ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 6.047

Volume 5, Issue 5, May 2017

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Enhancement of Performance Analysis in Anonymity MANET through Trust-Aware Routing Protocol

Swetha M S[1]
Assistant Professor, Department of IS&E
BMS Institute of Technology & Management
Yelahanka, Bangalore -560064, Karnataka – India

Dr. Thungamani M[2]
Assistant Professor, Department of CS&E
COH UHS, CAMPUS GKVKt
Yelahanka,Bangalore -560064, Karnataka – India

Ankita Mishra[3]
Student, Dept. of ISE
BMS Institute of Technology & Management
Yelahanka,Bangalore -560064, Karnataka – India

Abstract: A Mobile ad Hoc Network is a collection of nodes which is an infrastructure less network and hence can be easily established and deployed instantly. In addition to their normal operation, all the nodes in this kind of network act as routers as well. Because of the mobility and dynamic nature of the network, all the nodes are free to move randomly and hence topology of a MANET changes very frequently. This invites the complexity of routing the packets from source to destination. Also, as a MANET is a multi-hop network, the packets should pass through intermediate nodes which always need not be genuine all the time which poses many security issues in MANET's. Trust-Aware routing is a secure routing protocol which is a trust based secure routing scheme that considers information collected from neighbouring nodes. Based on the trust information received about a node from its neighbouring nodes and its past history of transactions, we assign a trust value for every node in the network. Here, every node has the complete details about the neighbouring nodes in the group; this information can be used by the source node in evaluating the trust value of all the nodes in the network. If this value is less than a specific threshold set by the coordinator nodes, that specific node can be considered as a malicious node and hence routing paths should not involve such nodes, which guarantees secure path routing. This protocol has been implemented on NS-2 and results show that this protocol achieved better performance in terms of the packet delivery ratio and throughput when compared to existing routing schemes in literature.

Keywords: MANET, security, routing.

I. INTRODUCTION

In the recent years, Computers and Information Technology has become an emerging field and is growing day by day. In spite of the efforts put forth towards finding secure computing environments, there are lot of threats left unaddressed on the security, integrity and privacy of the data exchanged in communications. A mobile ad hoc network (MANET) is a communications network that can be defined as a collection of independent, dynamic, wireless and mobile nodes that can be established without the help of any pre-existing infrastructure. As every node in a MANET is a wireless node, it has a limited transmission range, and hence cannot communicate with all the other nodes in the network directly. This has lead MANET to be a multi hop network. Every node in a MANET moves randomly in and out of it and hence the topology of this network changes dynamically. This feature of MANETs also results in frequent changes in the location of the mobile nodes which makes routing task more complicated. As the nodes are mobile, and hence there is no continuous power supply, the transmission power of the nodes is limited. As MANET is an infrastructure less and easily reconfigurable network, deployment is very easy and installation costs are very low, which has led to its wide range of application areas. MANETs have applications in many emergency and rescue situations like military, earthquakes, floods, war zones, medical and industrial fields, corporate offices, relief operation areas for disaster management, personal and home networks.

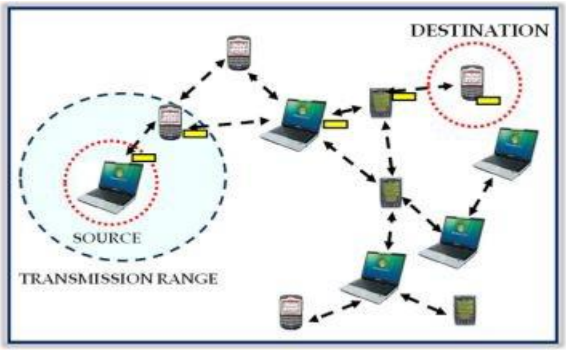

Fig.1.1 A Mobile ad hoc Network

1.1 Advantages of MANETs

The advantages of an Ad-Hoc network include the following:

- MANETs can be succeeded where there is less telecommunication infrastructure.
- MANETs provide access to information and services regardless of geographic location.
- Independence from central network administration.
- Self-configuring network, nodes are also act as routers.
- Less expensive as compared to wired network.
- Scalable—accommodates the addition of more nodes.
- Enhanced flexibility.
- Robust and powerful due to decentralized administration.
- The network can be set up at any place and time.

1.2 Attacks in MANETs

As there is no centralized authority and management authority taking are of the authenticity of the nodes and because of the wireless physical channel in MANET which is an open medium, it is very difficult and challenging to establish secure communication among the nodes. Due to this, MANET's are prone to different types of attacks like flooding attacks, Denial of Service Attack, Impersonation, Black hole attack, wormhole attack, misbehaviour of nodes etc. These attacks can also be specified as falling under different categories like passive and active attacks.

Passive attack: In this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping.

Active attack: In this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; causing routing disruption, network resource depletion, and node breaking.

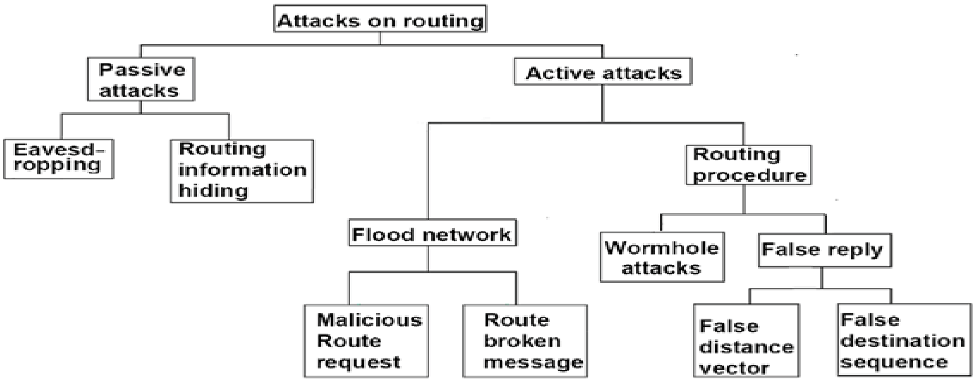

Fig.1.1.1 Classification of attacks on Routing

II. Literature Survey

A secure routing protocol which is a trust based secure routing scheme that considers information collected from neighbouring nodes. Based on the trust information received about a node from its neighbouring nodes and its past history of transactions, we assign a trust value for every node in the network. If this value is less than a specific threshold set by the coordinator nodes, that specific node can be considered as a malicious node and hence routing paths should not involve such nodes, which guarantees secure path routing.

A strategy based on trust aware routing has been suggested for Optimized Link State Routing (OLSR) protocol. The modified OLSRM protocol using trust aware routing framework has been proposed. The performance of new protocol OLSRM is evaluated for the two types of attacks viz. Black Hole Attack and Self Behavior Attack. The comparison of MANET performance using original OLSR and modified OLSRM protocol has been presented for 1000x400 square meter network area and results are discussed.

Trust-aware routing protocol based on the formation of trusted Mobile Process groups (MPG). MPG is a collection of processes or mobile nodes present in defined vicinity where they all lie within each other’s radio transmission range. The trusted MPG groups formed in MPGTAR calculate trust based on the mobility rate, membership time within a local group and the number of overlapping groups of a node. The proposed protocol continuously computes and updates the reliability, trustworthiness of a node and finds the confidence level in that node. If the node is trustworthy and reliable, the confidence in that node will be increased to trust the node for forwarding a data packet. Simulation of MPG-TAR was done using Glomosim simulator.

Trust-Aware Routing Protocol (TARP) is proposed for secure-trusted Ad-hoc routing. In TARP security is inherently built into the routing protocol where each node evaluates the trust level of its neighbors based on a set of attributes. TARP is based on three new concepts. First, for route establishment, a new secure ad-hoc routing mechanism is used. Second, six security parameters are considered in computing the trust-level of a node in a given route and include: *software configuration*, *hardware configuration*, *battery power*, *credit history*, *exposure and organizational hierarchy*. A secure route is established based on a confidence level prescribed by a user in terms of these attributes. Third, we present TARP reputation system and trust metric. Our performance evaluation shows that TARP is a robust trust routing algorithm that reacts quickly to the dynamics of the network.

III. Methodology

In the initial stage of network formation, every node stores the information about all neighbouring nodes connected to it. Based on the number of nodes present in the group and their location entire network can be treated as a collection of groups of nodes. Every peer group can have a coordinator node, a leader node which may track the information exchange details within the group and also in the entire network. These nodes are capable of collecting the information from their peers and the same can be exchanged to other groups when necessary. Since every node has the complete details about the neighbouring nodes in the group, this information can be used by the source node in evaluating the trust value of all the nodes in the network.

When a node has data to send to an intended destination, it first initiates a route discovery process, which includes sending of a route request and its identifier to all the neighbouring nodes of the source. Then all these nodes forward these request packets to all their corresponding neighbouring nodes and so on. To reduce the flooding of these request messages which adds more and more overhead on the network, a location based routing scheme can be employed in which based on the distances between the nodes and their location information, the number of duplicate request packets at a node can be reduced. When this request has been received by all the nodes in the network, the nodes will send a reply using the identifier information in the request path. Every node here exchanges service information, past history of transactions and reputation information regarding their neighbouring nodes.

This information upon collected by the source node, it evaluates a trust value for every nodes on the paths available to the destination node. The path is evaluated such that if the trust value for a specific node less than a specific threshold, that node can be considered as malicious and hence can be excluded in the path to destination which makes the chosen path more secure. This can be used to find a more secure path to the destination avoiding attacks like worm hole and black hole etc.

IV. Results and Analysis

The protocol has been implemented on simulation tool called NS2. Results obtained can be shown using NAM and Xgraph. A Wireless Channel, has been considered with Propagation model as Two way Ground model, a wireless Physical channel, using Omni directional antennas with a drop tail queue or a Priority queue of length 50. The number of nodes can be statically fixed or can be changed at runtime. Simulation is done varying from 20 to 100 nodes for different scenarios.

4.1. Performance analysis on Packet Delivery Ratio

Packet delivery ratio is evaluated based on the ratio of number of packets sent to the number of packets received. We have recorded the PDF with varied number of nodes at various time intervals and it is observed that even in the presence of malicious nodes, our protocol showed improved PDF ratio when compared to several existing protocols for MANETs.

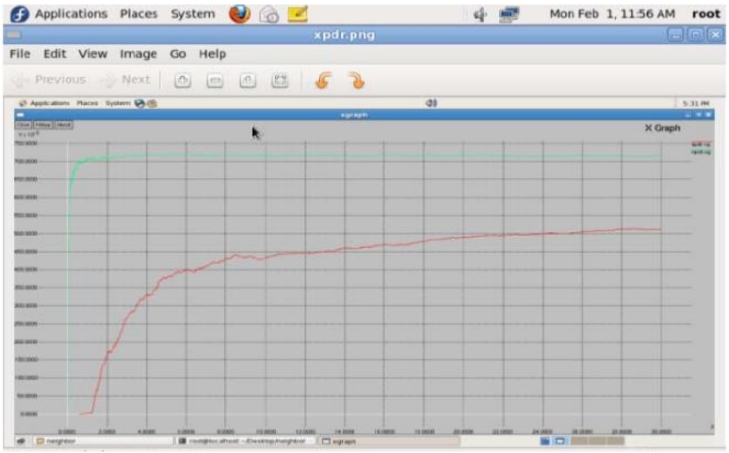

Fig.4.1 Performance Analysis using PDF

4.2. Performance analysis on Throughput

Throughput is evaluated based on the received packet size w.r.t the start and stop times at regular intervals of time. We have recorded throughput with varied number of nodes from 20 to 100 at various pause times. Throughput was more with minimal no. of nodes but as the no. of nodes increased throughput may gradually decrease.

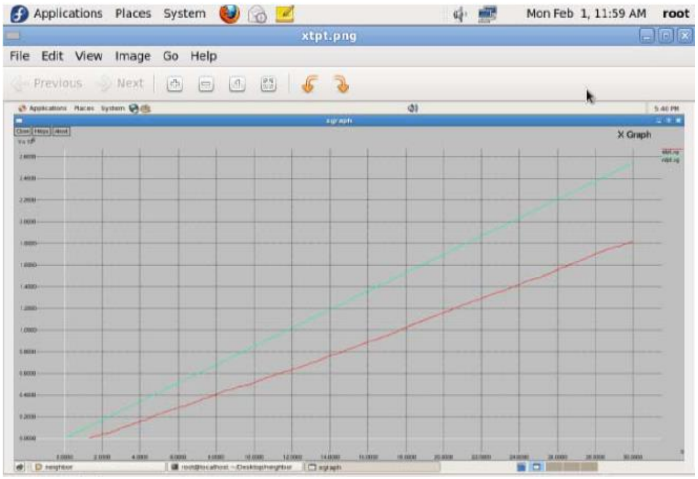

Fig.4.2 Performance Analysis using Throughput

4.3. Performance analysis using overhead

Overhead is evaluated based on the total number of control packets generated in the network. Because of the use of location based routing of request and reply packets, the no. of control packets exchanged has reduced there by reducing the overall overhead in the network.

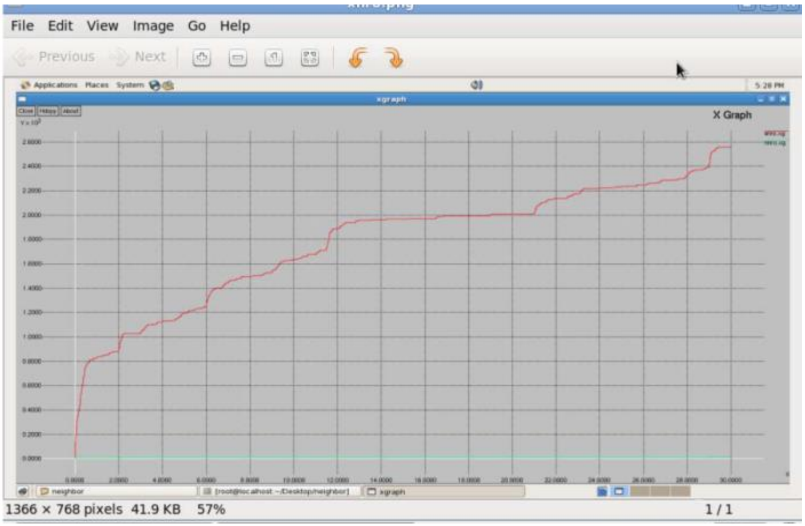

Fig.4.3 Performance Analysis using Overhead

4.4 Performance analysis on End-to-End delay

End-to-End delay is evaluated based on the sending time and receiving times of the packets. As the packet size increases, the time taken for transmission may gradually increase. We have considered our packet size as 512 bytes but that can be varied at runtime. Fig. 4.4 shows the delay recorded at various pause times.

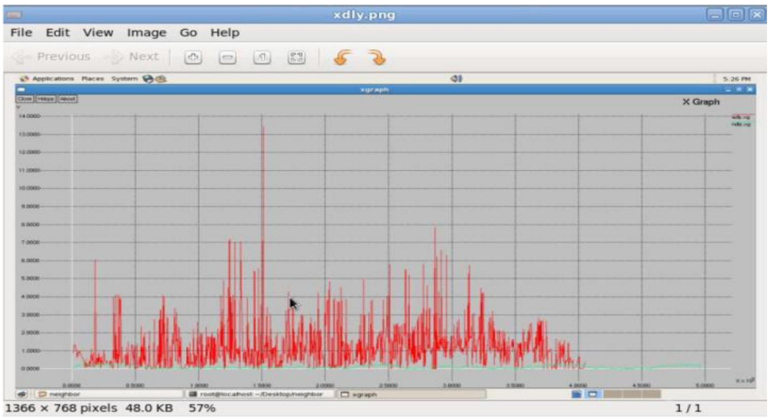

Fig.4.4 Performance Analysis using End-to-End Delay

V. APPLICATIONS

Mobile Ad-Hoc Networks allow users to access and exchange information regardless of their geographic position or proximity to infrastructure. In contrast to the infrastructure networks, all nodes in MANETs are mobile and their connections are dynamic. Unlike other mobile networks, MANETs do not require a fixed infrastructure. This offers an advantageous decentralized character to the network. Decentralization makes the networks more flexible and more robust.

The following are the applications of MANETSs:

- **Military arena:** Military equipment now routinely contains some sort of computer equipment. Ad- hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

- **Commercial Sector:** Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. This may be because all of the equipment was destroyed, or perhaps because the region is too remote. Rescuers must be able to communicate in order to make the best use of their energy, but also to maintain safety. By automatically establishing a data network with the communications equipment that the rescuers are already carrying, their job made easier. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

- **Personal Area Network (PAN):** Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc net-work can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context

- **Data Networks:** A commercial application for MANETs includes ubiquitous computing. By allowing computers to forward data for others, data networks may be extended far beyond the usual reach of installed infrastructure. Networks may be made more widely available and easier to use.

- **Sensor Networks:** This technology is a network composed of a very large number of small sensors. These can be used to detect any number of properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. The capabilities of each sensor are very limited, and each must rely on others in order to forward data to a central computer. Individual sensors are limited in their computing capability and are prone to failure and loss. Mobile ad-hoc sensor networks could be the key to future homeland security.

- **Bluetooth:** Bluetooth can provide short range communication between the nodes such as a laptop and mobile phone.

VI. CONCLUSION

In this proposed protocol, the source node evaluates the authenticity of the nodes in the path that can be used for data transmission based on the trust value computed from the information collected from all the nodes in the network. This method chooses the nodes with more authenticity in the path to destination; hence a better secure transmission path is obtained.

This method guarantees better performance in terms of increased packet delivery ratio and throughput and reduced delay and overhead even in the presence of malicious nodes and hence can overcome the difficulties w.r.t attacks like wormhole and black hole etc.

VII. Future Enhancement

As an enhancement, various types of metrics can also be used to decide on a nodes authenticity to achieve better and more security when more number of malicious nodes are present.

References

1. V.Sesha Bhargavi, S.Viswanadha Raju, “Enhancing Security in MANETS through Trust-Aware Routing”, IEEE WiSPNET Conference, 2016.
2. Kirti Aniruddha Adoni; Anil S. Tavildar, “Trust aware routing framework for OLSR protocol to enhance performance of Mobile Ad-Hoc Networks”, IEEE Conference, 2015.
3. Harjeet Kaur, Manju Bala, Varsha Sahni, “Study of Blackhole Attack Using Different Routing Protocols in MANET”, IJAREEIE, Vol. 2, Issue 7, July 2013.
4. Shawkat K Guirguis, Ommelhana S.Saaid, " Evaluating the performance of secure routing protocols in mobile ad hoc networks, International Journal of Advanced Research in Computer and Communication Engineering, Vol 1, No.9, Nov 2012.
5. Matthew F. Steele, “Security Verification of Secure MANET Routing Protocols” Thesis, March 2012.
6. Preeti Sachan and Prabitra Mohan Khilar, “Securing AODV routing protocol in MANET based on cryptogarphic authentication mechanism," IJNSA, Vol.3,No.5, Sep 2011.
7. V. Aakanksha, Pumam Bedi, “MPG-TAR: Mobile Process Groups Based Trust Aware Routing Protocol for MANETs”, IEEE Conference, 2010.
8. W. Creixell and K. Sezaki, “Routing Protocol for Mobile Ad Hoc Networks using Mobility Prediction”, Center for Spatial Information Science University of Tokyo, Tokyo, Japan.
9. Claude Crepeau ,QC Carlton R. Davis ; Muthucumaru Maheswaran “A Secure MANET Routing Protocol with Resilience against Byzantine Behaviours of Malicious or Selfish Nodes” in Advanced Information Networking and Applications Workshops, 2007.
10. L. Abusalah; A. Khokhar; M. Guizani, “ Trust Aware Routing in Mobile Ad Hoc Networks”, IEEE Conference, 2006.