Security Enhancement using Trust Management in MANETs

Ms.S.Shalini[1]
1PG Scholar,
Hindusthan College of Engineering
and Technology, Coimbatore, India.
shalinishalu352@gmail.com

Mrs.T.Manjula[2]
2Assistant Professor (EEE),
Hindusthan College of Engineering
and Technology, Coimbatore, India.
manjulavijaykumar83@gmail.com

Mr.B.Anand[3]
3Associate Professor (EEE),
Hindusthan College of Engineering
and Technology,Coimbatore, India.
b_anand_eee@yahoo.com

Abstract— The distinctive options of mobile ad hoc networks (MANETs), victimization recent advances in unsure reasoning originated from AI community, we tend to projected a unified trust management schemes Mobile Ad-hoc networks area unit self-organizing and self re-configuring multi hop wireless networks wherever, the structure of the network changes dynamically the safety of the OLSR protocol is rib by a selected variety of attack known as 'Black Hole' attack. During this attack a malicious node advertises itself as having the shortest path to the destination node. To combat with region attack, it\'s projected to attend and check the replies from all the neighboring nodes to search out a secure route with protection to our data, however this approach suffers from high delay. Associate in Nursing approach is projected to combat the region attack by victimization Trust management schemes with neighbors WHO claim to possess a route to destination. during this project we tend to area unit victimization NS2.34 software system for our projected model testing. and that we got the simplest result against the safety attack.

Index Terms— Mobile ad hoc networks, Attack, Direct and Indirect observation, Trust Management.

1 INTRODUCTION

Ad-hoc networks area unit wireless networks wherever nodes communicate with one another victimization multi-hop links. there's no stationary infrastructure or base station for communication. Every node itself acts as a router for forwarding and receiving packets to/from different nodes. AN ad-hoc network may be a assortment of wireless mobile hosts forming a short lived network while not the help of any complete infrastructure or centralized administration.

Mobile Ad-hoc networks area unit self-organizing and self-configuring multi hop wireless networks wherever, the structure of the network changes dynamically. this can be principally as a result of the quality of the nodes. Nodes in these networks utilize identical random access wireless channel, cooperating in a very friendly manner to partaking themselves in multi hop forwarding. The nodes within the network not solely act as hosts however additionally as routers that route information to/from different nodes in network.

Where there's no infrastructure support as is that the case with wireless networks, and since a destination node could be out of vary of a supply node transmittal packets; a routine procedure is often required to seek out a path therefore on forward the packets fitly between the supply and therefore the destination. at intervals a cell, a base station will reach all mobile nodes while not routing via broadcast in common wireless networks.

In the case of ad-hoc networks, every node should be able to forward knowledge for alternative nodes. This creates further issues in conjunction with the issues of dynamic topology that is unpredictable property changes. Security is that the main issue in MANETs, simple to attack mobile nodes in Edouard.

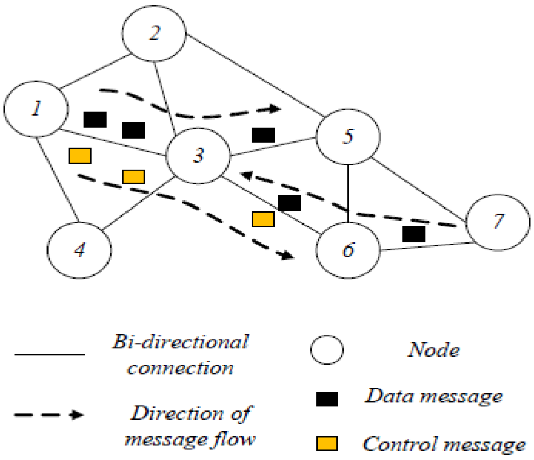

Fig .1 An Example of MANET

The security of the OLSR with changed DSR protocol is rib by a selected sort of attack known as 'Black Hole' attack. in a very part attack, a malicious node sends faux routing info, claiming that it\'s associate optimum route and causes different smart nodes to route knowledge packets through the malicious one. as an example in OLSR with changed DSR, the aggressor will send a faux RREP (including a faux destination sequence range that's made-up to be equal or on top of the one contained within the RREQ) to the supply node, claiming that it's a sufficiently recent route to the destination node.

This causes the supply node to pick the route that passes through the aggressor. Therefore, all traffic are routed through the aggressor, and thus, the aggressor will misuse or discard the traffic The route Confirmation Request (CREQ) and route Confirmation Reply (CREP) is introduced in to avoid the part attack. during this approach, the intermediate node not solely sends RREPs to the supply node however additionally sends CREQs to its next-hop node toward the destination node. once receiving a CREQ, the next-hop node appearance up its cache for a route to the destination.

The security of the OLSR with changed DSR protocol is rib by a specific style of attack known as If it\'s the route, it sends the CREP to the supply. Upon receiving the CREP, the supply node will make sure the validity of the trail by comparison the trail in RREP and therefore the one in CREP. If each area unit matched, the supply node judges that the route is correct. One downside of this approach is that it cannot avoid the region attack during which 2 consecutive nodes add collusion that\'s once ensuing hop node may be a colluding aggressor causing CREPs that support the inaccurate path.

The researchers planned an answer that needs a supply node to attend till a RREP packet arrives from >2 nodes. Upon receiving multiple RREPs, the supply node checks whether or not there\'s a shared hop or not. If there\'s the supply node judges that the route is safe. the most recoil of this answer is that it introduces time delay as a result of it should wait till multiple RREPs arrive.

In another try, the researchers analyzed the region attack and showed that a malicious node should increase the destination sequence variety sufficiently to convert the supply node that the route provided is sufficiently enough.

2 Proposed Method And Simulation

2.1 Trust Management In Manet

The trust-based data routing has been extensively studied in wireless networks including MANETs. The basic framework of a Trust Management System (TMS) includes a Reputation System (RS). Generally, the RS consists of reputation updating through direct observation(that is,first-hand information), reputation integration based on the indirect information from other members (i.e., second-hand information), and reputation aging in multiple feedbacks are compressed together. But using mobile agents for this purpose (which can already be deployed for functions like service discovery, clustering MANET etc.) will yield far better results as mobile agents are designed in such a way that they can easily cope with frequent disconnections and limited bandwidth characterizing MANET especially delay tolerant networks.

2.2 Trust In Mobile Agent Based Systems

In a distributed reputation management model is proposed that is based on Dempster-Shafer theory of evidence mobile agent based reputation management system has been proposed for ebusiness environments. The system uses direct interactions and feedback from customers in a social network using agents, where each customer models trustworthiness of a vendor

Thus, securing mobile agents and nodes in MANET by using the notion of trust is a comparatively new research paradigm. More importantly, assumption of a trusted third party or a trusted server and with 100% availability is practically not feasible in MANET. So the approaches based on a fully trusted node renders useless in resource constrained dynamic environments like MANET. Although some works have been done to detect blackhole attack or even wormhole attack in MANET but we did not come across any work that studies its effect on agents in MANET or uses the agents to detect such traps.

2.3 Trust Evaluation Algorithm

The distinctive features of mobile ad hoc networks (MANETs), including dynamic topology and open wireless medium, may lead MANETs suffering from many security vulnerabilities .the trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation, also called secondhand information that is obtained from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer theory, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method. Combining these two components in the trust model, we can obtain more accurate trust values of the observed nodes in MANETs as shown in the algorithm in Fig. 1.
Mobility management is closely related to multiple layers of network protocols, so developing multi-layer mobility management schemes. Power management: Power management aims to control connectivity, interference, spectrum spatial- reuse, and topology. Network monitoring: Several research issues exist in network monitoring.

2.4 Components Of Trust Model

The trust model has two components they are trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation, also called secondhand information that is obtained from neighbor nodes of the observer node, the trust value is derived using the Dempster-Shafer theory, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method. Combining these two components in the trust model, we can obtain more accurate trust values of the observed nodes in MANETs.

2.5 Dempster-Shafer Theory

The Dempster-Shafer theory, also known as the theory of belief functions, is a generalization of the Bayesian theory of subjective probability. Whereas the Bayesian theory requires probabilities for each question of interest, belief functions allow us to base degrees of belief for one question on probabilities for a related question. These degrees of belief may or may not have the mathematical properties of probabilities.

The Dempster-Shafer theory owes its name to work by A. P. Dempster (1968) and Glenn Shafer (1976), but the kind of reasoning the theory uses can be found as far back as the seventeenth century. The theory came to the attention of AI researchers in the early 1980s, when they were trying to adapt probability theory to expert systems.The Dempster-Shafer theory is based on two ideas: the idea of obtaining degrees of belief for one question from subjective probabilities for a related question, and Dempster's rule for combining such degrees of belief when they are based on independent items of evidence.

2.6 Bayesian Networks Interface

Bayesian networks model knowledge about propositions in uncertain domains using graphical and numerical representations. At the qualitative level, a Bayesian network is a directed acyclic graph where nodes represent variables and the graph represents conditional independence relations among the variables, in a sense to be described shortly.At the numerical level, a Bayesian network consists of a factorization of a joint probability distribution into a set of conditional distributions, one for each variable in the network. Additional knowledge in the form of likelihood functions can be used to update the joint probability distribution.

3 OUTPUT

We evaluate the planned theme in an exceedingly Edouard Manet routing protocol, the optimized link state routing protocol version a pair of (OLSRv2) , with the Qualnet machine. Intensive simulation results show the effectiveness of the planned theme. Turnout and packet delivery quantitative relation is improved considerably, with slightly inflated average end-to-end delay and overhead of messages.

3.1 Output Image

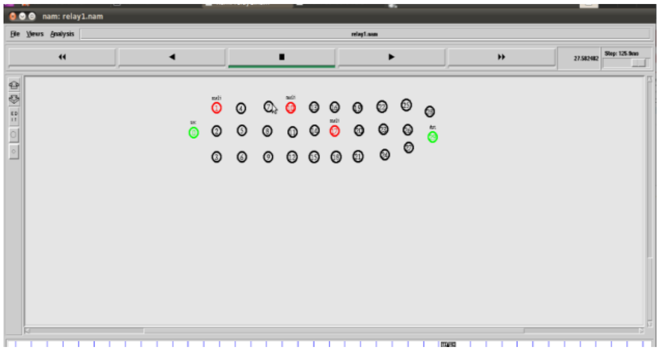

Fig.2 Direct Method

Collection of neighbors’ opinions will facilitate in justifying whether or not or not a node is hostile. This mechanism might scale back the bias from an observer. A scenario during which a node is benign to 1 node however malicious to others could also be quenched.

we have a tendency to propose a unified trust management theme that enhances the protection in MANETs exploitation unsure reasoning. within the planned theme, the trust model has 2 components: trust from direct observation and trust from indirect observation.

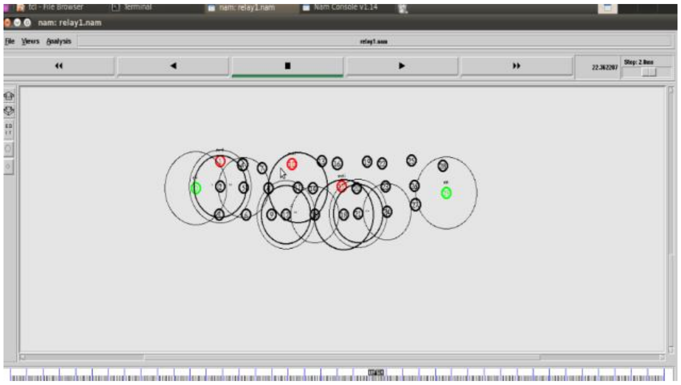

Fig.3 Indirect Method

3.2 Packet Delivery Factor

We will see that the projected theme features a a lot of higher PDF than the present theme as a result of the trust based mostly routing calculation can discover the wrongful conduct nodes.the results conjointly demonstrate that the projected theme with indirect observation has the very best PDF among these 3 schemes.in fig.4 we can also realize that the PDF of 3 schemes decreases bit by bit once the quantity of nodes grows.this is as a result of the collision of causation messages becomes a lot of frequent because the range of nodes of nodes will increase within the painter.

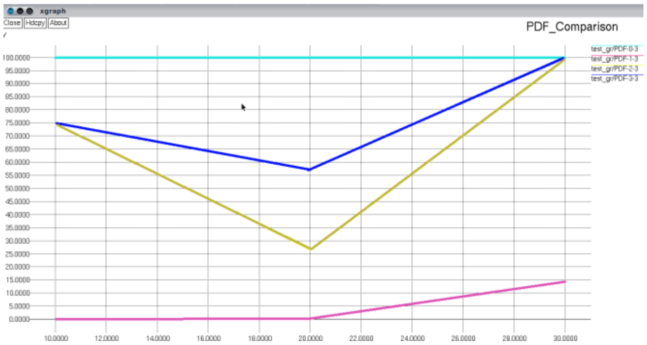

Fig.4 PDF Vs The No Of Nodes

3.3 delay Evalvation

we can see that,as the node rate will increase,the average end-to-end delay becomes longer.the reason is that trust primarily based routing path is typically a extended route from a supply node to a destination node.

The delay of a network specifies however long it takes for a little of information to travel across the network from one node or end to a different. it\'s usually measured in multiples or fractions of seconds.

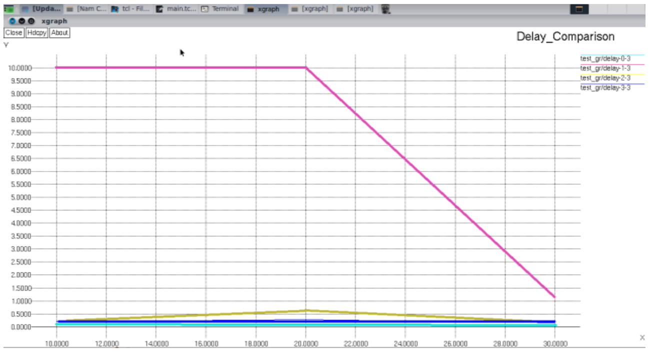

Fig.5 Delay Vs Node Velocities

3.4 Overhead Evalvation

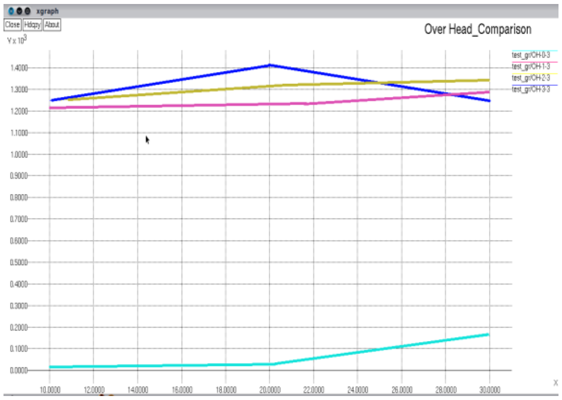

Fig.6 Overhead Vs No Of Nodes

The above graph indicates the overhead of proposed system the overhead is not very high. However, as the number of nodes increases, the percentage of overhead in messages drops dramatically.

V. CONCLUSION AND FUTURE WORK

We can see that, as the node speed will increase, the average end-to-end delay becomes longer. The during this project the routing security problems with MANETs, area unit mentioned. One kind of attack, the region, which may simply be deployed against the Edouard Manet, is delineating. Using trust management schemes.The percentage of packets received through the planned technique is best than that in OLSR WITH changed DSR in presence of cooperative region attack.

The solution is simulated victimization the worldwide Mobile machine and is found to attain the desired security with token delay & overhead. Future works is also focused on ways in which to scale back the delay within the network

we area unit reaching to extend the energy awareness of the nodes that area unit collaborating within the network. In traditional AODV it\'ll perpetually select shortest path. Therefore the nodes can lose its energy in fast manner. From our new theme we are going to extend trust aware with energy aware AODV protocol. While knowledge forwarding, the nodes can amendment the trail supported energy state of each nodes. Thus we are able to improve the QOS with improved Security. Finally we are able to improve prolong network.

REFERENCES

[1] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi ,“ A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)” International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[2] Biao Han, Member, Jie Li, Senior Member, and Jinshu Su, Member ,“ Secrecy Capacity Optimization via Cooperative Relaying and Jamming for WANETs”. IEEE Transactions on Parallel and Distributed Systems vol3,no.2,December2013.

[3] Fung Po Tso, Member, IEEE, Lin Cui, Lizhuo Zhang, Weijia Jia, Senior Member, IEEE,Di Yao, Jin Teng, and Dong Xuan, Member, IEEE,“ DragonNet: A Robust Mobile Internet Service System for Long-Distance Trains”.IEEE transactions on mobile computing, vol. 12, no. 11, November 2013.

[4] Hemant Kamle, Geetika Dubey,“ Scheme of security in Mobile Ad Hoc Networks using Route Blacklist Limit Mechanism”. International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012.

[5] Ing-Chau Chang, Member, IEEE, and Chia-Hao Chou,“HCoP-B: A Hierarchical Care-of Prefix with but Scheme for Nested Mobile Networks”,IEEE transactions on vehicular technology, vol. 58, no. 6, July 2009.

[6] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE ,“ Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach” Content is final as presented, with the exception of pagination.IEEE systems journal Volume3,issue-2,July 2014 .

[7] Khaled H. Almotairi, Member, IEEE and Xuemin (Sherman) Shen, Fellow, IEEE,“A Distributed Multi-Channel MAC Protocol for Ad Hoc Wireless Networks”,IEEE Transactions on Mobile Computing IEEE systems journal Volume3,issue-2,July 2013 .

[8] Manoharan. R, Rajarajan. S, Sashtinathan. S and Sriram. K,“A Novel Multi-hop B3G Architecture for Adaptive Gateway Management in Heterogeneous Wireless Network”.IEEE International Conference on Wireless and Mobile Computing,vol.34,no.3, December 2009.

[9] Oscar F. Gonzalez1, Michael Howarth1, George Pavlou,“Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks”,IEEE transactions on wireless communications vol.6, no. 7, June2011.

[10] Quansheng Guan,F.Richard Yu,Shengming Jiang,and Victor C. M. Leung, Fellow,“ Joint Topology Control
and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications,”IEEE transactions on vehicular technology,vol.61,no.6,july 2012.

[11] F. Richard Yu, Helen Tang, Peter C. Mason, and Fei Wang,“A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks”. IEEE transactions on network and service management, vol. 7, no. 4, December 2010.

[12] J. G. Rocha, L. M. Goncalves, P. F. Rocha, M. P. Silva, and S. Lanceros Mendez, “Energy harvesting from piezoelectric materials

fully integrated in footwear," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 813–819, Mar. 2010.

[13] Sameh Zakhary, Milena Radenkovic, and Abderrahim Benslimane, Senior Member,IEEE, "Efficient Location Privacy-Aware Forwarding in Opportunistic Mobile Networks"IEEE transactions on vehicular technology, vol. 63, no. 2, February 2014.

[14] Sanjeev Gangwar , DR. Saurabh Pal and DR. Krishan Kumar" Mobile Ad Hoc Networks:Comparative Study of QoS Routing Protocols", IJCSE, Vol 2,Issue1,771-775, January 2012.

[15] Shengrong Bu,F. Richard Yu,Xiaoping P. Liu, and Helen Tang,"Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks,"IEEE transactions on wireless communications vol.10, no. 9, September 2011.

[16] Sudakshina Dasgupta, Paramartha Dutta, "A Novel Game Theoretic Approach for Cluster Head Selection in WSN", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN:2278-3075, Volume-2, Issue-3, February 2013.

[17] A. Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," IEEE Trans. Ind. Electron., vol. 57, no. 3, pp. 840–849, Mar. 2010.

[18] Yanchao Zhang, Member,Wei Liu, Wenjing Lou, Member and Yuguang Fang, " Senior Member,Securing Mobile AdHoc Networks with Certificateless Public Keys". IEEE transactions on dependable and secure computing, vol. 3, no. 4, October-Dec 2014.

[19] Yang Qin, Dijiang Huang, Senior Member, IEEE, and Bing Li, Student Member, IEEE ," STARS: A Statistical Traffic Pattern Discovery System for MANETs"IEEE transactions on dependable and secure computing, vol. 11, no. 2, March/April 2014.

[20] Zhexiong Wei, Helen Tang, F. Richard Yu," Security Enhancements for Mobile Ad Hoc Networks with Trust Management"J.Wireless Commun.Networking, vol. 2013,pp. 188–190, February 2014.

S.Shalini obtained her B.E. in Electronics and Communication Engineering (Anna university of Chennai, 2013), M.E. in Applied Electronics (Anna university of Chennai, 2015).She is currently doing her project work on Mobile ad hoc networks which includes security.

T.Manjula obtained her B.E. in Electrical and Electronics Engineering (Bharathiyar University, 2004), M.E in Applied Electronics (PSG college of Technology, Coimbatore, 2009).At present working in Hindustan College of Engineering and Technology with the experience of 8 years. Her area of interest is wireless and embedded system.

Dr.B.Anand obtained his B.E & M.E from Annamalai University; chithamparam.He has served as a associate professor for 11 years in Hindusthan College of Engineering and Technology, Coimbatore. His area of interest is embedded system