Recogniztion And Exclusion of Malicious Node By Using Clustering Technique In Mobile Ad Hoc Network

Shweta Khushwah[1], Neelam Joshi[2]
[2] Assistant Professor
[1, 2] MPCT College, M.P. India

Abstract- *MANET (Mobile Ad-hoc Network) is a popular and widely used wireless network. MANET is a kind of self-organizing and decentralized system. It is a network made up of various wireless mobile nodes which collectively work together so that transmission is feasible between any of the nodes in the system. Nodes communicate with each other with the direct shared wireless radio links. All the mobile hosts act as routers in the network. Due to open and dynamic nature, this network is quite prone to number of attacks. In existing work, they calculated two trusted nodes in the cluster on the basis of highest energy. Malicious node has also highest energy and selected as a trusted node and forward the data to other attacker and it affects the whole network. They find two nodes in cluster with highest energy and make them cluster head. This CH is only considered as trusted and all the communication had done by these CHs. When data has to transfer then CH send packet to another cloud's CHs only. In our proposed work, we are finding only one cluster head which is most trusted node in a cluster. So we are using transmission range with highest energy to calculated cluster head. They have to fulfill both the criteria to eliminate the selection of malicious node. Our results show that our work has performed on NS2 and we improved the network performance.*

Keywords- Mobile Ad hoc network, Trust, DDoS Attack and Routing Protocol.

I. INTRODUCTION

A MANET is a collection of independent mobile nodes that might talk to every different through radio waves. The mobile nodes which are in radio variety of every other can directly speak, while others need the resource of intermediate nodes to course their packets. Each of the nodes has a wireless interface to talk with each different. These networks are completely dispensed, and can work at any region without the help of any fixed infrastructure as access points or base stations.

Figure 1 indicates an easy ad-hoc networks with 3 nodes. Node 1 and node 3 are not inside variety of every different, but the node 2 can be used to ahead packets among node 1and node 2. The node 2 will act as a router and people 3 nodes collectively form an -hoc network [1].

WHAT IS TRUST?

The perception of trust is significant to communication and network protocol designers where establishing trust relationships among participating nodes is important to enabling collaborative optimization of gadget metrics [1], trust is described as "a fixed of relations amongst entities that participate in a protocol. These associations are based on the testimony engendered by the previous interactions of entities within a protocol. In broad, if the interactions have been realistic to the protocol, then trust will build up between these nodes." Trust is outlined because the degree of belief concerning the mien of different entities [2].

1.1 Trust Metrics

Trust is evaluated on different metrics and different ways. Some schemes use continuous or discrete values to measure the level of trust. For Example, trust is described by a continuous value in [0, 1] or measured as discrete cost. Threshold primarily based procedures are also used to measure the agree with. Trust metrics which includes fuzzy based, opportunity primarily based, similarity, mobility, context based factors like strength, signal electricity, hop distance etc.

1.2 Properties of Trust in MANET

A trust decision framework ought to not paintings under the idea that all nodes are cooperative for MANETs. Trust must be determined in a noticeably customizable way without excessive computation and communication load.

- Trust is not static, it is dynamic.

- Trust is subjective.
- Trust isn't always necessarily transitive.
- Trust is asymmetric and not basically reciproca
- Trust is depending on context

II. DOS ATTACK IN MANET

Distributed DOS attack commonly happens in MANETS or in wireless networks. It is an attack wherein a couple of structures include collectively and goal a single gadget inflicting a denial of service. A denial of service (DOS) is an attack with a purpose of preventing legitimate users from using a specified network resource such as website, web service or computer system. A DDOS attack is sent a large scale attempt by malicious customers to flood the sufferer network with a vast numbers of packets. DDOS consists as proven in Fig. First attacker builds a network of susceptible nodes which might be used to initiate the attack. The susceptible nodes referred to as handler and agents. These handler and agents are then installed with tools called attack tools, which allow the handler and agents to carry out attacks under the control of the attacker. The attacker motivates the handler to start the attack, the handler then motivate the agents. The agents flood the victim [3].

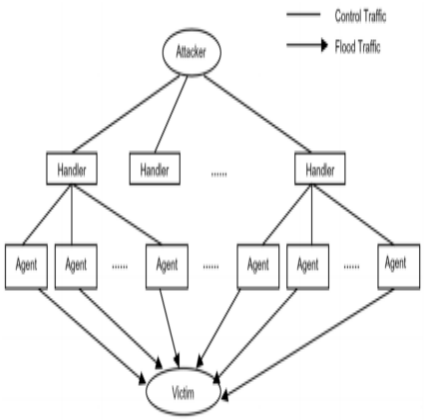

Fig -1: Architecture of DDos attack

III. LITERATURE SURVEY

Antesar M. Shabut et al. [2017] this paper investigates the troubles of data sparsity and cold start of recommender systems in current accept as true with fashions. It proposes a recommender gadget with clustering method to dynamically are seeking for similar suggestions primarily based on a certain time frame. Similarity among special nodes is evaluated based on essential attributes consists of use of interactions, compatibility of statistics and closeness among the mobile nodes. The recommender system is empirically tested and empirical evaluation demonstrates robustness in assuaging the issues of records sparsity and cold begin of recommender structures in dynamic MANET surroundings [4].

Sachi N. Shah et al.[2016] This paper proposed a new secure trust based routing scheme which is combination of social and QoS trust. The primary goal of our proposed scheme is to mitigate nodes performing various packet forwarding misbehaviors. We calculated four parameters for trust which are control forward ratio, data forward ratio, intimacy and residual energy. We present adversary model of the packet dropping attack against which our trust-based scheme is evaluated. Simulation effects in NS-2 show that the proposed scheme improves overall performance in phrases of PDR [5].

ShabinaParbin et al.[2016] In this paper, our proposed a trust and reputation management scheme for find out the trusted location in MANET environment. MANETs operates without fixed framework and all nodes in network perform like a router in sequence to forward information next receiver. Since the pivotal point rein lack, MANETs are additionally pregnable routing attacks as against various grids. Routing is one of the most serious attacks of wormhole attacks that are easier to be implemented nevertheless harder detection. Generally, it operates in two phases; in the first phase, wormhole channel nodes tend to draw more and more traffic route, and by other phase, they loss the grid by altering or dropping the grid traffic. In MANETs, numerous writers have implemented diverse results to prevent attacks [6].

RaihanaFerdous et al. [2016] In this setting, three routing protocols have been analyzed and compared: OLSR, DSR and AODV. The metrics are being used are Packet Delivery Ratio, Delay and Throughput. Network Simulator (NS2) has been used as tool for the experiments. The performance analysis of these protocols also compared for power usage using two trust-based models: Node based Trust Management (NTM) Scheme and TLEACH. Simulation results show that OLSR protocol performs well compared to AODV and DSR [7].

Shimmi Singh Rathour et al.[2016] In our proposed work we apply the trust method which calculates by dumpstersShafer theory, after trust calculation we apply support vector machine to classify nodes behavior on the basis of classification we find out malicious behavior of nodes. The simulation we have done on NS-2.35, with the help of these techniques we improve network efficiency in the form of packet delivery ratio or throughput [8].

Rupayan Das et al.[2016] This paper introduces an algorithm to design a Mobile Ad-hoc network (MANET) or Wireless Sensor Network (WSN) and compares the effect of different network and physical layer attacks (wormhole, black hole, jamming, byzantine) based totally on some QOS parameters in presence of AODV routing protocol. We simulate various attacks using the network simulator OPNET 14.5 and then analyze them in the basis of some quality of service parameters under AODV routing protocol [9].

Pradeep sing Tiwana et al.[2016] This paper is subjected to the connection of jellyfish reorder attack on zone routing protocol and without an assault on zone routing protocol with the growing number of nodes. The execution measurements are information total packets of data send over the network, number of received data packets, packets of distribution rate on network, thoroughpaced of network, standardized routing load. To probe the competence of this attack a meticulous simulative scrutiny is done under network simulator with and beyond jellyfish reorder attack [10].

Sunil Kumar Jangir et al.[2016] In this paper a methodical review is done on the recent state of the research results on wormhole attacks. The simulated results helps to quantify the comparative performances of the different solutions proposed. The various detection techniques and the types of wormhole modes like In-band Channel; High Power Transmission etc. are studied [11].

IV. PROPOSED WORK

MANET is a wireless network in which the nodes communicate through wireless medium. There are many attacks performed by the malicious nodes. Cluster is a method which is used to remove malicious node from the network. Trust value of the nodes is calculated and then cluster head is selected which is responsible for the secure transmission of data.

In existing work, they calculated two trusted nodes in the cluster on the basis of highest energy. Malicious node has also highest energy and selected as a trusted node. Then it can forward the data to other attacker and it affects the whole network. They find two nodes in cluster with highest energy and make them cluster head. This CH is only considered as trusted and all the communication had done by these CHs only. When data has to transfer then CH send packet to another cloud's CHs only. By this they eliminate the malicious nodes from the network and make path more secure.

In our proposed work, we are finding only one cluster head which is most trusted node in a cluster. So we are using transmission range with highest energy to calculated cluster head. They have to fulfill both the criteria to eliminate the selection of malicious node.

4.1 Proposed Algorithm

Step:1 Initialize network
Step:2 Find the neighbour nodes
Step:3 Compute the distance with all its neighbours

$$D = \Sigma\sqrt{((x2-x1)^2+(y2-y1)^2)}$$

Step:4 Form the cluster
Step:5 now find the cluster head of every cluster by calculating energy and transmission range of every node

The desired transmission range is calculated based on the desired node degree and the current node degree. The desired node degree is equal to the contention index incremented by one and contention index is the product of node density and the radius of cluster.

$d_d = ND + 1$
where, ND= nodedensity*D

step 4 The transmission range is thus calculated by using the formula of transmission range based clustering(TRBC)

$$Tr=\sqrt{((d_d/d_c)/clusterarea)}$$

Where, d_d is the desired node degree and d_c is the current node degree and the cluster area equals the area covered by the cluster.

Step 5 now which node is having higher energy and in the transmission range then it is taken as cluster head and considered as a trusted node.

V. RESULTS AND ANAYSIS

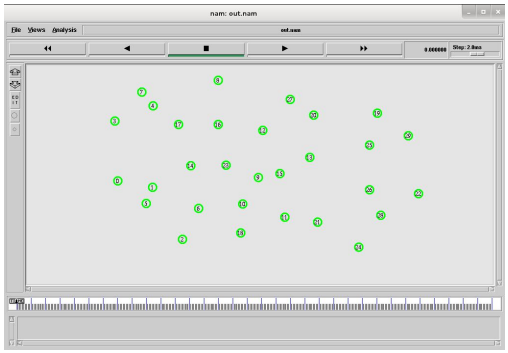

Fig -2 Initialization of network

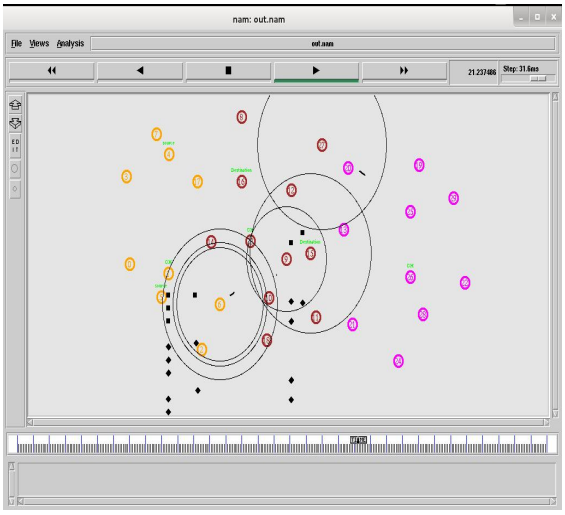

Fig -3: Communication among nodes

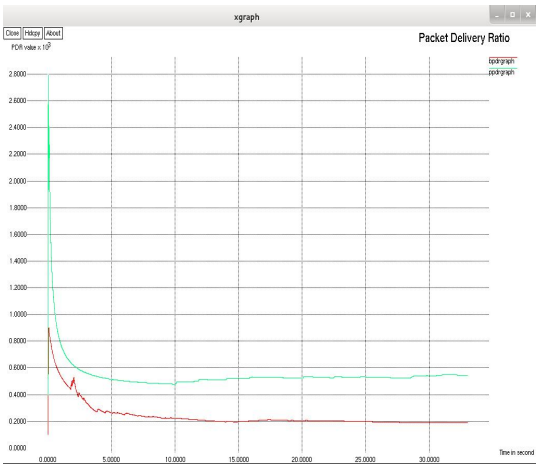

Fig -4: PDR Graph

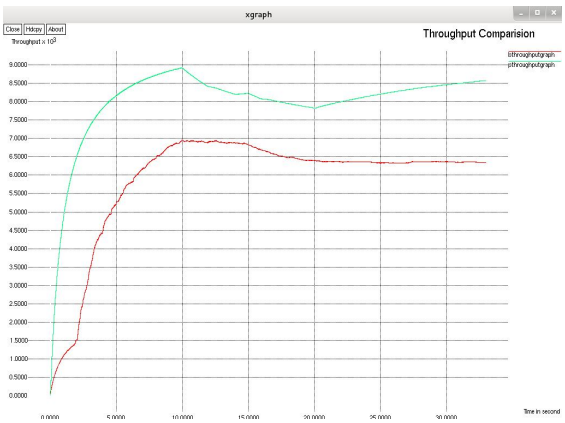

Fig -5: Throughput Graph

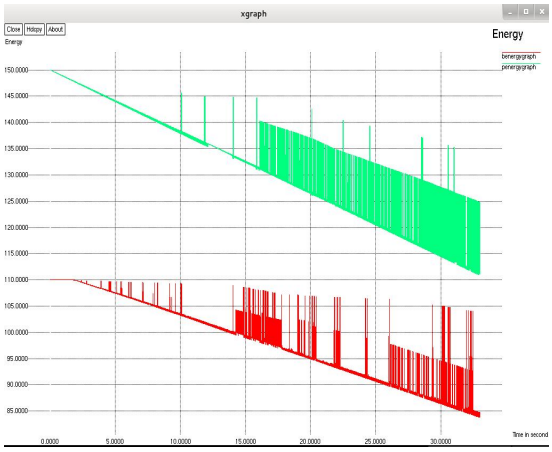

Fig -6: Energy Graph

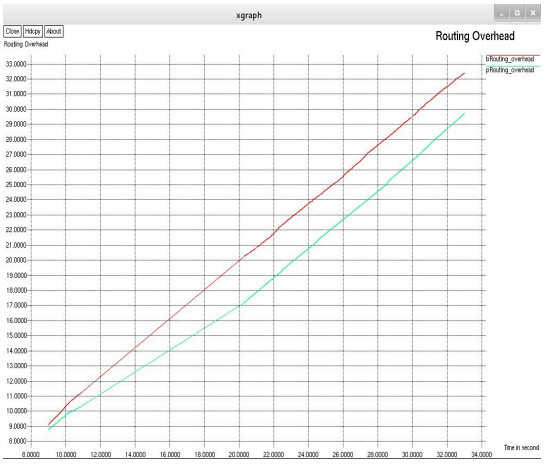

Fig -7: Routing Overhead Graph

VI. CONCLUSION

MANET is a wireless network in which the nodes communicate through wireless medium. There are many attacks performed by the malicious nodes. Cluster is a method which is used to remove malicious node from the network. Trust value of the nodes is calculated and then cluster head is selected which is responsible for the secure transmission of data. Cluster formation is mainly done to select trusted nodes in the area which can be used to forward the packets to other cluster head. We performed this procedure to improve the security of the network and enhance the network performance.

REFERENCES

[1] Aarti, Dr. S. S. Tyagi "Study of MANET: Characteristics, Challenges, Application and Security Attacks" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, ISSN: 2277 128X.

[2] Vijayan R, Jeyanthi N. "A Survey of Trust Management in Mobile Ad hoc Networks" International Journal of

Applied Engineering Research ISSN 0973-4562 Volume 11, Number 4 (2016) pp 2833-2838.

[3] Shakti Arora, Arushi Bansal "Survey on Prevention Methods for DDOS Attacks in MANETS" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014 ISSN: 2277 128X.

[4] Antesar M. Shabut, Keshav Dahal "Social Factors for Data Sparsity Problem of Trust Models in MANETs" 978-1-5090-4588-4/17/$31.00 ©2017 IEEE, 2017 Workshop on Computing, Networking and Communications (CNC).

[5] Sachi N. Shah, Rutvij H. Jhaveri "A Trust-Based Scheme against Packet Dropping Attacks in MANETs" 978-1-5090-2399-8/16/$31.00 c 2016 IEEE.

[6] Shabina Parbin, Leeladhar Mahor "Analysis and Prevention of Wormhole Attack Using Trust And Reputation Management Scheme in MANET" 978-1-5090-2399-8/16/$31.00 c 2016 IEEE.

[7] Raihana Ferdous, Vallipuram Muthukkumarasamy "A Comparative Performance Analysis of MANETs Routing Protocols in Trust-based models" 2016 International Conference on Computational Science and Computational Intelligence, 978-1-5090-5510-4/16 $31.00 © 2016 IEEE.

[8] Shimmi Singh Rathour, Nitin Manjhi "Trust Base Hybrid Approach for detection and Prevention MANET from Attacks" 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology (IIT).

[9] Rupayan Das, Sauvik Bal, Soumajit Das, Mrinal Kanti Sarkar, Debdeep Majumder, Anirban Chakraborty and Koushik Majumder, "PERFORMANCE ANALYSIS OF VARIOUS ATTACKS UNDER AODV IN WSN & MANET USING OPNET 14.5" 978-1-5090-1496-5/16/$31.00 © 2016 IEEE.

[10] Pradeep sing Tiwana, Nafiza mann "Jellyfish Reorder Attack on Hybrid Protocol in Mnaet Dissection on Variegated Parameters"2016 IEEE.

[11] Sunil Kumar Jangir, Naveen Hemrajani "A Comprehensive Review On Detection Of Wormhole Attack In MANET" 978-1-5090-5515-9/16/$31.00 ©2016 IEEE.