ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Survey on Trust Management and Secure Routing in MANET

Madhavan P, Dr P Malathi
Assistant professor, Dept of CSE, Srikrishna college of Technology
madhrace@gmail.com, pmalathi2004@yahoo.co.in.
Principal, Bharathiyar institute of Engineering for women

Abstract

MANET is a self configuring nodes which does not have fixex infrastructure. The existence of misbehaving nodes may paralyze the routing operation in MANETs. There are many issues related to replication of data like power, server and node mobility, networking partition and frequent disconnection. Cluster based data replication technique can be used for replication of data & energy level of node . The proposed approach is based on calculating trust value for updation and removing the selfish behavior of the mobile nodes from the wireless network

Keywords— *Manet, wireless sensor networks, spectrum hole access, wireless power transfer, Primary user ,secondary user, Sensor*

1. Introduction

1.1 Mobile Ad-Hoc Network (MANET)

Mobile ad hoc network (MANET) is a compilation of autonomous, mobile, wireless devices which forms a communications network even in the absence of fixed infrastructure. The main characteristics of MANET network designers is to provide "dynamic and self-healing, Mobile nodes move arbitrarily and free to move with in its range. . Energy and Bandwidth plays a vital role in prolonging the network life time. Based on the residual energy, nodes can be selected for routing process. Bandwidth defines the amount of data or range of information to be sent from source to destination.

The feature of Ad hoc networks has an added advantage with respect to quick deployment and easy reconfiguration..Emergency disaster relief personnel coordinating efforts after a fire, hurricane, or earthquake..

The three major drawback related to the quality of service in MANET are bandwidth constraints, dynamic topology of MANET and the limited processing and Storing capacity of mobile nodes.[3]

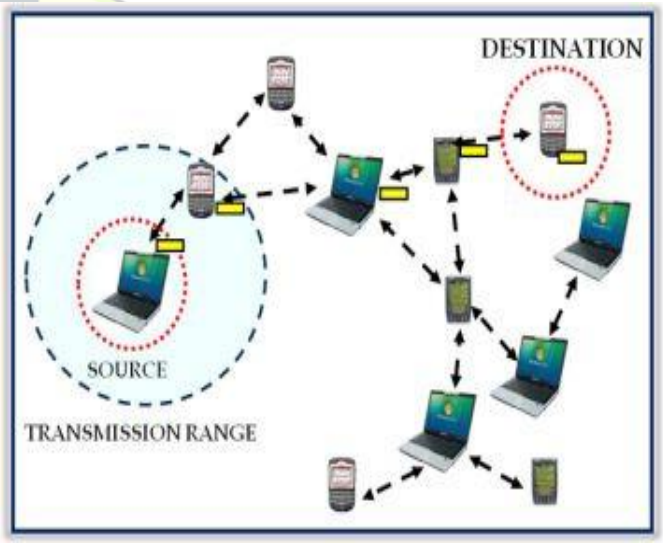


Fig 1:Mobile Adhoc Network

1.2 Mobile Databases in MANET

The mobile database system in a MANET is a dynamic distributed database system, which is composed of some Mobile Heads (MHs). Each MH comprises of local database system. [8]. In storing capacity of mobile nodes, Transaction Manager (TM) of a mobile multi database management system is accountable for providing dependable and steady units of computing to all its users. [6] Nodes in a MANET can be classified by there capabilities that is as a client or a server.
1. A Client or Small Mobile Host (SMH) is a node with reduced processing, storage, communication and power resources.
2. A Server or Large Mobile Host (LMH) is a node having a larger share of

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

resources. Servers, due to their larger capacity contain the complete DBMS and abide primary responsibility for data transmission and satisfying client queries. Clients typically have enough resources to cache portions of the database as well as some DBMS query and processing modules. [7]
There are three layers in a mobile distributed database system;

The application layer – In this layer the user queries are accepted.

The middleware layer – The layer that exists between client and server. This sends MH queries to the local database system. Once the data are fetched from the database, this information is transmitted to the user from the application layer

The database layer – In this layer all the information and data are stored.

The network layer – It manages nodes local information, process the data in routes and sends data packets between the query layer, and the cache layer.

The cache layer – It stores the data which are accessed frequently by the query nodes or their neighbors.

The query layer – It parses the syntax of user queries and determines the query types

Challenges of Mobile Databases in MANET
The main challenges of MANETs for mobile database are listed below:

Power - All mobile devices in the MANET are battery powered. The power plays a role in prolonging the network life time.

Mobility of the nodes - Due to the dynamic nature of a MANET, it exhibits frequent and unpredictable topology changes. The MANET not only operates within the ad-hoc network, but may also require access to a public fixed network. MANETs therefore should be able to adapt the traffic and propagation conditions to the mobility patterns of the nodes.

Resource availability – A node should supply mechanisms for proficient use of processing, memory and communication resources, while maintaining low power consumption. A node should bring about its basic operations without resources exhaustion.

Response Time – For calculating response time ,access time and tuning time must be considered. *Tuning time* is the measure of the amount of time each node spends in Active Mode. This is the time of maximum power consumption for a client. *Access time* measures the sensitivity of the algorithm. It refers to the amount of time a client must wait to receive an answer to a database query.

Quality of Service – Nodes become disengaged for a variety of reasons. This may be due to location or lack of power, dynamic nature and redundancy. The accuracy of information stored at each node: server and client are alike. When portions of the network become separated for a time, data accuracy may become impossible.

Data Broadcast - The size and contents of a broadcast have an effect on power consumption and the frequency of data queries. If the broadcast is too outsized, unnecessary information may be broadcast. If too little information, then wrong information is broadcasted. Thus increasing the on-demand requests. Also if several servers attempt to broadcast simultaneously, there will be a collision and the broadcast of all will be jumbled. 318 M. Qayyum, K.Ur.R. Khan, and M. Nazeer The issues mentioned are some of the major issues which we come across in the mobile database in MANET. Based on the above issues, it is necessary to provide a solution for the mobile database management. Below are some recent literature works which throw a light on the problems and its major solutions.

2. Related Work

Securing MAODV: Attacks and countermeasures

MAODV does not include any provisions for security; thus, it is susceptible to attacks by outsiders as well as malicious insiders. Many attacks on routing protocols for ad hoc networks have been described in the literature. Attackers may drop, modify, replay or fabricate routing messages. Nodes may also impersonate other nodes while sending fabricated messages. Further, multiple attacker nodes may collude to launch attacks, e.g. wormhole attacks. In general, attacks on MAODV can be divided into two categories: (i) attacks on route discovery and establishment, (ii) attacks on multicast tree maintenance. The route discovery and establishment protocols for MAODV are similar to the protocols used in AODV.

In contrast, the attacks on the multicast tree formation and maintenance in MAODV have no counterpart in unicast routing protocols. We describe below several attacks on the operation of MAODV. Each attack has a two-part name - the first part states which message (e.g., RREP) or which property (e.g., group leadership) is misused to launch the attack, and

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

the second part indicates the outcome of the attack, e.g., partition in the multicast tree. For brevity, group leadership is abbreviated as GL, partition in the multicast tree is abbreviated as PART, invalid route as INV and multicast tree formation as MTF. To launch an attack, if the message misused (e.g., MACT) includes a special flag (e.g., Join flag J), the message name includes the flag in parentheses (e.g., MACT(J)).

Attack against Route Discovery and Maintanance:

RREP-INV: When a node either wants to join a multicast group or find a route to a multicast group, it broadcasts a RREQ message. In this attack, a malicious node replies to the RREQ message with the goal of deceiving the node into believing it has found the best route to the multicast group. Consider a group member A that wants to join the multicast group. Broadcasts a RREQ packet with the multicast group address as the destination address and with the J (Join) flag set. Only nodes on the multicast tree qualify to send a reply (RREP) to this request. However, a malicious node M can respond to the RREQ packet with a RREP even if it is not on the multicast tree. A RREP packet includes the replying node's view of the group sequence number. Since A is likely to receive RREPs from multiple nodes, in order to increase the chances of the route to M being selected as the best route to the multicast group, M can fabricate the sequence number field in its RREP.

This attack can be launched by a non-tree-node or by a tree-node. If a non-tree-node succeeds in deceiving the joining node into believing it has a route to the multicast group, it can discard any future messages sent by the node to the group, effectively negating the work done by the route discovery protocol. A malicious tree-node's motivation for launching this attack is more subtle. A tree node that succeeds in becoming a root of many branches of the multicast tree can control the delivery of multicast data to all the nodes in these branches. It can therefore have a potentially large impact on the operation of the application that is using the multicast group.

3. Proposed Scheme

There are many issues for data replication of data like power, server and node mobility . The proposed approach consists of two phases; first phase consists of trust value calculation and in the second phase, secure the routing at the time of data transmission.

3.1 Initial phase – Trust value calculation

In the initial phase, The concept of trust is important to communication and network protocol designers where establishing trust relationships among participating nodes is critical. According to Eschenauer et al. [8], trust is defined as "a set of relations among entities that participate in a protocol. These relations are based on 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 [7], Trust has also been defined as the degree of belief about the behavior of other entities (or agents).

3.1.1 Received Signal Strength of Nodes

In the Received signal strength, we calculate the most stable node with respect to the signal strength received. In the signal strength scheme, each node communicate with there one hop neighbour with sending/receiving an "alive" message. Each node calculates the pairwise relative mobility metrics (RM) by reception of two successive "alive" message. The pairwise relative mobility metrics is calculated.

3.1.4 Steps for calculating Trust value:

Trust value calculation is based on energy and the number of packets that the node has transmitted or discarded.
Initially 46 nodes are created. Source and Destination is selected for the data transmission.

Trust value for the each node is calculated by using the loss monitor agent, the data packets received by the particular node is found out, which has been used for the trust value calculation.

Residual energy for the each node is calculated which results in remaining energy of the individual node after data packet transmission.

The high residual energy and trusted value for the route is found for the reliable transmission of data packets from the source to destination.

Thus the trust value is calculated for each node for secure transmission of packets.

3.2 Second Phase – Security or Detective non cooperative node

In the second phase, the MANET is susceptible to passive and active attacks . The Passive attacks is not more severe, whereas the active attacks involve actions performed by adversaries such as replication,change of data and removing of exchanged data. In particular, attacks in MANET can cause congestion, and which may distract the flow of packets and disconnects the rest of the network..

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Selfish node: It operates usally in the Route Discovery and the Route management phases of the routing protocol. It suppress the data or flow of information and attempts to benefit from other nodes, but refuse to share its own resources.

Malicious node: It acts to the detriment of the network by manipulating routing. The routing protocols use hop count as parameter. A node can falsely claim a low hop count to a destination, enabling it to intercept traffic for that destination. Node identities are not authenticated, so a node can claim to be the destination of a route.

Malicious Behavior is defined as "When a node breaches any of the security principles and is therefore under any attack. Such nodes exhibit one or more of the following behavior.

Packet Drop- Simply consumes or drops the packet and does not forward it.

Battery Drained- A malicious node can waste the battery by performing unnecessarily operations.

Bandwidth Consumption- Whenever a malicious node consumes the bandwidth so that no other legitimate node can use it.

Malicious Node Entering- A malicious node can enter in the network without authentication.
Stale Packets- This means to inject stale packets into the network to create confusion in the network.

Delay- Any malicious node can purposely delay the packet forward to it.

Link Break- This can result in restricting the two legitimate nodes from communicating if the malicious node is between them.

Denying from Sending Message- Any malicious node may deny from sending messages to other legitimate nodes.

Fake Routing- Whether there exists a path between nodes or not, a malicious node can send fake routes to the legitimate nodes in order to get the packets or to disturb the operations. It is necessary to detect the malicious node for secure transmission.

3.2.1 Steps for detecting selfish node

Malicious nodes are the misbehaving nodes in the network environment, which degrades the performance of the network by producing the enormous packet loss.

It is necessary to identify the attacker node, in order to avoid the performance degradation. The malicious node was identified by using the threshold value.

Threshold value is the predefined value which is like setting the limits to avoid the unnecessary packet losses.

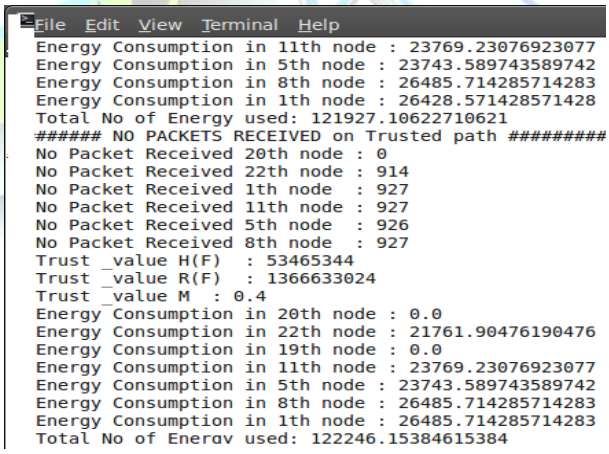
Threshold value is set as 0.3 in this work, so that the node with trust value less than 0.3 is not considered for routing and it is decided by the cluster head.

The node with the less trust value are neglected in order to avoid the packet loss and delay in data transmission which may lead to the low throughput results and increases the control overhead process.

Cluster head plays the vital role in controlling the each of its member activities.

The intruder node was detected by the cluster head and that particular node is not used for the data transmission. The node with less trust value is detected as the malicious node by the cluster head and it is labeled as "detected".

4. Results and Output:



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Fig 2.Trust value calculation

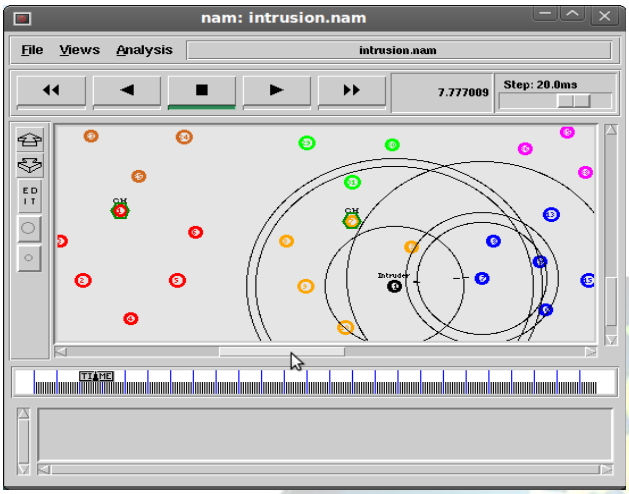


Fig 3.Intruder node 1

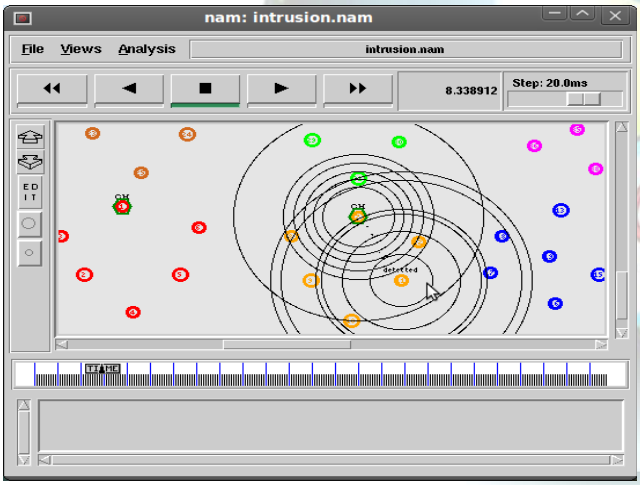


Fig 4. Detection of intruder node

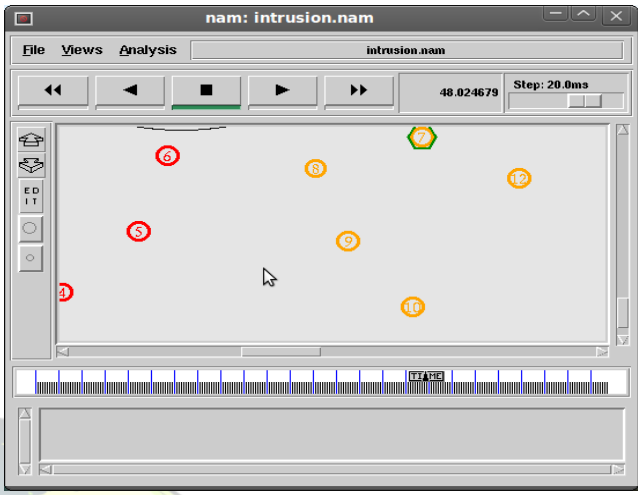


Fig .5 Removal of intruder node

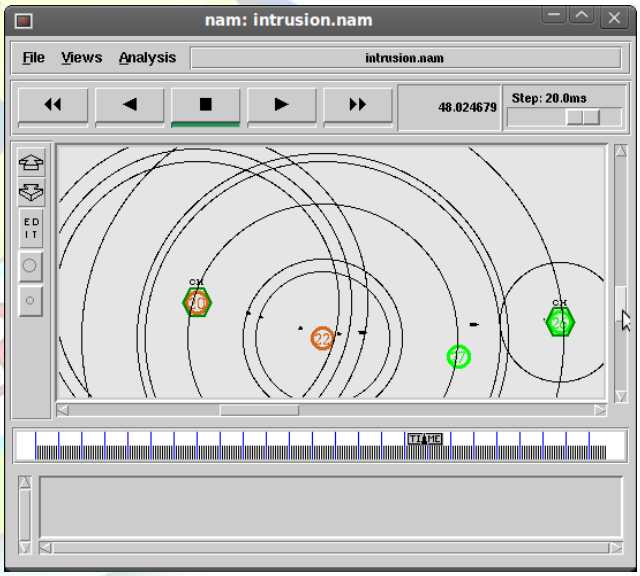


Fig 6.Packet Transmission

5. Conclusion

Trust value and security in a MANET environment focuses on to improve reliability and availability of data to the mobile clients (node). There are many issues revolving around network at the time of transmission in such a scenario like power, server and node mobility, networking partition and frequent disconnection. We propose a trust value calculation for discovering a reliable routing path at the time of transmission and for the selfish node detection for identifying the non cooperative node and also discard the node from the routing path. These proposed scheme helps to improve the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

network performance based on energy, bandwidth and the strength of the signal Thus our scheme solves the mobility prediction as well as overhead problem in mobile database system in a MANET.

6. References

1. Orwat, M.E., Levin, T.E., Irvine, C.E.: An Ontological Approach to Secure MANET Management. In: Proceedings of the 2008 Third International Conference on Availability,

2. Saad, M.I.M., Ahmadnn, Z.: Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol. European Journal of Scientific Research 32(4), 444–454 (2009)

3. Uma, M., Padmavathi, G.: A comparative study and performance evaluation of reactive quality of service routing protocols in Mobile Adhoc networks. Journal of Theoretical and Applied Information Technology 6(2) (2009)

4. Wu, B., Chen, J., Wu, J., Cardei, M.: A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Xiao, Y., Shen, X., Du, D.-Z. (eds.) Wireless/Mobile Network Security. Springer (2006)

5. Huang, Y., Jin, B., Cao, J., Sun, G., Feng, Y.: A Selective Push Algorithm for Cooperative Cache Consistency Maintenance over MANETs. In: Kuo, T.-W., Sha, E., Guo, M., Yang, L.T., Shao, Z. (eds.) EUC 2007. LNCS, vol. 4808, pp. 650–660. Springer, Heidelberg (2007)

6. Gruenwald, L., Banik, S.M.: A Power-Aware Technique to Manage Real-Time Database Transactions in Mobile Ad-Hoc Networks. In: Proceedings of the 12th International Workshop on Database and Expert Systems Applications, pp. 570–574 (2001)

7. Fife, L.D., Gruenwald, L.: Research Issues for Data Communication in Mobile Ad-Hoc Network Database Systems. ACM SIGMOD Record 32(2), 42–47 (2003)

8. Li, J., Li, Y., Thai, M.T., Li, J.: Data Caching and Query Processing in MANETs. JPCC 1(3), 169–178 (2005)

9. Hadim, S., Al-Jaroodi, J., Mohamed, N.: Middleware Issues and Approaches for Mobile Ad hoc Networks. In: Proceeding of IEEE Consumer Communications and Networking Conference (CCNC 2006), Las Vegas, Nevada (January 2006)

10. Artail, H., Safa, H., Pierre, S.: Database Caching in MANETs Based on Separation of Queries and Responses. In: Proceeding of WiMo