A Survey on Trusted Fault Tolerant System in MANET With Data Recovery

Meenakshi Dubey Prof. P.S. Patheja Prof. Vijay Lokhande

Abstract
Date Recovery is an important feature in Mobile ad-hoc network. Communication between the nodes in adhoc network depends the radio range, node mobility as well as intermediate nodes because they communicate with the help of intermediate nodes, that means each mobile node is treated as a route and so arises the problem of data security, different trust methods have been proposed before and have secured the data from dropping and modification as well as capture attack but in our proposed work we are trying to design reputation base trust allocation for the node and if any fault occur in any of the transaction we will try to identify the particular node using some analysis. The implementation model basically focuses on those nodes which do not actively participate in a network. We will be using Location Aided Routing (LAR) protocol for that purpose. Will try to analyze through Network Simulator-2 test based architecture and will try to identify node trust level.

Keywords: AODV, Faulty Node, LAR, Link Fault, Routing Table, Trust, TFT-AODV.

1 INTRODUCTION

Mobile ad hoc networks (MANETs) are basically peer-to-peer multihop mobile wireless networks that have neither fixed communication infrastructure. Due to its ad hoc nature and mobility control is more complicated. Beside Internet, which has dedicated nodes for network operations such as routing, packet sending, and management of network, all these functions must be performed by all mobile nodes themselves in MANETs. Routing the packets efficiently is a primary challenge for MANET.

The current AODV protocol is an on-demand algorithm, as it builds routes between nodes only when desired by source nodes. The routes are maintained only till they are needed by the sources. AODV makes use of sequence numbers for keeping the freshness of routes. A new model is proposed (TFT-AODV) to provide a trusted fault tolerant approach with recovery features for MANET. For providing security, confidential packets are transmitted through nodes with highest trust levels. A link fault, location fault and node behaviors are taken into consideration before transmitting a packet to provide a fault tolerant model. When there is a loss of packet in the network this TFT model recovers this lost packet using a recovery manager.

Ad hoc networking involves computers, typically wireless mobile nodes (MNs) that cooperatively form a network without user administration or configuration. Whether it be a laptop which is acting as a node or a sensor, is in charge of routing information between its neighbors, thus it maintains network connectivity. Several reviews of unicast MANET routing protocols exist, and several performance evaluations have been done. Location information has been applied to MANET protocols in order to improve the performance. of a protocol, enable scalability, or both. The application of location information has demonstrated performance improvements and promised dramatic scalability.

An ad hoc network might consist of devices such as laptops, cellular phones, and so on. Within its transmission range each node will be able to communicate directly with any other node. For communicating with nodes that are residing beyond this range intermediate nodes will be needed to pass on the messages hop by hop.

2 MANET CHALLENGES

Mechanism of Friendship overcomes the path reliability problem in this issue by increasing all

- *Meenakshi Dubey is currently pursuing Master of Technology degree program in Computer Science Eengineering from BIST, Bhopal(RGPV University), India, PH-7775085167. E-mail: meenakshi0786@gmail.com*
- *Prof. P.S. Patheja is currently Head of Deptt.of masters degree program in Computer Science Engineering Deptt. BIST, Bhopal(RGPV University), India PH-9893273243. E-mail: pspatheja@gmail.com*
- *Prof. P.S. Patheja is currently Head of Deptt.of masters degree program BIST, Bhopal(RGPV University), India PH-9893273243. E-mail: pspatheja@gmail.com*
- *Prof. Vijay Lokhande is currently Head of Deptt.of masters degree program in Computer Science Engineering Deptt. BIST, Bhopal(RGPV University), India PH-8871118864. E-mail: vijaylokhande.07@gmail.com*

nodes to become friends before joining a MANET network. These nodes can become friends & can help with each other, because of this mechanism provides a mutual trust between them and when they enter the network, they can vote for each other (those who have become friends) which can increase reputation rating and guarantee reliability of path. So, with the growing number of nodes joining bounded in friends' relationships, the higher number of co-operative nodes can be generated.

2.1 Approaches to solve MANET are as follows:-

Routing: - To increase reputation, develop a mutual trust among nodes and guarantee path reliability.

Security: - For those nodes which are not in the friends' list, avoid nodes to share their Security associations.

Resource Management:- The selective behavior of forwarding (i.e. forward packets only between friends) is not only able to save nodes' resources but also avoid them.

Auto-Configuration:- Providing a secure method to automate MANET multi hop operations.

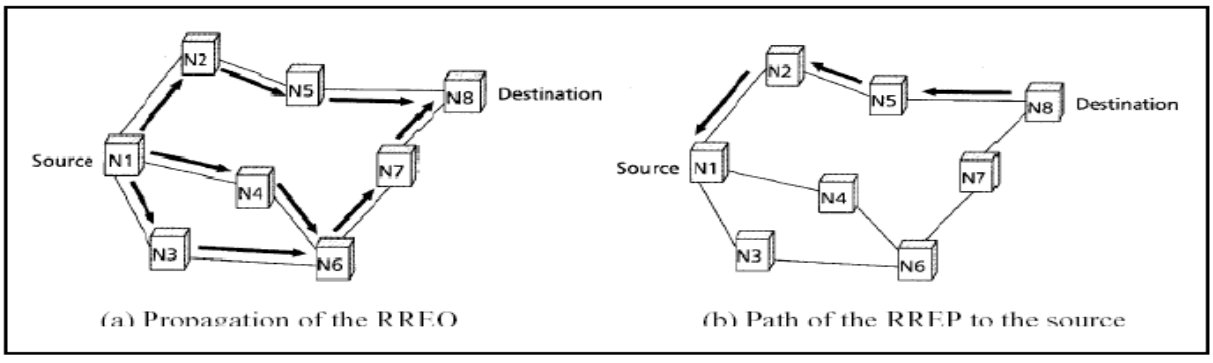
2.2 AODV:

AODV protocol use to build routes using a route request / route reply query. When a route is desired by a source node to a destination for which it is not having a route, it broadcasts a route request (RREQ) packet across the network. Nodes which are receiving this Packet will update their information for the source node and will set up backwards pointers to the source node in the routing tables. In addition to the IP address of source node, current sequence number, and broadcast ID, the RREQ also contains the most latest sequence number for the destination of which the source node is aware of. A node which receives the RREQ can send a route reply (RREP) if it is either the destination or if it has a route to the destination with the corresponding sequence number greater than or equal to that of RREQ. If this is the case, it will unicasts a RREP to the source. Otherwise, it has to rebroadcasts the RREQ. Nodes keep track of the RREQ's broadcast ID & source IP address. If they receive a already processed RREQ, they discard the RREQ and will not forward it.

As the RREP propagates back to the source, nodes will set up their forward pointers towards the destination. It may start forwarding the data packets to the destination once the source node receives the RREP message. If the source receives a RREP later which contains a greater or the same sequence number with a smaller hop-count, then for that destination it may update its routing information and begin using the better route. As long as the route is active, it will be maintained. A active route is one whose data packets are periodically travelling from the source to the destination along that path. Whenever the source stops sending data packets, time out for the links will and eventually be deleted from the routing tables of intermediate nodes. If breaking of a link occurs while the route is active, a route error (RERR) message to the source node to inform it of the current unreachable destination(s)is propagated. After receiving the RERR, if the route is still required for the route, it can reinitiate the route discovery.

Because of the inherent security AODV protocol is chosen. Notice that one of the differences between AODV and DSR is that, DSR requires every packet to carry the routing information, whereas, in AODV, once the route is established, the data packets just carry the flow-ID. So, in DSR, we have to encrypt the routing information in every data packet which is, not impossible, but not desired.

Fig. 2: AODV Route Discovery.



3 BRIEF LITERATURE SURVEY

MANETs generally use multihop routing rather than single-hop routing for the delivery of packets to their destination. In MANET each device is free to move independently in any direction, and therefore will change its links frequently to other devices. Each should forward traffic unrelated to its own use, and therefore act as host & router both. The initial challenge in building a MANET network is equipping every device to maintain the information required to properly route traffic continuously. A factor that affects MANET for providing secured routing of packets is Security, to solve this issue trust based models are developed

3.1 LOCATION-AIDED ROUTING

Mobile ad hoc networks consist of wireless mobile hosts that in the absence of a fix infrastructure communicate with each other. In a Mobile Ad hoc NETwork (MANET) routes between two hosts may consist of hops through other hosts in the network . Mobility of Host can cause unpredictable and frequent topology changes. Therefore, finding and maintaining task of routes in MANET is non trivial. So with the goal of achieving efficient routing many protocols have been proposed. The approach of these algorithms differ as used for searching a new route and/or modification of a known route, when hosts move.

3.2 TRUSTED FAULT TOLERANCE LOCATION AIDED ROUTING (TFT-LAR)

The current LAR protocols for MANET deals with a node's mobility as it is unpredictable due to its random mobility. In order to monitor these changes a Distance Update Threshold (DUT) is used or a map is created to get the location information iteratively . Security is a factor that affects MANET for providing secured routing of packets, to solve this issue trust based models are developed . The nodes in an ad hoc network may have varying mobility which might be low or high, to deal with this various protocols (LAR and Directed flooding method) are combined.

When all these issues are considered, a new model is proposed (TFT-LAR) to provide a trusted fault tolerant approach with recovery features for MANET. For providing security, confidential packets are transmitted through nodes with highest trust levels. A link fault, location fault and node behaviors are taken into consideration before transmitting a packet to provide a fault tolerant model. When there is a loss of packet in the network this TFT model recovers this lost packet using a recovery manager.

3.3 TFT MODEL WITH DATA RECOVERY

A TFT-LAR for Mobile Ad Hoc network is an interconnection of a number of mobile nodes having various properties. There will be a source, a destination and intermediate nodes through which the packets get transmitted, during this transmission the nodes may have many faults or defects due to link, node failure and due to its variable location, all these faults make the node to misbehave . When there is a defect in the node's behavior alternate nodes are selected, and the contents of those misbehaved nodes are loaded onto a recovery manager. At the beginning, the message is transmitted from the source node.

The minimum distance and the directions of sending the packets are obtained using the location information Feature. These trust levels are made use for sending a confidential message as only the nodes with the highest trust levels are selected for transmission. The work considers six levels of confidentiality; they are ordinary, important, confidential, very confidential, one-one confidential, group confidential. For an ordinary message trust levels are not used, for a confidential message node with high trust levels are utilized and for very confidential message nodes with highest trust levels are utilized.

The proposed TFT model is compared with the existing LAR models and it is possible to recover the lost packets from the recovery manager in this model. The compliance with the existing packet format is also checked after having added an

additional octet for the confidentiality levels. The TFT mobile ad-hoc network model can be improvised by optimizing the code and limiting the direction of search for shortest distance with high mobility. The trust level of the node is made to increase if the packet transmission is successful through them and it is decreasing due to their misbehaviors or unreachable locations.

4 WORK ACCOMPLISHED SO FAR

Researchers are continuously working on MANET with data recovery and the numbers of techniques are proposed by the research community. Few of them are described here:-

Chandrasekaran S et al.[3] propose a Trusted Fault Tolerant model incorporate user data recovery features in mobile Ad Hoc network using Location Aided Routing (LAR) protocol. The LAR protocol in MANET is challenged by a complicated interaction of congestion, contention, and mobility. Link Faults are covered by the fault model addressed here that occur in the packet transmission due to the high mobility of the nodes and the congestion of node occurs when there is no storage capacity for the buffers at the nodes to hold the incoming packets. When the node moves away from the source to an unreachable location after having received the packets the location fault occurs. There implementation model focuses on nodes which do not actively participate in a network that are considered as selfish or misbehaving nodes. There performance of the model is improvised using location awareness feature and node trust levels based on which the recovery of the lost packets is achieved. But they only focus data recovery level in future incorporate with trust and un-trust node identification and manage the trust threshold and prevent through data distortion from un-trusted nodes.

Jiejun Kong et al. proposed A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks [6]. In this work researcher propose a feasible adversary model of such attacks, several instantiations are then presented and study the principles of designing corresponding countermeasures, they conclude that ad hoc networks deployed in hostile environments need new countermeasures to resist such passive attacks. Passive routing attacker watch the data incoming and outgoing information and can't modified data packets its utilized that information in future scope, passive attack more risk than active attack.

Gabriel Ghinita, Mehdi Azarmi et. al. in his work titled "Privacy-Aware Location-Aided Routing in Mobile Ad Hoc Networks" [7] investigates protocols that support MANET routing without disclosing exact positions of nodes. In his work each node defines its own privacy profile, and reports masked location information to its neighbors. His proposal adopts a novel strategy for advertising beacons, to prevent inference of node locations. They also propose packet forwarding heuristics that rely on cloaking regions, rather than point locations. Through that technique we protect the node from denial of service and cannot identifies personal node information like node mobility, direction and locality.

Amrit Suman et al. proposed Behavioural Study of Wormhole Attack in Routing for MANET [8]. They present an analysis of three routing protocols within wireless network where wormhole attack is occurred. By different analysis it can be observed that AODV performs better than other two protocols. AODV has better techniques to prevent data from attacks, future we elaborate denser mobility environment and protect the data from hazard.

Wang, Miao et al. provide the mathematical model to identify the trust values and formalizes the generic framework of trust mechanisms in a probabilistic manner, gives the mathematical description for Peer Trust-like trust mechanisms, it attempts to figure out some unclear questions, based on Peer Trust-like schemes we compute similarity via Euclidean distance, it should all feedback be counted in and compare Peer Trust-like mechanisms with other distance similarity computations [9].

Xiaodong Wang et al. present a trustworthiness evaluation model based on Bayesian network. Here they computed node's trustworthiness in the form of direct and indirect trustworthiness. Researcher apply Bayesian network to compute online duration of nodes, link speed of nodes, routing forwarding ratio and energy as four

entities to compute direct trustworthiness. And other side indirect trustworthiness is archived by node's single-hop neighbor's collaboration. Their proposed model allows dynamic evaluation policy. And their outcome obtains dynamically precious and sensitive fixable trustworthiness timely using simulation tool [10].

Shishir K. Shandilya et al. [11] proposed flooding attack detection and prevention model that is distributed cooperative model in which all the node locally run the intrusion detection code and cooperate with each other to detect and prevent flooding attack in the network. Their work they have used the Dynamic Source Routing (DSR) routing protocol along with the trust estimation function. Because the communication between the nodes in the MANET depends on the cooperation and the trust level on its neighbors so to calculate the trust level we have used the trust estimation function in the Route discovery phase of the basic DSR routing protocol which will calculate the trust level of each neighboring node. Various parameters they have used for trust estimation are: Total number of RREQ packet sent by the neighbor in per unit of time, then the total number of packet successfully transmitted by the neighbor, and Ratio of number of packet received correctly from the neighbor to the total number of received packet.

Yuanyuan Jin, Laizhong Cui et al. [12] they describe about trust calculation, they design trust management system on the bases of reputation-based trust research is the main stream direction in this area. This kind of trust is based on the user's direct experience or indirectly interaction experience to get another user's trust. According their architecture structure, reputation system can be divided into two types: centralized reputation system; distributed reputation system, both the technique applies for trust calculation in any environment.

5 PROBLEM FORMULATION: SIGNIFICANCE AND NEED OF PROPOSED RESEARCH WORK

A AODV-LAR Trust and Non Trust for Mobile Ad Hoc network is an interconnection of a number of mobile nodes having various properties. There will be a source, a destination and intermediate nodes through which the packets get transmitted, during this transmission the nodes may have many faults or defects due to link, node failure and due to its variable location, all these faults make the node to misbehave. When there is a defect in the node's behavior alternate nodes are selected, and the contents of those misbehaved nodes are loaded onto a recovery manager. At the beginning, the message is transmitted from the source node. The minimum distance and the directions of sending the packets are obtained using the location information feature .The nodes which are at the shortest distance from the source node are selected. The trusted fault tolerant model of mobile ad-hoc network is proposed with the user recovery feature.

The link faults that occur in the packet transmission due to the high mobility of the nodes is covered by the fault model addressed here and congestion of node occurs when there is no storage capacity for the buffers at the nodes to hold the incoming packets. When the node moves away from the source to an unreachable location after having received the packets the location fault occurs. Our implementation model will focus on the nodes which do not actively participate in a network that are considered as selfish or misbehaving nodes. The performance of the model can be improvised using location awareness feature and node trust levels based on which the recovery of the lost packets is achieved.

6 PROPOSED METHODOLOGY /PLANNING OF WORK

- Next work is to extend our routing capability for migrating services from one device to another in the network as an efficient fault-tolerant mechanism in the pervasive world of network.
- The TFT mobile ad-hoc network model can be improvised by optimizing the code and limiting the direction of search for shortest distance with high mobility. The proposed TFT model is compared with the existing LAR and AODV models and it is possible to recover the lost packets from the recovery manager in this model.
- It can be implemented either using ns2 or GloMoSim simulators.

7 EXPECTED OUTCOME OF THE PROPOSED WORK

The TFT mobile ad-hoc network model can be improvised by optimizing the code and limiting the direction of search for shortest distance with high mobility. The trust level of the node is made to increase if the packet transmission is successful through them and it is decreasing due to their misbehaviors or unreachable locations. Next work is to extend our routing capability for migrating services from one device to another in the network as an efficient fault-tolerant mechanism in the pervasive world of network.

Following are the in expected outcome in brief:

1. Improve packet drop rate due to selfish node.
2. Optimize the code.
3. Using both LAR and AODV protocol for both Trusted and Untrusted Systems.

8 REFERENCES

[1] **Lidong Zhou and Zygmunt J**. HaasHappy sankranti/pongalhttp://crackspider.net/ "Securing Ad Hoc Networks "In Proc IEEE , special issue on network security, November/December, 1999.

[2] **Marjan Kuchaki Rafsanjani, Ali Movaghar, and Faroukh Koroupi**" Investigating Intrusion Detection Systems in MANET and Comparing IDSs for Detecting Misbehaving Nodes" World Academy of Science, Engineering and Technology 44 2008

[3] **Chandrasekaran S and Shanmugam Udhayakumar** "Trusted Fault Tolerant Model of MANET with Data Recovery" IEEE computer Society, 978-0-7695-4543-1/2011 IEEE, DOI 10.1109/ICINIS.2011.67

[4] **S. Mash,** "Fonnalizing trust as a computational concept," PhD Thesis, 1994

[5] **Grandison T,Sloman M**,"A survey of trust in internet applications", IEEE Communications Surveys, 2000.

[6] **Jiejun Kong, Xiaoyan Hong, Mario Gerla** "A New Set Of Passive Routing Attacks In Mobile Ad Hoc Networks" This Work Is Funded By Minuteman Project And Related STTR Project Of Office Of Naval Research

[7] **Gabriel Ghinita, Mehdi Azarmi** et. al. "Privacy-Aware Location-Aided Routing in Mobile Ad Hoc Networks" Eleventh International Conference on Mobile Data Management 2010 IEEE DOI 10.1109/MDM.2010.47