Research Paper
Impact Factor: 4.164
Refereed Journal

IJMDRR
E- ISSN –2395-1885
ISSN -2395-1877

TRUST BASED ON DEMAND MULTIPATH ROUTING IN MOBILE AD-HOC NETWORKS

Mr. Shiv Kumar Dwivedi
Assistant Professor of Computer Science ,Shri Agrasen Girls College, Korba,Chhattisgarh.

Abstract
A Mobile Ad hoc Network (MANET) is a self-organized system comprised of mobile wireless nodes with peer relationships. Due to multi-hop routing and absence of any trusted third party in open environment, MANETs are vulnerable to attacks by malicious nodes. In order to decrease the hazards from malicious nodes, we introduce the concept of trust to MANETs and build a simple trust model to evaluate neighbours' behaviours - packet forwarding. Extended from AODV route protocol, a trust-based reactive multipath routing protocol for MANETs, termed as Ad hoc On-demand Trusted-path Distance Vector (AOTDV) is proposed. This protocol discovers multiple loop-free paths which are evaluated by hop count and trust. The two-dimensional evaluation provides a flexible and feasible approach to choose a shortest path in all trusted paths to meet the dependable or trust requirements of data packets. Performance comparison of AOTDV and other related routing protocols shows that AOTDV is able to achieve a remarkable improvement in packet delivery ratio and end-to-end delay and to reduce black-hole, gray-hole and modification attacks.

Keywords: - Trust, honest values, security, attacks, AODV, Security, Trusted AODV, MANET.

Introduction

A Mobile ad hoc network is an infrastructure fewer networks self-possessed of wireless network nodes. These nodes are self configurable and dynamically setup the paths among themselves to transmit packet. In a MANET, each node act as router and the connectivity is achieved using multihop communication between nodes where any wire- less node can join and leave the network at an instant of time. Several routing protocols have been proposed by various researchers such as DSR [13], DSDV [14] and AODV [8] etc. but they did not consider any security issues. These protocols can be categorized into two main types: proactive and reactive [4]. Proactive protocol depends on the routing tables which are maintained at each node whereas reactive protocol finds a route to a destination on demand, whenever communication is needed. Ad hoc on demand distance vector (AODV) is reactive routing protocol proposed by C. Perkins [11] which is very efficient in terms of performance and widely used protocol so far. AODV is on demand routing protocol where routes are only established when needed and it belongs to the class of distance vector. In distance vector every node knows its neighbors and costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance is set to infinity. Every node sends the whole routing table to its neighbors, so they can check if there is another useful or shortest route to another node using this neighbor as next hop. When a link gets breaks, count-to-infinity problem could arise. The count- To-Infinity [11] and loop problem is solved with the sequence number concept. Security in MANET is a major aspect in terms of packet forwarding and routing. The dynamic nature of mobile ad hoc networks makes it more susceptible to various types of attacks. Attacks in mobile ad hoc networks can be classified into two main categories: passive attack and active attack [7]. In Passive attack the attacker snoops the data exchanged in the network without altering it or disrupts the operation of the network. Detection of a passive attack is very difficult for the operation of the network itself does not get affected. An active attack attempts to alter or destroy the data being exchanged in the network and it disrupts the normal operation of the network. Further active attacks can be classified into two categories: external attacks and internal attacks [7]. External attacks are carried out by the nodes that do not belong to the network and internal attacks are carried out by compromised nodes that are actually part of the network. Internal attacks are more severe and difficult to detect when compared to external attacks. Wormhole, Black hole, DOS attack etc. comes under the category of internal attacks. Routing algorithm needs mutual trust between nodes for secure communication.

Routing Protocols

Ad-hoc On-Demand Distance Vector Routing (AODV)

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol builds on the DSDV algorithm previously described. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts by creating routes on an on-demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, as nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a Path Discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbours, which then forward the request to their neighbours, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located. AODV utilizes destination sequence numbers to ensure all routes are loop-free and contain the most recent route information. Each node maintains its own

sequence number, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies a RREQ. Along with its own sequence number and the broadcast ID, the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ. During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbour from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by unicasting a route reply (RREP) packet back to the neighbour from which it first received the RREQ. As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of symmetric links. Routes are maintained as follows. If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbour notices the move and propagates a link failure notification message (a RREP with infinite metric) to each of its active upstream neighbours to inform them of the erasure of that part of the route. These nodes in turn propagate the link failure notification to their upstream neighbours, and so on until the source node is reached. The source node may then choose to reinitiate route discovery for that destination if a route is still desired.

Dynamic Source Routing (DSR)

Dynamic source routing (DSR) is based on source routing where the source specifies the complete path to the destination in the packet header. All intermediary nodes along the path simply forwards the packet to the next node as specified in the packet header. This means that intermediate nodes only need to keep track of their neighbouring nodes to forward data packets. The source on the other hand, needs to know the complete hop sequence to the destination. This eliminates the need for maintaining latest routing information by the intermediate nodes as in DSDV. In DSR, all nodes in a network cache the latest routing information. When more than one route to the destination is found, the nodes cache all the route information so that in case of a route failure, the source node can look up their cache for other possible routes to the destination. If an alternative route is found, the source node uses that route; else the source node will initiate route discovery operations to determine possible routes to the destination. During route discovery operation, the source node floods the network with query packets. Only the destination or a node which already knows the route to destination can reply to it, hence avoiding the further propagation of query packets from it. If a broken link is detected by a node, it sends route error messages to the source node. The source node on receiving error messages will initiate route discovery operations. Unlike DSDV, there are no periodically triggered route updates.

Trust Model

It is clear trust relationship involves two entities (subject and object) and a specific action. The uncertainty of trust exists because subject is not sure whether the object will carry out the action or not. One of the earliest literatures about computational trust is Marsh's Formalism that uses the outcomes of direct interactions among entities to compute situational and general trust. Situational trust is the level of trust in another for a specific situation, while general trust means overall trust worthiness in spite of the situation. Several trust models have been developed for trust management. These models can be classified into two groups; centralized models and decentralized models. In centralized models, trust values are maintained in common central nodes or through an authorized third party. The simplest method is to sum the number of positive ratings and negative ones separately and keep a total score which equals to the positive score minus the negative score. This method is used in eBay's reputation forum. The requirement of a trusted third party goes against the nature of MANETs.

In decentralized models, a node assigns a trust /trust/worthiness value for every communicated node. Most researchers are advocating the use of rating and prefer to complex rating aggregation algorithms to evaluate from several aspects and filter out the bad rating. However, these sophisticated models are not appropriate for MANETs where resources are scarce and network topology is dynamic. Several trust models have been developed for peer –to-peer systems based on sharing recommendation information to establish reputation. Although in n principle these models could be applied to routing in MANETs, additional recommendation information exchanging incurs significant networks overhead.

Existing Work

In based paper, to introduce a simple trust model based on packet forwarding ratio to evaluate neighbors' behaviours, and propose a novel multipath reactive routing protocol for MANETs, termed as Ad hoc On-demand Trusted-path Distance Vector (AOTDV). In a route discovery, this protocol is able to create multiple loop-free paths between a source and a destination through hop-by-hop route. Each route has a cost vector composed of hop count and trust value. Furthermore, this protocol

provides a flexible and feasible approach to choose a shortest path in all trusted paths to meet the dependable or trust requirements of data packets. Performance comparison of AOTDV and two related routing protocols shows that AOTDV is able to achieve a remarkable improvement in the packet delivery ratio and alleviate most malicious attacks.

The proposed routing protocol is practical to enhance the dependability of routing and to detect malicious nodes in MANETs. In particular, the main contributions of our work can be summarized as follows:

1. Based on packet forwarding ratio, a simple and practical trust model is created to evaluate the behaviours of route nodes.
2. An on-demand multipath routing protocol (AOTDV) is proposed for MANET, in which top *k* shortest path and trustiest path are formed during one route discovery.
3. QoS-aware packet forwarding is established to satisfy user-specific requirements for dependability. Accordingly an adaptive mechanism is proposed to select a forward path dynamically in terms of the trust requirement of one packet.
4. We evaluate the AOTDV protocol and present experimental results in NS-2 simulator. It is shown that AOTDV is dependable to route packets and alleviate the attacks of malicious nodes in MANETs.

Existing Routing Problems

1. **Asymmetric links:** Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network. For example consider a MANET(Mobile Ad-hoc Network) where node B sends a signal to node A but this does not tell anything about the quality of the connection in the reverse direction.
2. **Routing Overhead:** In wireless ad-hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.
3. **Interference:** This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.
4. **Dynamic Topology:** This is also the major problem with ad-hoc routing since the topology is not constant. The mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted, i.e. fixed network routing table updating takes place for every 30sec . This updating frequency might be very low for ad-hoc networks.

Proposed Methodology

Trust Derivation

No Matter what kind of trust models, two types of evolution, direct trust and indirect trust, are available. Direct trust is first-hand information for neighbours and easy to obtain. In order to simplify trust model, we only\y use the history of direct interaction among nodes to compute trust.

Packet Forwarding Ratio (FR) is the proportion of packets which have actually been forwarded correctly. Correct forwarding means the forwarding node not only transmits the packet to his next hop node but also forwards devotedly. For instance, a malicious neighbour node forwards the data packet after tampering with data. If the sender monitors this illegal modification, The FR of the neighbour will decrease. Let NC (t) represents the cumulative count of correct forwarding and NA (t) signify the total count of all requesting before time t. The count of correct forwarding in a time window (from time it-w to it) is equal to NC (it) - NC (it-w), where w represents the length of the time window. Let FR (it) be packet forwarding ratio in the window. FR (it) is defined as follows:

$$FR(t) = \begin{cases} N_c(t_i) - N_c(i_t - w), & t_{i>w} \\ \hline N_A(t\,i) - N_A(it-w), & t_i \leq w \end{cases} \quad (1)$$

Where i=1, 2, 3,.... Assume that the difference d of ti+1−ti (i>1) is fixed. FR (it) is calculated at a fixed interval of d units of time. The constant d, termed Trust Update Interval, is a very critical component of a trust model and determines the time a node should wait before updating a trust value to its neighbour. Forwarding records in recent w units of time are considered and the history records out of recent window fade as time goes by.

Proposed Methodology

In this section, we present new and best trust based network routing factors will be including for **"Trust Based on Demand Multipath Routing in Mobile Ad-Hoc Networks"**.

Modified Routing Aodv Algorithm

As an attempt to further improve performance of MANET, we further modify the functionality of node receiving RREP in R-AODV. Fig. compares the route discovery processes of R-AODV and Modified R-AODV (MR-AODV or HAODV) in presence of a malicious node. As shown in Fig. (a), when a malicious node is detected by an intermediate node after receiving RREP, R-AODV marks the RREP as DO_NOT_CONSIDER and marks the node sending RREP as MALICIOUS_NODE in the routing table; the RREP is then forwarded on the reverse path to the source which updates routing tables of all the nodes on the reverse path with malicious node entry; a route towards destination is chosen by selecting unmarked RREPs.

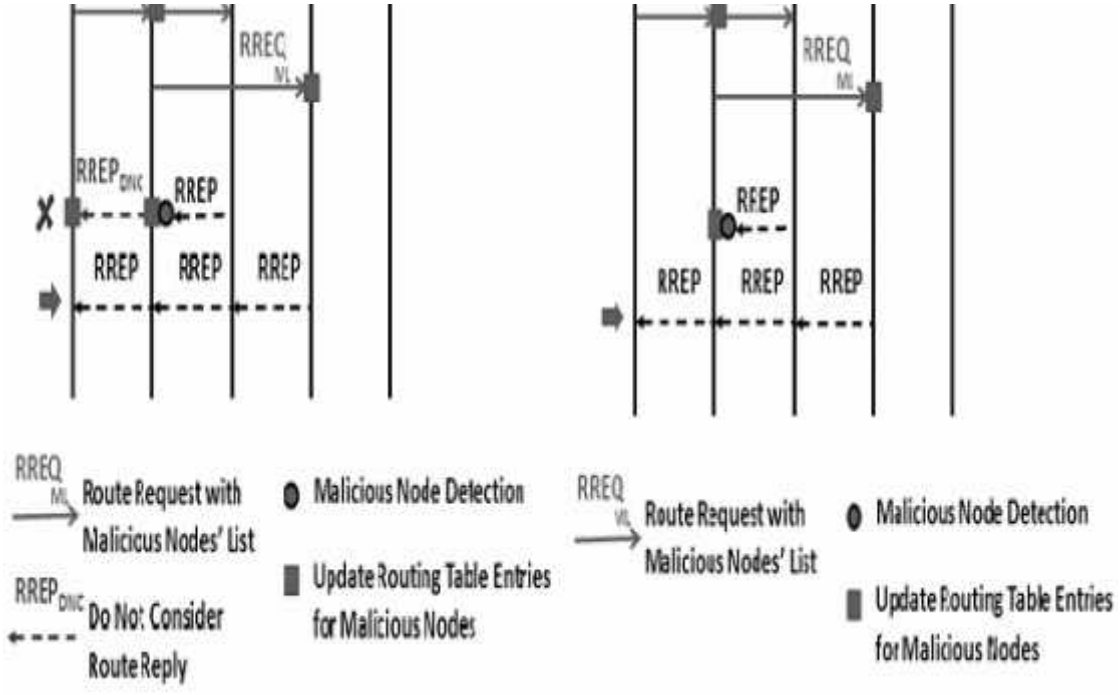

Fig. (a) Fig. (b)

Figure 4.3: Comparison of route discovery processes of R-AODV and MR-AODV under attack

On the other hand, in MR-AODV, when a node detects a malicious node, it updates the routing table with malicious node entry and discards the RREP as shown in Fig. (b); it is neither forwarded on the reverse path nor requires a DO_NOT_CONSIDER flag; thus, all RREPs reaching to the source node will be sent by genuine nodes only; the RREP indicating shortest fresher path will be chosen for data transmission by the source node. Thus, MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehavior.

For using MR-AODV we find out trust value of node. The following formula is use for evaluating the trust value:

Peak = node_count[int(index)] + rpcount + peak + sque;

[PEAK VALUE = (REPLY PACKET + PREVIOUS PEAK VALUE + SEQUENCE NUMBER OF PACKETS).
Here, PEAK VALUE is a variable identified the Trust Value.
REPLY PACKET is a variable identified the reply or response by destination node.
SEQUENCE NO.OF PACKETS is identified the sequence of packets which travels between the multiple nodes.]

route_node[int(index)] = 1;

[Here, int[index] is an size of an array which is count the send request(RREQ) by nodes]

```
printf("Peak Value Obtained by : %d \n",peak);
int val = rt->rt_seqno - peak;
if(val > 10)
{printf("\t\t\t\t\t\t\tRoute not Detected \n \t\t\t\t\t\t\tStop The Simulation");}
else
{printf("\t\t\t\t\t\t\t Route Detected \n");}
```

Conclusion & Future Work

In this paper we have proposed an algorithm and named it DAODV. This algorithm detects Balck-hole MANETs. This algorithm works in proactive as well as reactive manner. Our proposed mechanism is capable of handling Black-Holes which already exist and those which occur during transmission. It works equally fine for cooperative Black-holes, where many other algorithm fails. Although there will be overhead of running initial method and maintaining log at the intermediate nodes for transmitting and dropping packets. It is better from other detection and avoidance algorithm in the sense that most of them use complex heavy calculations of encryption and decryption. But this algorithm will not be able to handle cooperative Black-Holes after the initial method has completed. In the future work we will enhance DAODV for the above said problem to resist cooperate Black –Hole attack at any stage and we will also try to verify and validate this algorithm on a standard simulator.

This protocol provides a flexible and feasible approach to choose a shortest path in all trusted paths to meet the dependable or trust requirements of data packets. Multiple paths can also be used to balance load by forwarding data packets on multiple paths at same time. Performance comparison of AOTDV, AODV and AOMDV routing protocols shows that AOTDV is able to achieve a remarkable improvement in the packet delivery ratio and prevent most malicious attacks. For future work, we plan to extend our trust model to other ad hoc network routing protocols like DSR, DSDV and TORA. We will also conduct a comprehensive performance evaluation to compare AOTDV with other trust-based routing protocols.

References

1. Tameem Eissa & Shukor Abdul Razak & Rashid Hafeez Khokhar & Normalia Samian, " Trust-Based Routing Mechanism in MANET: Design and Implementation" , Springer.Science, 2011.
2. Watchara and Sakuna ,"CAODV: Free Blackhole Attack in Ad Hoc Networks", International Conference on Computer Networks and Communication Systems, IPCSIT vol-35, 2012.
3. Jin-Hee Cho, Ananthram Swami, Ing-Ray Chen ," A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, 2011.
4. NaghamH. Saeed, MaysamF. Abbod, and Hamed S. Al- Raweshidy ," MANET Routing Protocols Taxonomy", International Conference on Future Communication Networks 2012.
5. Manel Guerrero Zapata ," Secure Ad hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, Volume 6, Number 3, 2006.
6. S.A.Razak, S.M.Furnell,P.J.Brooke ,"Attack against Mobile Ad Hoc Networks Routing Protocols", Network Research Group ,University of Plymouth, 2009.
7. C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile Computer Systems and Applications, 1999.
8. Poonam Gera, Kumkum Garg, Manoj Misra ," Trust Based Multi-Path Routing for End to End Secure Data Delivery in MANETs", ACM 978-1-4503-0234-0/10/09, 2010.
9. Rajiv K. Nekkanti, Chung-wei Lee, "Trust Based Adaptive On Demand Ad Hoc Routing Protocol", ACMSE, Huntsville, Alabama, USA, 2004.
10. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay ," Different Types of Attacks on Integrated MANET-Internet Communication ",International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), 2005.
11. Charles E. Perkins and Pravin Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers", ACM SIGCOMM 94,1994.
12. Yogendra Kumar Jain, Pankaj Sharma "Trust based Ad hoc On-demand Distance Vector for MANET" National Conference on Security Issues in Network Technologies (NCSI-2012).
13. Dr. S.S.Dhenakaram, A.Parvathavarthini , An Overview of Routing Protocols in Mobile Ad-Hoc Network,2012.
14. Resnick, P. and Zeckhauser, R.:'Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation.