Reduction of Malicious Nodes using RTT & Clustering in Mobile Ad Hoc Network

Rammurti Gupta[1] Akhilesh Bansiya[2]
[2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Vedica Institute of Technology, Bhopal, India

Abstract— Mobile Ad-hoc Network (MANET) is an unpredictable network, the nodes are in the variable state. The node can effortlessly enter and exit from the network. It is a group of autonomous systems which is independent of infrastructure and hence it decreases the cost and deployment time. In the existing work, they used fuzzy logic which decides the rules for the trust evaluation of the nodes. Rules should be defined previously which is difficult to manage for the unknown variables. This method is not suitable for the dynamic nature of the network. So we applied better technique which generates the more trustful network. In our proposed work, trust is calculated by sending the Route Request (RREQ) packets to the network then the destination node send Route Reply (RREP) packet. Calculate RTT for distance between the sender and destination nodes. We select the path by taking the shortest RTT and then form clusters. Calculate the energy of each node in cluster and select cluster head of maximum energy. Cluster head forward the data from source to destination. This method removes the chance of malicious node from the network.

Key words: Mobile Ad Hoc Network, Intrusion Detection System, NIDS, HIDS, Trust

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a gathering of wirelessly mobility nodes forming a transitory network deprived of any established substructure. The nodes are autonomously to move and establish themselves into a network. MANET doesn't necessitate any static substructure e.g. base stations; so, it's a good networking excellent for connecting mobility devices spontaneously and rapidly. The below figure demonstration a MANET [1]

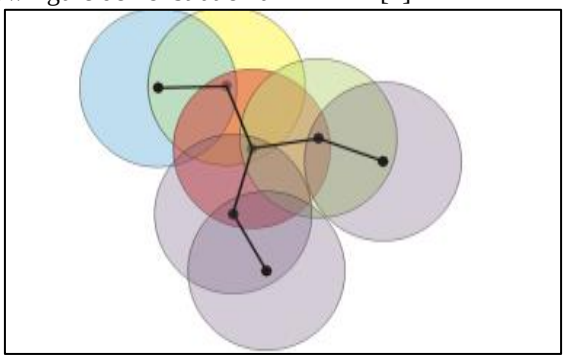

Fig. 1: MANET

II. INTRUSION DETECTION SYSTEM (IDS)

IDS can be well-defined as the protector system which self-detects malicious activities within a network, and thus generates an alarm to alert the security device at a locality if intrusions are considered to be illegal on that network or host. There me many approach to classify IDS. In several IDS implementation, many classes are group in a sole device. Particularly, we define two main IDS taxonomy. First category is depending on the IDS method of and analysis strategy, which have two main types and one hybrid model. These three general groups of IDS may also be utilized on network-based and host-based IDS systems.

1) Anomaly-Based Detection
2) Signature-Based Detection (Misuse Detection)
3) Specification-Based Detection hybrid Detection)

Second group is depending on data collection monitoring and mechanism activity, either on multiple-host or on sole-host within network:

1) Network-based IDS (NIDS)
2) Host-based IDS (HIDS)

Commonly, NIDS utilizes Signature-based detection and HIDS utilizes Anomaly-based detection. All method has its weaknesses and strengths; each is complanurtary to another. Successful IDS will employ both technologies (HIDS and NIDS). We equate HIDS and NIDS in case of their weaknesses and strengths to show how the two can work together to give further effective IDs and protection [2].

III. TRUST

Trust is normally accomplished by indirect trust mechanisms with agencies servers and trusted certification authentication in wired networks. However, to establishing the indirect trust mechanism necessitates certain mechanism for start authentication and is usually behave with physical or locality-depend authentication schemes. Trust founding in MANET is still a uncover and challenging area. The MANET behavior is depending on trust your neighbor relationships. These relationships initiate, develop and terminate dynamically and have usually short life spans. The trust relationships are extremely sensitive to attacks in such network. There are several of reasons that some nodes in such network can easily mould these relationships to grab required information. For a total of area, comprising better service, selfishness, malicious intent, and some nodes can easily mould these relationships to extract desired objectives. Moreover, the fixed trust substructure absence, availability, shared wirelessly physical and medium vulnerability, ephemeral connectivity, create trust establishment virtually impossible. To overcome these difficulties, trust has been recognized in MANET utilizing a no. of suppositions comprising pre-formation nodes with secret keys, or an omnipresent essential trust authority occurrence. In our view, these suppositions are against the very MANET nature that are assume to be spontaneous and improvised [3].

IV. IDS IN MANET

IDS serve as an alarm mechanism. It detects the security of compromises happened to a PC and then difficulties alarm message to an object. An ID contains an audit data collection agent, which keep track of the activities within the system, a detector which analyzes the review data and matters an o/p report to the site security officer. IDS in MANET, two ideas necessity to be distinguished: IDs methods and IDs architecture. IDs methods mention to the thought for instance misuse and anomaly detection. They generally solve the issue like, how an ID detects an intrusion with a few algorithms, given few audit data as input data. The IDs architecture deals with difficulties in a bigger scope. IDs architecture necessity to employ some IDs methods as a module. But it also comprises several another modules, for instance a module on how the nodes in a network can collaborate in decision making regarding intrusion detection. In wired network, a node can typically create IDs decision depend on the data gather locally. So, an IDs method can meet the essential for IDs once it is diffuse on a node. In wireless network, however, it is very difficult for a node to make decision just based on data collected locally. Nodes must exchange or collaborate data at smallest in creating an intrusion detection decision. Therefore, an architecture to define the roles of different nodes and the way they communicate is very significant in wireless IDS. The IDs method is basically independent from the architecture or environment. In other words, anomaly and misuse detection can be exploited in wirelessly atmosphere just as they are in wired network. The difference in implementation is mostly on what audit data to take as input to the algorithm. Still, mostly IDS exploit anomaly detection because of the usual nature of in MANET. The analyses focus on dissimilar architectures of IDS in MANET, rather than dissimilar detection methods. Many literatures do not describe the detection methods utilized in detail. Certain even just states which the architecture can exploit both anomaly and misuse detection methods. Therefore, focuses on the different architectures of IDS, rather than the detection techniques that the architectures use. Attacks in MANET and the security task of IDS in MANET. Then, the requirements for IDS in MANET are identified. Finally, the likely IDS architectures in MANET are analyzed [1].

V. LITERATURE SURVEY

Antesar M. Shabut et al. [2017] this paper examines the sparsity of data problems and cold starts of recommender systems in current trust models. It defines a recommender system with clustering approach to dynamically seek like recommendations based on a certain timeframe. Similarity amid dissimilar nodes is evaluated depend on significant attributes comprises utilize of interactions, compatibility of info and closeness amid the mobile nodes. The recommender system is empirical analysis and empirically tested demonstrations robustness in easing the sparsity of data problems and cold initial of recommender systems in a dynamic MANET environment [4].

Jeronymo M. A. Carvalho, et al [2016] this paper, proposes to achieve this ability by applying a grouping of different techniques to the design of a Collaborative MANET IDS. The system enhances the mobile network security using a secondary network of sensors, multilateration, predictive location algorithm, and information sharing protocol. To illustrate the concept, they established a military tactical scenario simulation using three distinct software tools [5].

Andrea Lupia, et al. [2016] in this paper, the dynamic watching could aid in saving energy with no affecting the IDS accuracy. They introduced a function that changes the monitoring probability a packet depending on the honesty of the comprise agent. The outcomes of this work illustration that the detection accuracy can be unaltered under some conditions, improving the energy saving [6].

Mr. P.Ramkumar et al. [2016] in this paper, a system is defining to detect the misbehaving node in a homogeneous along with a heterogeneous atmosphere. In such networks, to monitor the nodes behavior over an extensive atmosphere it is define to realize IDS with only a sole monitor node to be elected. This node will monitor the functions of all nodes in the whole network. If there is any disruption in the usual behavior of a communication channel then the monitor node will identify the node, which is a malicious node [7].

Raihana Ferdous et al. [2016] in this paper, three routing protocols have been compared and analyzed DSR, AODV and OLSR. The metrics are being used are PDR, Delay and Throughput. Network Simulator (NS2) has been utilized as tool for the experiments. The performance analysis of these protocols also compared for power usage using two trust-based models: Node depend Trust Management (NTM) Scheme and TLEACH. Simulation results show that OLSR protocol performs well compared to AODV and DSR [8].

ShimmiS singh Rathour, et al. [2016] in this paper, our proposed work we apply the trust method which calculates by dempsters shafer theory, after trust calculation we apply SVM to classify nodes behavior on the basis of classification we discover 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 PDR or throughput [9].

Pradnya M. Nanaware et al. [2016] The paper gives solution for malicious nodes detection from the network depending on the trust of the node. In this paper, various parameters are considered to recognize the maliciousness. The parameters comprise the energy of node, the mobility nodes and two social parameters. The detection is depending on the trust value for the particular node [10].

V. Sesha Bhargavi et al. [2016] this paper, focuses on a new hybrid secure routing protocol S-DSR that establishes a secure communication path across the nodes in the network which can improve the throughput and PDR etc. This protocol helps in discovery the best path for secure file transmission depend on the trust information from the neighboring nodes. This protocol attains better PDR and reduced delay when compared with protocols like AODV, AOMDV etc [11].

Ningrinla Marchang, et al. [2016] in this paper, they define is to lessen the active time duration of the IDSs without compromising on their efficiency. To validate our define method they replica the interactions amid IDSs as a multi-player cooperative game in that the players have

partially conflicting and partially cooperative objectives. They theoretically analyze this game and support it with simulation outcomes [12].

VI. PROBLEM STATEMENT

In the existing work, they used fuzzy logic which decides the rules for the trust evaluation of the nodes. Rules should be defined previously which is difficult to manage for the unknown variables. This method is not suitable for the dynamic nature of the network. So we applied better technique which generates the more trustful network.

VII. PROPOSED WORK

In our proposed work, trust is calculated by sending the Route Request (RREQ) packets to the network then the destination node send Route Reply (RREP) packet. Now we calculate RTT (Round Trip Time) for calculating the distance between the sender and destination nodes. We select the path by taking the shortest RTT and then form clusters. Calculate the energy of each node in cluster and select cluster head of maximum energy. Cluster head forward the data from source to destination. This method removes the chance of malicious node from the network.

A. Proposed algorithm

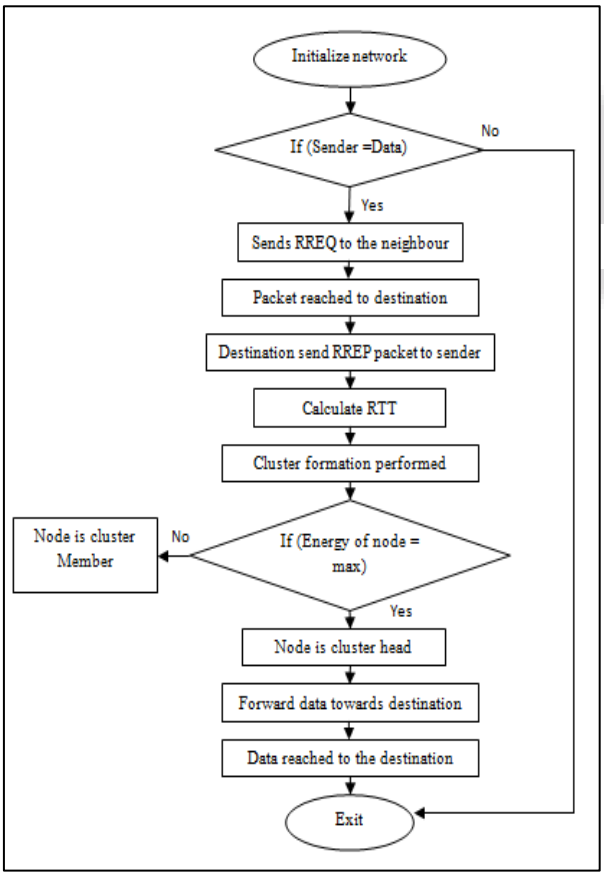

Fig. 2: Flowchart of Proposed Work

- Initialize network
- If sender has data
- Then it sends RREQ to the neighbour nodes
- Else
- Exit
- Packet reached to destination through all routes
- Now destination node send RREP packet to sender
- Calculate RTT for distance between sender and receiver
- RTT = Outgoing trip time + Incoming trip time
- Cluster formation performed
- If (Energy of node = max)
- Node is cluster head
- Else
- Cluster member
- Forward data from cluster heads towards destination
- Data reached to the destination from trusted nodes
- Exit

VIII. RESULT ANALYSIS

A. NAM:

Nam is a Tcl/TK based animation tool for performing network simulation traces and valid packet traces of world.

B. Xgraph

The xgraph program draws a graph on an X show given data examine from either data files or from standard input if no files are specified.

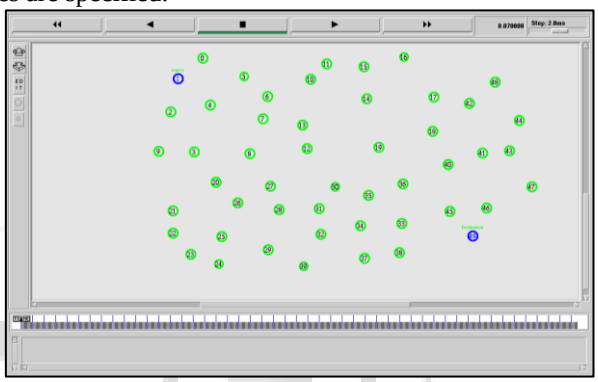

Fig. 3: Initialization of Nodes with source and destination

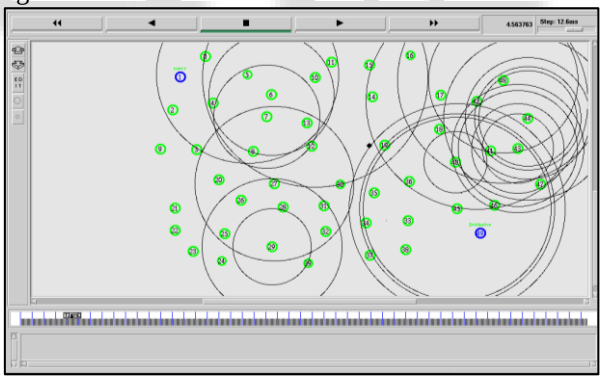

Fig. 4: Communication Starts

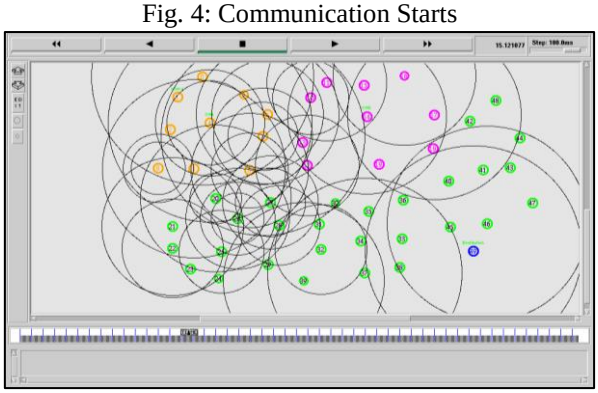

Fig. 5: Nodes communicate after forming clusters

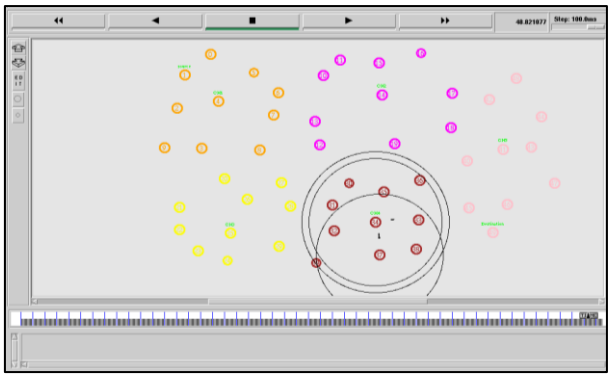

Fig. 6: Communicate till data reached to destination

C. Xgraph:

Results in graphical form:

1) Packet Delivery Ratio:

It defines as the fraction of packets deliver from source in the direction of destination. The graph represents a PDR graph among base approach as well as proposed approach. This PDR value is enhanced in proposed than an existing approach.

Packet Delivery Ratio = Number of packet received / number of packets sent

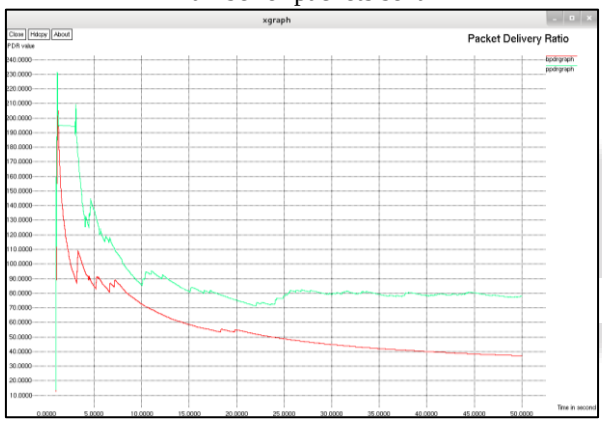

Fig. 6: PDR Graph

2) Throughput:

The transmitting of data lying on bandwidth is call as throughput. The graph signifies a throughput graph among base approach as well as proposed approach. The throughput of the proposed approach is fine than the presented approach.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

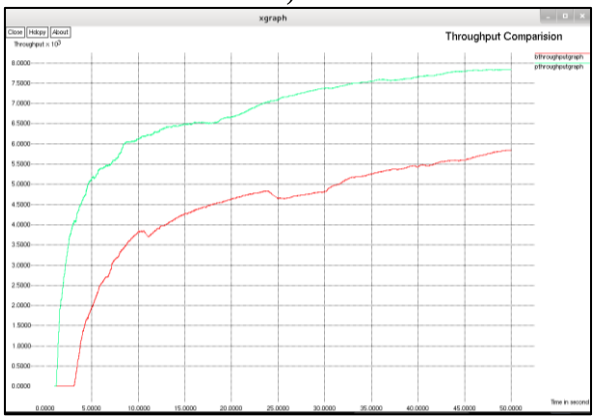

Fig. 7: Throughput Graph

3) Energy:

Determine of the ability of a system to change. Initial energy (Transmitting) and Energy loss (Receiving) remaining Residual.

Energy = Initial Energy / Number of node in Route or Remaining Energy

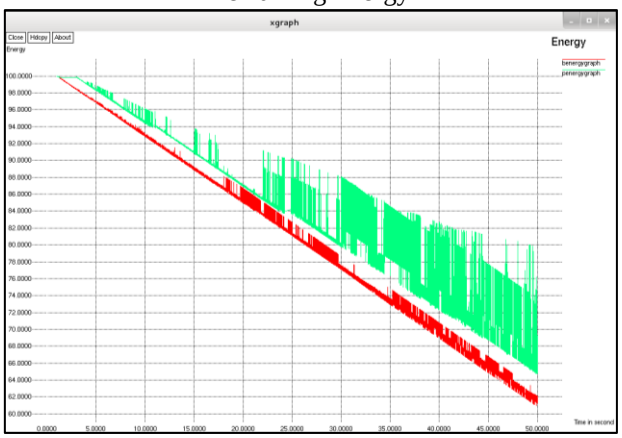

Fig. 8: Energy Graph

4) Routing overhead:

It is defined as the flooding of information in the network transmitted by application, which utilize a bit of easy to get to transfer rate of communication protocols. The graph represents a routing overhead graph among base approach as well as proposed approach. The proposed approach has an extra overhead than the base approach. Since the overhead be supposed to be minimum except as the routing enhances in the proposed work the overhead also increases.

Routing overhead = Number of packets control in particular time.

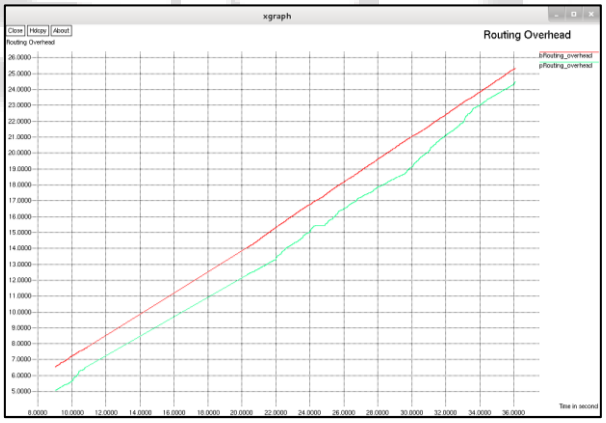

Fig. 9: Routing overhead Graph

IX. Conclusion

Mobile ad hoc network is a network which contains many malicious nodes which affects the performance of network. Trust is the main components of the network which is useful for eliminating the nodes which are selfish and malicious behaviour. Behaviour can be negative and positive in terms of packets forwarding and dropping. Round Trip Time is the total time between the sender and receiver for the transmission of the data from the source to destination and then from the destination to the source. We improved the security of the network which can be seen in the form of throughput, packet delivery ratio and routing overhead. In future work, we can perform authentication and confidentiality together to achieve more security in the

network. Hybrid techniques can be used to encrypt and encrypt the data to protect it from the attackers.

REFERENCES

[1] Arun Kumar. R, Abhishek M. K, Tejashwini. A. I, Niranjan J. T, Pradeep R.P "A Review on Intrusion Detection Systems in MANET" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.
[2] Bahareh Pahlevanzadeh and Azman Samsudin "Distributed Hierarchical IDS for MANET over AODV+" Proceedings of the 2007 IEEE Intemational Confbrence on Telecommunications and Malaysia International conference on communications, I 4-17 May 2007, penang, Malaysia.
[3] Nimitr Suanmali , Kamalrulnizam Abu Bakar "Trust Model in MANET : An Overview" '04, Month 1–2, 2004.
[4] Antesar M. Shabut , Keshav Dahal "Social Factors for Data Sparsity Problem of Trust Models in MANETs" 2017 Workshop on Computing, Networking and Communications (CNC), 978-1-5090-4588-4/17/$31.00 ©2017 IEEE.
[5] Jeronymo M. A. Carvalho, Paulo C. G. Costa "Collaborative Approach for a MANET Intrusion Detection System using Multilateration" 978-1-5090-3267-9/16/$31.00 ©2016 IEEE.
[6] [6]Andrea Lupia, Salvatore Marano "A Dynamic Monitoring for Energy Consumption Reduction of a Trust-Based Intrusion Detection System in Mobile Ad-hoc Networks" 2016 IEEE.
[7] Mr. P.Ramkumar , Ms.V.Vimala and Ms.G.Sivakama Sundari "HOMOGENEOUS AND HETROGENEOUS INTRUSION DETECTION SYSTEM IN MOBILE AD HOC NETWORKS" 2016 IEEE.
[8] Raihana Ferdous, Vallipuram Muthukkumarasam "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.
[9] ShimmiS ingh Rathour,Nitin Manjhi "Trust Base Hybrid Approach for detection and Prevention MANET from Attacks" 978-1-5090-2080-5/16/$31.00 ©2016 IEEE.
[10] Pradnya M. Nanaware , Dr. Sachin D. Babar "Trust System Based Intrusion Detection In Mobile Ad-hoc Network (MANET)" 2016 International Conference on Next Generation Intelligent Systems (ICNGIS), 78-1-5090-0870-4/16/$31.00 ©2016 IEEE.
[11] V. Sesha Bhargavi Dr. M.Seetha S.Viswanadharaju "A Trust Based Secure Routing Scheme for MANETS" 978-1-4673-8203-8/16/$31.00 c 2016 IEEE.
[12] Ningrinla Marchang, Member, IEEE, Raja Datta, Senior Member, IEEE, and Sajal K. Das, Fellow, IEEE "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. XX, NO. XX, XXX 2015.

