Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Improving Scalability and Security using Region Based Routing Protocol in Mobile Ad Hoc Network

Ramniwas Lodhi
Department of CSE/IT
Madhav Institute of Technology and Science
Gwalior, India

Neha Bhardwaj
Department of CSE/IT
Madhav Institute of Technology and Science
Gwalior, India

Abstract: Mobile ad hoc network is infrastructure-less network in which nodes communicate to each other wirelessly. MANET is easily prone to attacks as compared to wired network. There are methods available to improve the security of the network. These methods provide integrity, confidentiality and non-repudiation. RSS (Receive Signal Strength) technique provides security by calculating trust on the basis of signal strength. It has some issue and to overcome this issue, Region Based Routing is used that eliminates the duplicate entry from the routing table. In our proposed work we are applying Region Based Routing in the network. Region based routing is used to select some region for data forwarding and it eliminates the duplicate entry from the routing table. This makes it suitable for large network as in this we are only concerned with the small region. Other parameter that affects network is scalability. Scalability is the term used to enlarge the network size and improve the performance. It enables the node to communicate to each other in increased coverage area.

Keywords: Mobile ad hoc network, Secure Routing, Routing based protocol, Trust and Certificate revocation.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of two or more nodes equipped with wireless communications and networking capability. The nodes within the radio range can immediately communicate with each other. The nodes that are not within each other's radio range can communicate with the help of intermediate nodes where the packets are relayed from source to destination. Each node should be configured with an unique identity to ensure the packets correctly routed with the help of a routing protocol of a MANET. MANETs have distinct advantages over traditional networks: (a) it can be easily set up and dismantled; (b) it is a cost-effective solution for providing communication in areas where setting up fixed infrastructures is not a suitable option constraint such as geographical location, financial implications, etc; (c) it can be set up in emergency situations (e.g., rescue mission). A node requires authentication for secure information exchange and to avoid the security threats. However, establishing secure communication in a MANET is particularly challenging task because of the following issues: (a) shared wireless medium; (b) no clear line of defense; (c) self organizing and dynamic network; (d) most of the messages are broadcasted; (e) messages travel in a hop-by-hop manner; (f) nodes are constrained in terms of computation and battery power. In this paper, we focus on the problem of secure route discovery and data transmission in an independent MANET [1].

Fig.1. Ad hoc Network

II. SECURE ROUTING FOR MANET

Security protocols for MANET's can be mainly categorized in two major categories:
Prevention: This mechanism involves protocols which prohibit the attacking node to initiate any action. This approach requires encryption technique to authenticate the confidentiality, integrity, non-repudiation of routing packet information Detection and Reaction: Detection and Reaction mechanism as the name suggest will identify any malicious node or activity in the network and take proper action to maintain the proper routing in the network. On the basis of our survey, secure routing protocols can be classified as Figure 2 [2]

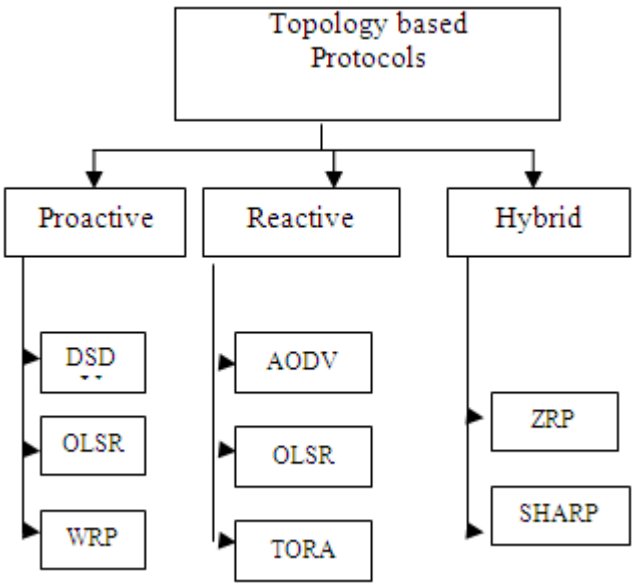

Fig.2:- Classification of Routing Protocols of MANET

III. TRUST

The concept of trust is important to communication and network protocol designers where establishing trust relationships among participating nodes is critical to enabling collaborative optimization of system metrics. According to Eschenauer et al., trust is defined as "a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities." According to, Trust has also been defined as the degree of belief about the behavior of other entities (or agents) [3].

IV. CERTIFICATION REVOCATION

Scheme In our previous work, we increase and decrease a trust counter depending on the behavior of the node. These trust values are saved in NTT where nodes which have trust value lower than the threshold trust value TCthr are termed as malicious. In the certificate revocation scheme, when the node's "Expiry time" (ET) elapsed, the node broadcasts a renewal request packet (RWREQ) to its neighbors. Node which receives a RWREQ, checks its node status from the NTT. If the nodes have value less than the TCthr value, then the RWREQ is dropped or else the node sends a Renewal Reply Packet (RWREP), along with a new IT and ET field, back to the node. Due to the redundancy technique, the renewal of nodes does not consume time or halts, even if any movement of nodes or node failure or even disconnection in network occurs. Thus our work increases the integrity factor of the data in the network due to certificate authority scheme along with resisting against the outside attackers. Our scheme also reduces the overhead of nodes because of the redundancy factor, as it reduces the time consumption and dependency over the nodes [4].

V. REGION BASED ROUTING PROTOCOL

The primary purpose of the RBR protocol is to efficiently construct routes between any two nodes in a Global-MANET with low routing overhead. To achieve this goal, we explore the possibility of using hop count information in the route discovery. By using hop count information, RBR localizes route discovery to a small topo - logical region by reducing the number of nodes to which the route request packet is propagated. Limiting the route discovery region results in fewer route discovery messages, and has a substantial impact on the consumption of energy and bandwidth in the Global-MANET. RBR can find a route effectively either between any two MNs or between an MN and the AP in a Global-MANET. When a source node desires to communicate with a node on wired networks, it will initiate a route discovery to the AP if there is no a valid route available to the AP. Once a route is found, the source node begins forwarding data packets to the AP. Then, the AP forwards the data packets to the destination node through the wired line by using routing protocols of the wired networks [5].

VI. AODV

The Ad hoc On Demand Distance Vector (AODV) routing algorithm is a routing protocol designed for ad hoc mobile networks. Both unicast and multicast routing is possible in MANET. It is an on demand algorithm, that builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. In Addition, AODV forms trees which connect multicast group members. These trees are composed of the group members and the nodes needed to connect the members. AODV protocol uses sequence numbers to ensure the freshness of routes. It is self-starting, loop-free and scales to large numbers of mobile nodes [6].

VII. LITERATURE SURVEY

v Antesar M. Shabut et al. [2017] This paper investigates the problems of data sparsity and cold start of recommender systems in existing trust models. It proposes a recommender system with clustering technique to dynamically seek similar recommendations based on a certain timeframe. Similarity between different nodes is evaluated based on important attributes includes use of interactions, compatibility of information and closeness between the mobile nodes. The recommender system is empirically tested and empirical analysis demonstrates robustness in alleviating the problems of data sparsity and cold start of recommender systems in a dynamic MANET environment [7,8].

Zakir Ullah et al. [2016] The purpose of malicious node is to attack network while the motivation behind selfish node is to save its assets by not cooperating with other, so appropriate security measures must be provided for handling the asserted types of nodes. Trust management is one of the schemes that can be utilized for dealing with the affirmed nodes in MANET. However, trust management in MANET is a challenging task because of its unique characteristics. This paper investigates general issues related to each step of trust management in MANET and explores trust management schemes developed for routing security in MANET [9].

Sagar R Deshmukh et al. [2016] this paper proposes an AODV-based secure routing mechanism to detect and eliminate black hole attack and affected routes in the early phase of route discovery. A validity value is attached with RREP which ensures that there is no attack along the path. The proposed method is simulated in NS2 and performance analysis is carried out. Utilization of mobile devices is burgeoning rapidly and consequently mobile ad-hoc networks (MANETs). The self configuring and infrastructure less property of MANETs makes them easily deployable anywhere and extremely dynamic in nature. Lack of centralized administration and coordinator are the reasons for MANET to be vulnerable to active attack like black hole. Black hole attack is ubiquitous in mobile ad hoc as well as wireless sensor networks. Black hole affected node, without knowing actual route to destination, spuriously replies to have shortest route to destination and entice the traffic towards itself to drop it. Network containing such node may not work according to the

protocol being used for routing. Commonly used protocols like ADOV, DSR, and so forth in MANET are not designed to tackle black hole attack or black hole affected routes [10].

Abhijit Kundu et al. [2016] this paper presents a new on-demand power saving routing algorithm for mobile ad-hoc networks. The protocol is based on node identification using kmeans & Convex Hull that gives less hopping, energy saving on demand routing protocol. K-means identify cluster from sender node then convex-hull find the outer region area of the cluster using some mathematical expression find out the best node to forward the data here also used one priority based protocol for energy saving node identification [11].

V. Sesha Bhargavi et al. [2016] In this paper, our propose a trust-based secured file sharing system, namely S-DSR protocol, for disconnected MANETs. The system uses this S-DSR protocol to derive a node's authenticity and find a secure path for file sharing without involving any malicious nodes in the path. This protocol has been implemented on network simulator and results show that this protocol provides better packet delivery ratio and less overhead than several existing protocols [12].

Sagar R. Deshmukh et al. [2016] this paper proposes a DSR-based secure routing to detect black hole attack. The proposed solution, attaches a validity value with RREP. This validity value is checked by the first intermediate hop along the route reply and ensures that there is no black hole attack along the path [13].
Raihana Ferdous, et al. [2016] In this paper, 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 [14].

VIII. PROBLEM STATEMENT

In existing technique author apply RSS (Receive Signal Strength) technique in which node calculates trust on the basis of signal strength. But it's not an efficient procedure because malicious node drop packet by using the identity of other nodes. So on the basis of this approach we cannot recognize exact malicious node.
Secondly, the calculation of trust performed by indirect, direct and globally methods which are very time consuming process for detecting the malicious or misbehavior nodes in the network.

IX. PROPOSED WORK

To overcome this problem we are applying Region Based Routing in the network. Region based routing is used to select some region for data forwarding and it eliminates the duplicate entry from the routing table. This makes it suitable for large network as in this we are only concerned with the small region. Scalability can be achieved by this method. Firstly the source node adds the address of the destination node in the packets. Now the region is formed by calculating the distance between source and destination. Then the intermediate nodes forward the data to the neighboring nodes within the region and reached to destination through the trusted nodes to make it secure and reliable.

Proposed algorithm:

Step:1 Initialize network
Step:2 Select source and destination nodes
Step:3 Now put the destination address in the HELLO packet
Step:4 Apply region based routing protocol to find the suitable area
Step:5 Calculate distance between the source and intermediate node by Euclidean Distance

$$d = \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2}$$

Step:6 Update routing table
Step:7 Calculate the trust value of each node
Step:8 Then forward the data into that particular region
Step:9 Data reached to the destination through the trusted nodes
Step:10 Exit

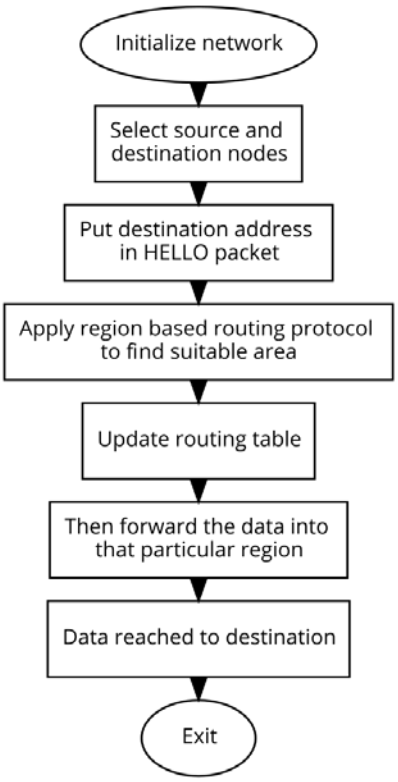

Fig.3 Flowchart of Proposed algorithm

X. RESULT ANALYSIS

1. Packet delivery ratio:

It outlines the proportion of packets deliver from supply towards destination. The graph show a PDR graph among base approach as well as proposed approach. This PDR rate is improved in proposed than existing approach.

PDR = No. of packets received / No. of packets sent

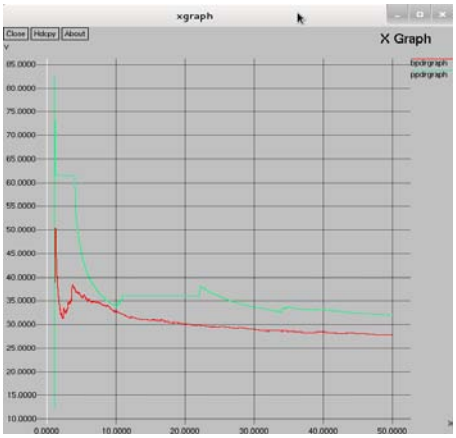

Fig. 4 Packet delivery ratio

2. Throughput:

The transfer of information lying on information measure is decision as output. The graph represents a output graph among base approach moreover as projected approach. The output of the projected approach is okay than the present approach.

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

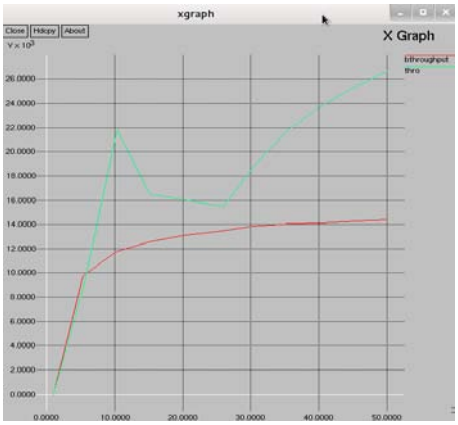

Fig. 5 Throughput

3. Packet drop:

The difference in number of packets received than the number of packets sent is known as packet drop. From the graph, it is shown that the proposed work is better than the existing work as the number of packets drop is less in the proposed work.

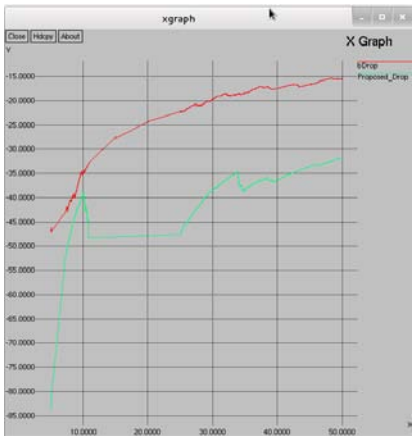

Fig.6 Packet Drop

XI. CONCLUSION

In this paper, we discussed mobile ad hoc network which is most useful topic in the research area. It provides the network which provides the communication among nodes without the need of any wire. We proposed a technique which generate one region then transfer the data from that particular area. This improves the scalability of the network and also provides the secure path for the data transfer. Our results show that we enhanced the network performance by increasing the throughput and packet delivery ratio. It decreases the packet dropping in the network which improves the efficiency of the network.

REFERENCES

[1] Waleed S. Alnumay and Uttam Ghosh "Secure Routing and Data Transmission in Mobile Ad Hoc Networks" International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.1, January 2014.

[2] Parul Tomar, Prof. P.K. Suri and Dr. M. K. Soni "A Comparative Study for Secure Routing in MANET" International Journal of Computer Applications (0975 – 8887) Volume 4 – No.5, July 2010.

[3] K.Seshadri Ramana Dr. A.A. Chari Prof. N.Kasiviswanth "A SURVEY ON TRUST MANAGEMENT FOR MOBILE AD HOC NETWORKS" International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April2010, 10.5121/ijnsa.2010.2206.

[4] Rajaram Ayyasamy1 and Palaniswami Subramani2 "An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad-hoc Networks" The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.

[5] Rui Teng, "RBR: A Region-Based Routing Protocol for Mobile Nodes in Hybrid Ad Hoc Networks" 0163-6804/06/$20.00 © 2006 IEEE IEEE Communications Magazine • November 2006 .

[6] Nidhishkumar P. Modi1 , Krunal J. Panchal "A Literature survey on Improving AODV protocol through cross layer design in MANET" © 2014 IJEDR | Volume 2, Issue 4 | ISSN: 2321-9939.

[7] 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.

[8] Zakir Ullah , Muhammad Hasan Islam and Adnan Ahmed Khan "Issues with Trust Management and Trust Based Secure Routing in MANET" 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST).cations (CNC), 978-1-5090-4588-4/17/$31.00 ©2017 IEEE.

[9] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople "AODV-Based Secure Routing Against Blackhole Attack in MANET" IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India.

[10] Abhijit Kundu, Ritika Misra, Atreyee Kar, Sagarika Debchoudhury, Shilpa Pareek, Somen Nayak and Ratul Dey "ON DEMAND SECURE ROUTING

PROTOCOL USING CONVEX-HULL & K-MEAN APPROACH IN MANET"2016 IEEE.

[11] V. Sesha Bhargavi , Dr. M.Seetha and S.Viswanadharaju "A Hybrid Secure Routing Scheme for MANETS" 978-1-4673-6725-7/16/$31.00 ©2016 IEEE.

[12] Sagar R. Deshmukh, Dr. P. N. Chatur "Secure Routing to Avoid Black Hole Affected Routes in MANET" 2016 Symposium on Colossal Data Analysis and Networking (CDAN), 978-1-5090-0669-4/16/$31.00 © 2016 IEEE.

[13] 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, 78-1-5090-5510-4/16 $31.00 © 2016 IEEE DOI 10.1109/CSCI.2016.170.

[14] Banoth Rajkumar, Dr.G.Narsimha, "Trust Based Certificate Revocation for Secure Routing in MANET", 2nd International Conference on Intelligent Computing, Communication & Convergence (ICCC-2016), pg no. 431 – 441.