Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 11 (22): 3744-3749, 2011
ISSN 1812-5654 / DOI: 10.3923/jas.2011.3744.3749

Path Selection Technique for Highly Transmission Ratio and Reliable Routing in Manet

[1]H. Sh. Jassim, [2]S. Yussof, [1]S.K. Tiong, [1]K.H. Chong and [1]S.P. Koh
[1]College of Engineering,
[2]College of Information Technology, University Tenaga Nasional, KM7,
Jalan Uniten-Ikram, 43000 Kajang, Selangor, Malaysia

Abstract: Mobile ad-hoc network (MANET) is collection of wireless nodes that operates without using a centralized network infrastructure such as a base station. Since the wireless range is limited, the nodes mutually cooperate with their neighbors in order to extend the overall communication range of the network for forwarding packets. Ad-hoc On-demand Distance Vector (AODV) is one of the commonly used protocols in ad-hoc networks. AODV is a dynamic routing protocol that is able to find the shortest path from a source node to a destination node in MANET based on hop count. However, due to the nature of MANET, it is very easy to introduce malicious nodes in MANET. These malicious nodes may try to compromise the routing protocol functionality and make MANET vulnerable to security attacks which lead to unreliable routing. Therefore, security has become a primary concern in providing protected communication among nodes in MANET. In this study, we propose a Reliable Dynamic Trust-based Routing (RDTR) protocol by integrating a trust mechanism with a shortest path routing algorithm for establishing and maintaining trustworthy routes in MANET.

Key words: Routing protocol, trust, short, reliability, path selection and updating

INTRODUCTION

Mobile ad-hoc network (MANET) is a peer-to-peer wireless network which does not have a fixed infrastructure or a centralized controller. It is a dynamic network where links can be formed and broken dynamically due to mobility. Since there is no centralized controller, each node in MANET relies on each other for forwarding packets. Therefore, there is a need to use a routing protocol which relies on cooperation between nodes to forward packets from hop to hop to reach a specified destination. Examples of routing protocols used in MANET are Ad-hoc On-demand Distance Vector (AODV) Destination Sequenced Distance Vector (DSDV) (Khan *et al*., 2008), Dynamic Source Routing (DSR) (Johnson *et al*., 2007), The Optimized Link State Routing protocol (OLSR) (Kumar and Sengupta, 2010) and Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol (Jing *et al*., 2006).

All communications between nodes pass through several intermediate nodes where each intermediate node performs the functions of a router. However, the lack of cooperation due to misbehavior caused by malicious or selfish nodes may severely disturb or ruin the performance of the network.

Previous studies have developed many solutions designed for establishing trusted relationships between nodes in static networks (Sloman *et al*., 2001). Other researchers have developed solutions designed around dynamic broadcasting or multicasting problems (Cheng and Yang, 2010). However, not many of them address to the security threats in routing protocols. At this point, researches have not fully addressed the performance issues that may arise if trust is incorporated into the routing protocol.

This study proposes an implementation of trust mechanism incorporated in the Ad Hoc On-demand Distance Vector routing protocol (AODV) in order to establish trusted relationship among nodes. This mechanism works in parallel with the idea of calculating the hop counts in order to find the shortest path in AODV routing protocols. Thus, the proposed method will provide a short, trustworthy path for MANET nodes to transfer data.

AODV is a famous reactive (on-demand), hop-by-hop, single-path routing protocol. Like most of routing protocols, it is based on two main mechanisms which are route discovery and maintenance. Route discovery in AODV starts with the broadcasting of the Route Request (RREQ) message by the source node which contains its ID and the destination node's ID to all its neighbors. All neighbors that receive this particular RREQ message for the first time then rebroadcast it after storing the ID of the sender. The sender's ID is used to store the reverse path

Corresponding Author: H. Sh. Jassim, College of Engineering, University Tenaga Nasional, KM7, Jalan Uniten-Ikram, 43000 Kajang, Selangor, Malaysia

to the source. The route discovery process ends when the destination node receives the RREQ message where it would response by sending a Route Reply (RREP) message back to source node. RREP uses the reverse path to the source which is already maintained by the intermediate nodes. Being a single-path routing protocol, AODV only keeps a single path for any destination. In case of the route failure, the protocol needs to initiate another route discovery procedure which may put a massive load on the network. Having only a single route to a destination node increases the probability of a malicious node existence in the discovered path (Cheng and Yang, 2010).

Trust Ad Hoc On-demand Distance Vector (TAODV) (Li *et al*., 2004) uses trust metrics to allow for better routing decisions and penalize uncooperative nodes. For example, node N1 can judge whether the other node N2 could be trusted according to the trust value that N1 obtains about N2. Based on the trust level, N1 can decide whether to go on communicating with N2 or get N2 to prove itself. N1 can also obtain a more credible trust value of N2 by exchanging values with other nodes and calculating the new trust value of N2. In this way, we can achieve real self-organized trust relationships among all the nodes. In TAODV, the routing middies and routing table of AODV has been extend with trust information which can be updated directly through monitoring in the neighbourhood. In TAODV, the new path will be selected based on trust value only. This means that the hop count or the shortest path criteria is not considered.

Many trust models have been implemented in networking. This article will focus on Direct and Recommended Trust Model only. In this kind of trust model the semantics of direct trust values is different from that of recommended trust values. Yahalom *et al*. (1993) found that when doing authentication in open networks an entity often requires other entities' recommendations. These entities can be viewed as Authentication Servers (AS). This trust model is to prevent contradicting or malicious recommendations from different authentication servers. Thus, it is necessary to provide a mean of estimating the trustworthiness of an AS. This trust model divides trust relationships into two types: direct trust and recommended trust. It introduces trust values to substantiate the trust and then derive new trust value from existing ones. Different trust values can be combined together to evaluate the trustworthiness of an entity. Direct trust means that node *A* can trust another node directly using all the existing experiences in *A* about that node. The recommended trust in this trust model often comes along a path. This is effective when the one-hop trust value has been known (Jassim *et al*., 2009).

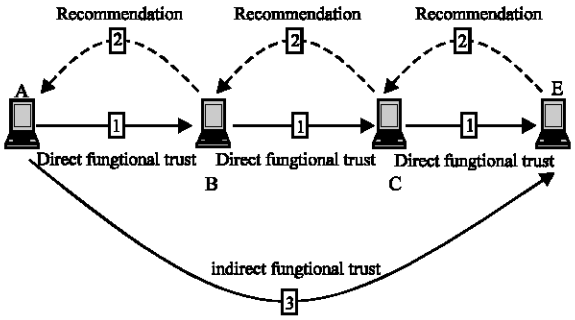

Fig. 1: Direct and recommendation trust

Figure 1 illustrates an example of direct and recommended trust. When node A wants to send information to node E, node A needs to authenticate node E since node A does not have direct trust with node E. In this case, node A will ask other nodes' recommendations. Node B who has direct trust for node E, can recommend node E to node A which has direct trust for node B. As a result, Node A can trust node E based on the recommendation reply from node B.

Chuanhe *et al*. (2007) introduced a trusted routing protocol for mobile ad hoc networks; called Dynamic Mutual Trust based Routing protocol (DMTR). In DMTR, trust among nodes is represented by trust score which consists of direct trust score and indirect trust score. Trust updating and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. Path selection is based on trust score of the path. DMTR assumes that the network layer is based on DSR. This study has not been applied or optimize for on demand routing protocols such as (AODV or DSDV).

NETWORK MODEL AND ASSUMPTIONS

To evaluate the proposed approach in a MANET with malicious nodes, we provide a misbehaving model for the simulation. The misbehavior that we are focusing on in our simulation is the no forwarding behaviors which commonly occur in MANETs due to either internal attackers or malfunction nodes. No forwarding means that a node participates in a wireless network but does not forward any routing messages, such as ROUTE REQUEST and ROUTE REPLY messages. The node may also perform normal routing operations but silently drop certain data packets. This simulation varies the number of misbehaving nodes from 0 to 20 nodes out of 50 nodes so that the maximum percentage of misbehaving nodes in the simulated network is 40% which is an extremely high ratio in real network environment. These nodes are chosen randomly by Tcl's (Welch *et al*., 2003) built-in

pseudo-random number generator and the chosen nodes will keep dropping routing packets or data packets for a period of 900 seconds. This work assumes that there is a watchdog system for monitoring the misbehaviour of nodes.

The MANET topology is modelled as a dynamic topology with unfixed geographical region, Gi (Vi, Ei), where Vi represents the set of wireless nodes (i.e., routers) and Ei represents the set of communication links connecting two neighboring routers falling into the radio transmission range.

The notations that are used in this paper can be summarized as follows:

Gi (Vi, Ei) = The MANET topology graph
s = The source node of the broadcast request
D = {d 0,d 1,...dm}, the set of destinations of the broadcast request
PTi (s, dj) = A path from s to dj on the tree Ti
S (u, I) = The degree of satisfaction of ith time S (u, i) S (u, i)$\in$[0, 1]
TF (u ,I) = The weight of ith transactions
T_l = The trust value on the communication link l
Trust (u) = The node u's trust score during the periodical time t
c_l = The direct trust on the communication link l
CTi = The total of trust score for each node along path of the tree Ti
$\triangle$(Pi) = The total of hop counts on the path Pi
(Bp) = The best path computed based on both trust score and hop count from source to destination

TRUST REPRESENTATION AND PATH SELECTION

Trust (u) represents the node u's trust score during the periodical time t. The range of Trust (u) is given as {0 ≤ Trust (u) ≥ 100} where 0 denotes that the node is untrustworthy, 100 denotes that the node is fully trustworthy.

The direct trust of node u is defined as:

$$Direct_{Trust}(u) = \frac{\sum_{i=1}^{m} S(u,i) * TF(u,i)}{\sum_{i=1}^{m} TF(u,i)} \quad (1)$$

The indirect trust of node u is measured by other nodes' recommendations and is defined as follows:

$$INDirect_{Trust}(u) = \frac{\sum_{i=1}^{m} t\ u(i) *\ t\ d(i)}{\sum_{i=1}^{m} Td(i)} \quad (2)$$

$INDirect_{Trust}$ (u) represents the indirect trust of node u while $Direct_{Trust}$ (u) is the direct trust of node u relative to node i's direct trust.

The node u trust denotes that:

$$Trust(u) = \alpha * Direct_{(trust)}(u) + \beta * INDirect_{(trust)}(u) + \gamma * Trust_{l}(u) \quad (3)$$

Trust (u) represents the trust score collected for node u during the time t. α, β, γ are the weight of direct trust, indirect trust and trust score respectively as collected during the time t.. α, β, γ ranges from [0 to 1].

Hence, at any point, the Routing Request message (RREQ) and Routing Reply RREP in AODV contain a list of all the nodes visited with their trust score added to the total of trust score for each not along the path (CTi). Whenever a node receives a RREQ or RREP messages, it will check the updates of the route to the source node. It then checks for the best path (best path (Bp) of intermediate nodes which is computed by Eq. 4.

The best path (Bp) selected is defined as:

$$(Bp)\ Max = \left\{ \frac{\sum_{Tie P_i^{(s,dj)}} C_{Ti}}{\sqrt{\triangle(P_i) \cdot \triangle(P_i)}} \right\} \quad (4)$$

Reliable Dynamic Trust Based Routing Protocol (RDTR): AODV routing protocol can be modified to select an optimum path during the route discovery cycle based on both trust and the number of hops (trusted and shortest path). When the route request and route reply (RREQ and RREP) messages in RDTR are generated or forwarded by the nodes in the network, each node appends its own trust score to the trust accumulator (CTi) on these route discovery messages. Each node also updates its routing table with all the information contained in the control messages as shown in Table 1.

As the RREQ messages are broadcasted, each intermediate node that does not have a route to the destination forwards the RREQ packet. Hence, at any point, the RREQ packet contains a list of all the nodes visited with their trust score value added to trust summation accumulator (CTi).

Whenever a node receives an RREQ packet, it will check the updates of the route to the source node. It then checks the path score (Bp) for intermediate nodes which was computed by Eq. 4.

A new entry is made in the routing table for any of the intermediate nodes and 60% trust is assigned to them,

Table 1: Example of routing table

Node	Next hop	Hop cnt	Trust score	Indirect trust	Best path (Bp)
1	1	1	95	81	87
5	2	4	88	75	81
7	1	5	70	61	63

if one did not already exist. If a route entry for a node does exist and if the Best Path (Bp) to any of the intermediate nodes is greater than the previously known Best Path (Bp) to that node, the routing table entry is updated for that node and a new trust values will be computed as specified in Eq. 1-3.

This nature of updating the routing table together with maintaining the lifetime for each route entry helps to invalidate the stale entries and keep the route entries current, thus improving the routing accuracy of the protocol.

As the RREP message is unicasted back to the source, each intermediate node forwards the RREP packet by adding its trust to the trust accumulator (CTi) in the packet. Hence, at any point, the RREP packet contains all the previously visited nodes. Similar to the RREQ message, the routing table is updated for each intermediate node visited by the RREP message in addition to the update done in the destination node.

In RDTR, nodes will update their routing table based on the information attached in RREQ or RREP messages.

Performance analysis: In here, the simulation results of the proposed RDTR protocol are presented. There will be one scenario and for that scenario, there are three performance metrics that will be measured which are:

- Packet delivery fraction
- Average end-to-end delay of data packets
- Normalized routing load

The first two metrics are the most important for best efforts traffic. The routing load metric evaluates the efficiency of the routing protocol. These metrics were chosen because they are able to measure the efficiency of the routing protocol.

In this simulation, 50 nodes are fairly distributed within 1500 x300 m area with transmission range of 250 m. The pause time is varied from 0 to 125 and the simulation period is 900 sec. Nodes are allowed to move up to the speed of 25 m sec^{-1} which is a reasonable maximum speed. The simulation parameters for this scenario are shown in Table 2.

There are two test cases in this simulation for evaluating the new protocol:

- The normal AODV protocol under the misbehaviour effect. Some of the network nodes will drop data packets based on the percentage of misbehaved nodes
- The proposed RDTR protocol, under the misbehaviour effect. Some of the network nodes will drop data packets based on the percentage of misbehaved nodes

Theoretically, it is expected that the proposed RDTR protocol will achieve higher packet delivery rate compared to the normal AODV in the situation where the nodes can drop packets. Of course, the highest packet delivery rate is achieved when the nodes do not drop packets at all. When it comes to end-to-end delay, it is expected that RDTR protocol will have slightly higher delay compared to AODV due to the possibility that it may take a longer path which is more trusted. The normalized routing load for RDTR also is expected to be slightly higher compared to that of AODV due to the fact that it will generate more messages if a longer path is chosen.

Figure 2 illustrates the packet delivery fraction of both test cases. In this simulation, when pause time is set to 0 (continuous motion), both protocols obtain low packet delivery fraction due to the continuous movement of nodes. As the pause time is increased, the packet delivery fraction increases as well. However, regardless of the value of pause time, RDTR always perform better than AODV due to the lower probability of packet drop for choosing to route only over trusted nodes.

Figure 2 shows the average end-to-end delay for both test cases. Since there are several misbehaved nodes in the network, there will be broken routes in both test cases. This will require the nodes to find a new route to

Table 2: Simulation parameters

Number of nodes	50 nodes
Simulation time	900 sec
Map size	500 m x 500 m
Max speed	25 m sec^{-1}
Mobility model	Random way point
Traffic type	Constant Bit Rate (CBR)
Packet size	512 bytes
Connection rate (Nominal radio range)	4pkts sec^{-1}
Pause Time	0,25,50,75,100,125 (sec)
Number of connection	5

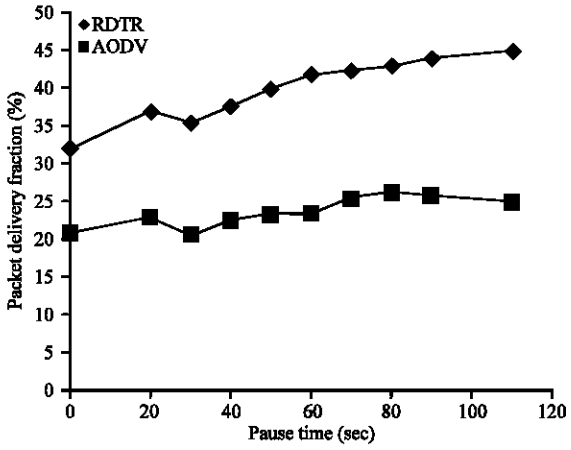

Fig. 2: Packet delivery fraction under 40 to 50 percentage of malicious misbehaviors

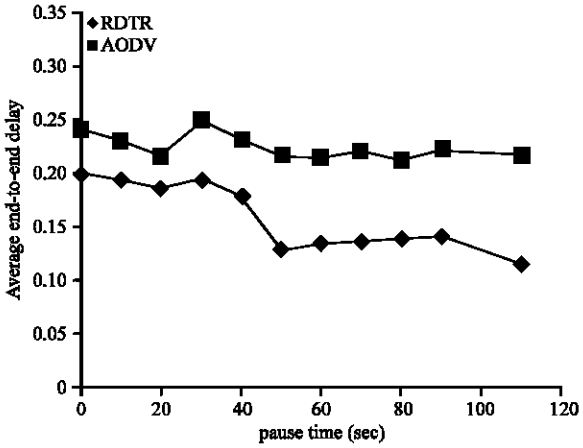

Fig. 3: Average end-to-end delay under 40 to 50 percentage of malicious misbehaviors

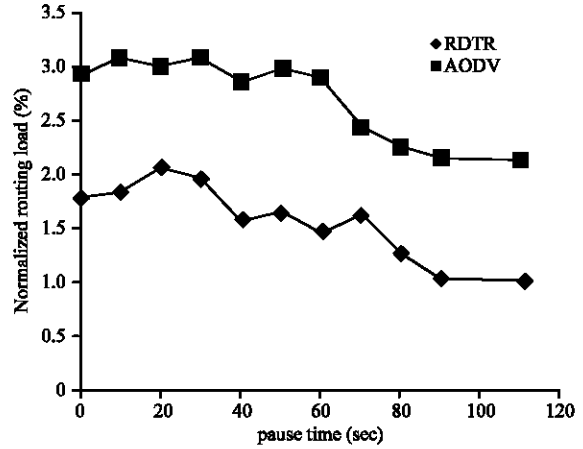

Fig. 4: Normalized routing load under 40 to 50 percentage of malicious misbehaviors

the destination which in turn will increase the end-to-end delay. In theory, RDTR may have higher average end-to-end delay as compared to the normal AODV protocol because the trusted path selected by the best path mechanism may be longer than the shortest path calculated by AODV. However, this experiment has shown that RDTR actually performs better than AODV. This is because by selecting to route packets only through trusted nodes, the possibility of having broken routes and having to recalculate the path is lower in RDTR. In AODV, even though the path chosen is the shortest path, the path may have to be recalculated because the earlier path may contain misbehaved nodes. This eventually leads to the increase of the end-to-end delay in AODV.

Figure 3 illustrates the normalized routing load. As mentioned earlier, theoretically it is expected that the normalized routing load in RDTR will increase due to the extra messages that need to be generated when chosen path is longer than the shortest path. However, the experiment result shows otherwise. RDTR actually generates lower load compared to AODV (Fig. 4). The explanation for this is similar to the one given for the end-to-end delay case. In AODV, the rate for broken route is higher and therefore the nodes have to do extra work to find a new route. RDTR performs better by not having to recalculate its path so often.

CONCLUSION

In this study, we proposed a new MANET routing algorithm called Reliable Dynamic Trust-based Routing protocol (RDTR) which is basically an extension to the AODV routing protocol that integrates a trust mechanism with a shortest path routing algorithm to establish and maintain trustworthy routes in the network. The proposed algorithm was implemented and simulated using the NS-2 network simulator. In the simulation, each node is given a trust value and this value is associated with the possibility of the node to perform a packet drop. With the inclusion of trust mechanism, it is expected that Reliable Dynamic Trust based Routing (RDTR) protocol would result in a higher percentage of successful data delivery as compared to AODV. It is also expected that the end-to-end delay and normalized routing load will be higher compared to that of AODV because the packets may need to take a longer route (which is more trusted) and the nodes need to generate more routing messages. The simulation result shows that the use of RDTR does provide a higher percentage of successful data delivery. However, the simulation has also shown that the RDTR protocol performs even better than AODV with respect to end-to-end delay and normalized routing load. Therefore, it can be concluded that RDTR provides both enhanced reliability and performance.

ACKNOWLEDGMENTS

This study is supported by MOSTI (Ministry of Science, Technology and Innovation, Malaysia) with project code 01-02-03-SF0202.

REFERENCES

Cheng, H. and S. Yang, 2010. Genetic algorithms with immigrants schemes for dynamic multicast problems in mobile ad hoc networks. J. Eng. Appl. Artif. Intell., 23: 806-819.

Chuanhe, H., C. Yong, S. Wenming and Z. Hao, 2007. A trusted routing protocol for wireless mobile ad hoc networks. Proceedings of the IET Conference on Wireless, Mobile and Sensor Networks, December 12-14, 2007, Shanghai China, pp: 406-409.

Jassim, H.S., S. Yussof, T.S. Kiong, S.P. Koh and R. Ismail, 2009. A routing protocol based on trusted and shortest path selection for mobile ad hoc network. Proceedings of the 9th Malaysia International Conference on Communication, December 15-17, 2009, Kuala Lumpur, Malaysia, pp: 547-554.

Jing, F., R.S. Bhuvaneswaran, Y. Katayama and N. Takahashi, 2006. On-demand multipath routing protocol with preferential path selection probabilities for MANET. Proceedings of the 20th International Conference on Advanced Information Networking and Applications, April 18-20, 2006, Vienna, Austria, pp: 758-762.

Johnson, D., D. Maltz and Y. Hu, 2007. The dynamic source routing protocol for mobile ad hoc networks. http://tools.ietf.org/html/rfc4728.

Khan, K.U.R., R.U. Zaman and A.V. Reddy, 2008. Performance comparison of on-demand and table driven ad hoc routing protocols using NCTUns. Proceedings of the 10th International Conference on Computer Modeling and Simulation, April 1-3, 2008, Cambridge, UK., pp: 336-341.

Kumar, S. and J. Sengupta, 2010. AODV and OLSR routing protocols for wireless ad-hoc and mesh networks. Proceedings of the International Conference on Computer and Communication Technology, September 17-19, 2010, Allahabad, Uttar Pradesh, India, pp: 402-407.

Li, X., M.R. Lyu and J. Liu, 2004. A trust model based routing protocol for secure ad hoc networks. Proc. IEEE Aerospace Conf., 2: 1286-1295.

Sloman, M., J. Lobo and E. Lupu, 2001. Policies for distributed systems and networks. Proceedings of the International Workshop on Policies for Distributed Systems and Networks, January 29-31, 2001, Bristol, UK., pp: 29-31.

Welch, B.B., K. Jones and J. Hobbs, 2003. Practical Programming in Tcl and Tk. 4th Edn., Prentice Hall, USA., ISBN-13: 9780130385604, Pages: 882.

Yahalom, R., B. Klein and T. Beth, 1993. Trust relationships in secure systems: A distributed authentication perspective. Proceedings of the IEEE Computer Symposium on Research in Security and Privacy, May 24-26, 1993, Oakland, CA., USA., pp: 150-164.