the DOS attack detection system which is equipped with the MCA (Multivariate Correlation Analysis) technique and EMD (Earth Mover's Distance) these techniques able to distinguish DoS attack from the legitimate network traffic. In [10], a method called MrDR and the acronym stems from its stages: monitoring, detection, and rehabilitation. These stages help in Detecting misbehaving nodes whether they are malicious or selfish. [11], author has proposed to mitigate inside and outside DoS attackers in VANETs using HMAC (Hash-based Message Authentication Code) signatures computed from private and public key pair are used for authenticating the communicating entity. In [12], the designed quorum-based frequency hopping (FH) algorithms that mitigate DoS attacks on the control channel of an asynchronous ad hoc network. In [13], proposed a method to mitigate the surface for DoS attacks. The method in the partitioning of memory lines within the main memory. In [14], introduces pre authentication process before signature verifying process to deal with the kind of DoS attack in VANETs. In [15], A scheme to mitigate the effects of DoS attacks in identity management (IdM) systems through the reorganizations of the system components.

3. PROPOSED WORK

The proposed method for detection and prevention of DoS attack uses OLSR routing protocol. Secure routing protocol is divided in two categories based on the safety method, i.e. cryptographic mechanism and trust based mechanism. We choose trust mechanism to secure the protocol because it has a better performance rather than cryptography method. Trust calculation is based on the behavior and activity information of each node. Trust value is divided in to Trust Global and Trust Local. Trust global is a trust calculation based on the total of received routing packets and the total of sending routing packets. Trust local is a comparison between total received packets and total forwarded packets by neighboring node from specific nodes. Nodes conclude the total trust level of its neighbors by accumulating the local and global values. When a node is suspected as an attacker, the protection mechanism will isolate it from the network before communication is established. Protection mechanism concentrate to cover an active attack such as DoS, Proposed mechanisms are only in the network layer and communication factor on the physical layer which can affect

the link quality are ignored. We just modify in the routing protocol mechanism. We evaluate the proposed solution using NS-2 in the ad hoc network topology.

3.1 Flow of Work

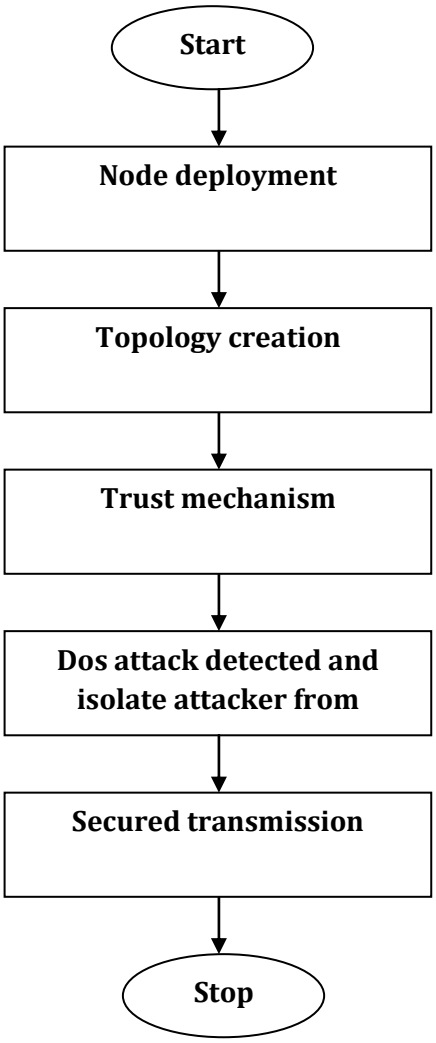

Fig-2 Data flow diagram

Algorithm 1: Detection and prevention of dos attack.

Step 1: Let N be the total number of nodes and x be the number of Denial of service nodes (DoS). Let S be the source node.

Step 2: Input values of N and x.

Step 3: Randomly assign x nodes as DoS nodes among N nodes.

Step4: Initially topology control (TC) and HELLO messages are passed and multi point relay (MPR) chosen by the nodes. MID (Multiple Interface Declaration) are transmitted by nodes to get address of each node.

Step5: The node selects the shortest distance between itself and one of the destinations node MPRs and hence the shortest path to the destination is found.

Step6: The MPR until the destination chosen may act as attacker by sending many HELLO messages. Based on the probability by HELLO message easily all nodes can detect attacker. Then the node is announced as attacker and the node details are sent to each node to eliminate that node.

Step7: The source node S forwards the packets to destination through the secured route.

Step8: Compute the performance metrics, namely, throughput, packet delivery ratio, packet received, delay, jitter, good put, normalized overheads, dropping ratio.

Step9: Stop

4. SIMULATION RESULTS AND DISCUSSION

The simulation experiments are conducted using NS-2 simulator by using the proposed mechanism. The performance analyzed in terms of packet received, packet drop ratio, delay, jitter, throughput, good put, normalized overheads, dropping ratio.

Packet received: It is the total number of packets received by the receiver at a given time. The Fig.3 Shows the packets received are more in case of proposed method and packets received are less with DoS attack.

Table-1 Simulation parameters

Parameters	Value
Packet size	2000 bytes
Simulator	NS-2
Transmission range	200mts
Node placement	Randomly
Number of DOS in percentage	1% ,2% ,3%, 4%, 5% of total nodes
Simulation runtime	80sec to 200sec
Number of mobile nodes	50 nodes
Topology	1000*1000(m)
Routing protocol	OLSR
Traffic	Constant Bit rate(CBR)

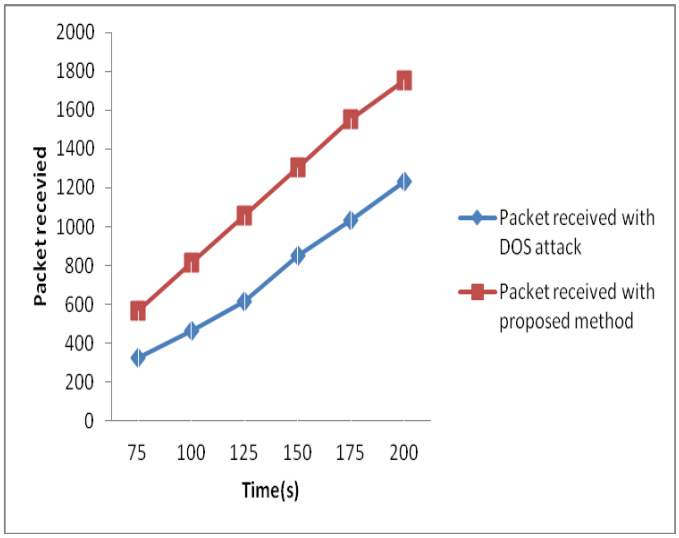

Fig.-3 Comparisons for packet received with DoS attack and with proposed method.

Packet delivery ratio: It is the ratio of total data packets received successfully at destination to the number of data packets generated at the source. The Fig.4 shows the packet delivery ratio is more with the proposed method than with DoS attack.

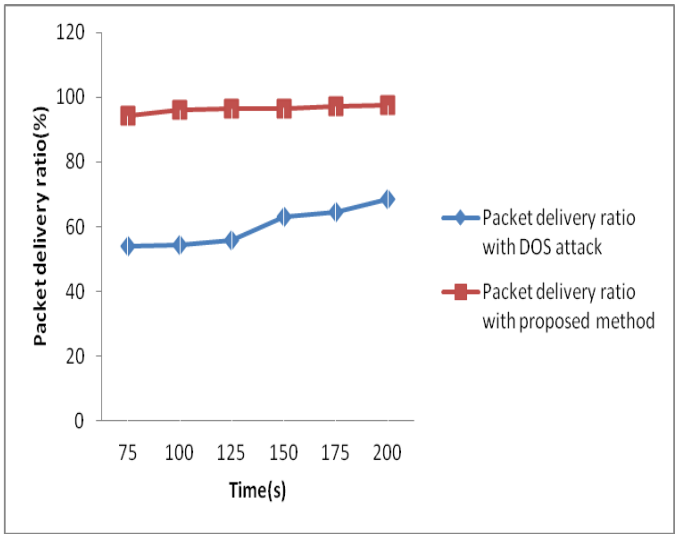

Fig-4 Comparisons for Packet delivery ratio with DoS attack and with proposed method.

Delay: It is the average time space between the generation of a packet at a source node and successful delivery of that packet at destination node. The Fig.5 shows the delay is less in the proposed method than with the DoS attack.

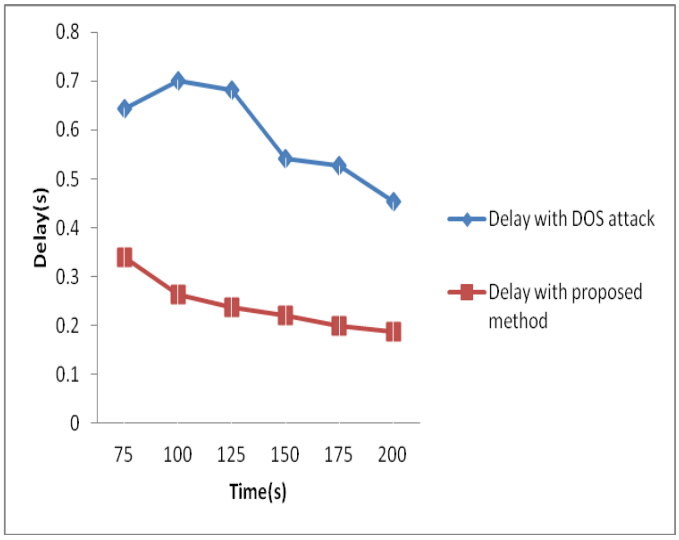

Fig-5 End –to-end delay with DoS attack and with proposed method.

Jitter: It is defined as variation in the delay of received packets. Fig.6 shows the jitter is less in case of proposed method than with the DoS attack.

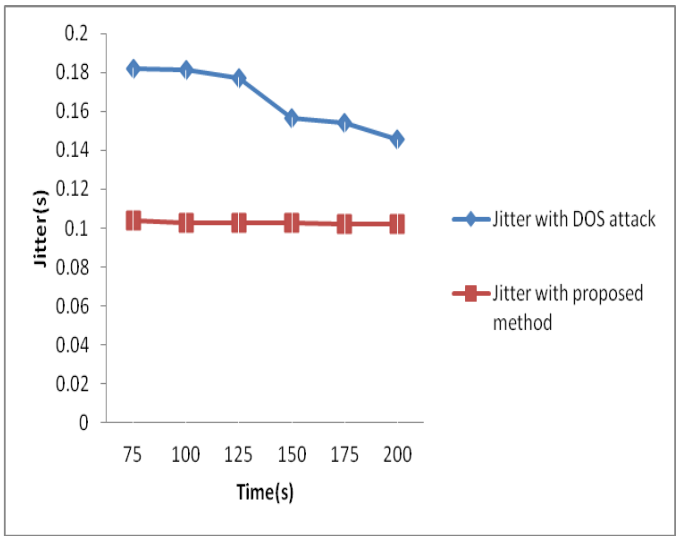

Fig-6 Comparison for jitter with DoS attack and with proposed method.

Throughput: It is the rate of successfully transmitted data packets per second in the network during the simulation. The Fig.7 shows the throughput is more with the proposed method than with the DOS attack.

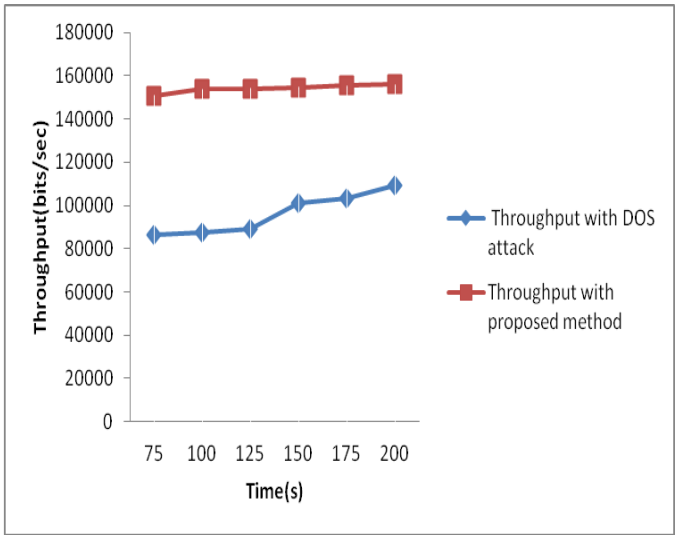

Fig-7 Comparison of throughput with DoS attack and with proposed method.

Good put: It is the number of useful information bits delivered by the network to a certain destination per unit of time. The Fig.8 Shows the good put is more with the proposed method.

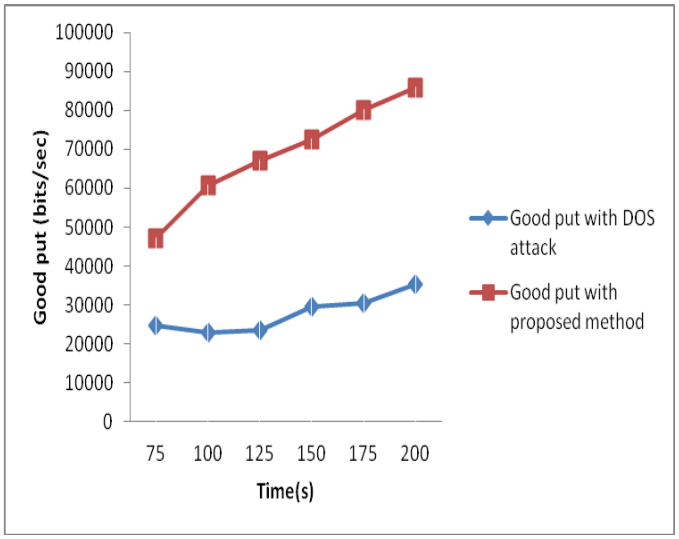

Fig-8 Comparison for good put with DoS attack and with proposed method.

Normalized over head: Any combination of excess or indirect computation time, memory, bandwidth, or other resources that are required to perform a specific task is termed as normalized overhead. The Fig.9 shows the overhead is less with proposed method.

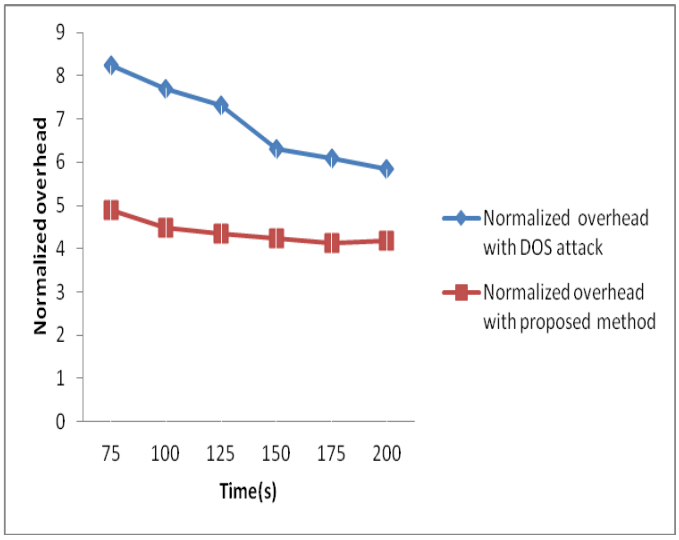

Fig-9 Network overhead with DoS attack and with proposed method.

Dropping ratio: It is defined as difference between total numbers of packets sent and total number of packets received The Fig.10 shows the dropping ratio is less with proposed method and it is more with DOS attack.

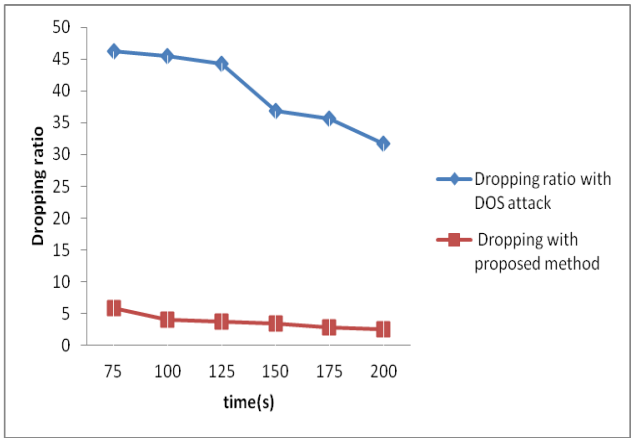

Fig-10 Comparison for dropping ratio with DoS attack and with proposed method.

Table-2 Comparison of Throughput obtained by varying simulation run time for 75sec, 100sec , 125sec, 150sec, 175sec , 200sec of N=50 nodes for proposed

Simulation run time	Throughput with DOS attack	Throughput with proposed method
75	86277.1	150918
100	87255.6	153781
125	89244.8	154177
150	101171	154663
175	103064	155497
200	109422	156000

Table-3 Comparison of E2E delay obtained by varying simulation runtime for 75sec, 100sec , 125sec, 150sec, 175sec , 200sec of N=50 nodes for the proposed method with DOS attack.

Simulation run time	E2E delay for DOS attack	E2E delay with proposed method
75	0.644441	0.33926
100	0.701514	0.263347
125	0.680581	0.238357
150	0.542163	0.220542
175	0.526206	0.199727
200	0.452469	0.186256

Table-4 Comparison of PDR (packet delivery ratio) obtained by varying simulation run time for 75sec, 100sec , 125sec, 150sec, 175sec , 200sec of N=50 nodes for proposed method with DOS attack.

Simulation run time	PDR for DOS attack	PDR for proposed method
75	53.8333	94.16
100	54.4706	96.00
125	55.7273	96.27
150	63.1852	96.59
175	64.375	97.12
200	68.3509	97.44

5. CONCLUSION AND FUTURE WORK

The routing protocols tend to be vulnerable to various attacks in MANETs. Hence a lot of security measures are required for secured use of MANETs. A novel method is focused on detection and prevention of Denial of Service attack in MANETs. The proposed trust based mechanism which is based on graph theory approach to secure the protocol because it has a better performance rather than cryptography method, by calculating the trust values of all neighboring nodes and hence detects and prevent the attacker and isolated it from the network. Among various detection and prevention techniques, proposed method is proved to be the best one for reducing the complexity. These results indicate that the proposed algorithm is more promising in effectively and competently detecting and preventing different types of attacks in MANETs.
Future work can be carried out by using different detection and prevention techniques for different types of attacks.

REFERENCES

[1] M. Rmayti, Y. Begriche, R. Khatoun, L.Khoukhi¤, D. Gaiti ICD,. "Denial of Service (DoS) attacks detection in MANETs using bayesian classifiers", 2014.

[2]. Yugandhara Patil, Ashok M Kanthe "Survey: Comparison of mechanisms against denial of service attack in Mobile Ad-Hoc Networks", 2015.

[3]. Sheetal Akhilesh Ahir, Nilesh Marathe , Puja Padiya . "IAMTT- New method for resisting network layer Denial of service attack on MANET", 2014, pp.762-766.

[4].S.B.Aneith Kumar, S.Allwin Devaraj, J. Arun kumar. "Efficient detection of denial of service attacks in MANET", Volume 2, Issue 5, May 2012, pp.470-475.

[5].Ajay Vikram Singh, Moushmi chattopadhyaya. "Mitigation of DoS attacks by Using multiple encryptions in MANETs", 2015.

[6]. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Senior Member, IEEE,
Priyadarsi Nanda, Member, IEEE, and Ren Ping Liu, Member, IEEE. "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", VOL. 25, NO. 2, february 2014.

[7]. Meenakshi Patel, Sanjay Sharma, "Detection of Malicious Attack in MANET A Behavioral Approach", 2012.

[8]. Stavros Papadopoulos, Anastasios Drosou, and Dimitrios Tzovaras, "A Novel Graph-Based Descriptor for the Detection of Billing-Related Anomalies in Cellular Mobile Networks", 2016.

[9]. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda,Ren Ping Liu, and Jiankun Hu. "Detection of Denial-of-Service Attacks Based on Computer Vision Techniques",VOL. 64, NO. 9, Sep 2015.

[10]. Albandari Alsumayt, John HaggertyJohn Haggerty, Ahmad Lotfi, " Performance, Analysis, and Comparison of MrDR Method to Detect DoS Attacks in MANET", 2015.

[11]. Pooja. B, Manohara Pai M.M, Radhika M Pai, Nabil Ajam, Joseph Mouzna. "Mitigation of Insider and Outsider DoS Attack against Signature Based Authentication in VANETs", 2014.

[12]. Mohammad J. Abdel-Rahman, Hanif Rahbari, and Marwan Krunz, Philippe Nain " Fast and Secure Rendezvous Protocols for Mitigating Control Channel DoS Attacks", 2013.

[13]. Pierre Schnarz_y, Clemens Fischer_y, Joachim Wietzke_, Ingo Stengel. "On a Domain Block Based Mechanism to Mitigate DoS Attacks on Shared Caches in Asymmetric Multiprocessing Multi Operating Systems", 2014.

[14]. Li He and Wen Tao Zhu, "Mitigating DoS Attacks against Signature-Based Authentication in VANETs", 2012.

[15]. Ricardo Macedo, Yacine Ghamri-Doudane and Michele Nogueira. "Mitigating DoS attacks in Identity Management Systems Through Reorganizations", 2015.