Journal of Computer Science 10 (9): 1859-1864, 2014
ISSN: 1549-3636
© 2014 Science Publications
doi:10.3844/jcssp.2014.1859.1864 Published Online 10 (9) 2014 (http://www.thescipub.com/jcs.toc)

EVALUATING AN AUTHENTICATED TRUST BASED ADHOC ON DEMAND DISTANCE VECTOR FOR MALICIOUS NODES ISOLATION IN MANET

Sumathi, A. and B. Vinayaga Sundaram

Department of Information Technology, MIT Campus, Anna University, Chennai, India

Received 2013-11-27; Revised 2014-02-10; Accepted 2014-04-30

ABSTRACT

MANET networks are defined as the wireless self configuring networks that are capable of operating without the support of any fixed infrastructure and a central coordinator which makes the routing a complicated task. For detecting misbehaving and selfish nodes between the intermediate nodes it is essential to evaluate the Intermediate Trust Value (ITV) for each node in the network, so that malicious node is isolated. A threshold value is maintained and if the ITV of a node falls below the threshold value, then it is considered as a misbehaving node and are avoided for data communication in a MANET network. Simulation results are evaluated under blackhole attack which also proves that the proposed Authenticated Trust based AODV protocol (AT-AODV) eliminates blackhole attacks and performs well in malicious nodes isolation which increases the packet delivery ratio.

Keywords: AODV, AT-AODV, Trust, Malicious Nodes, Blackhole Attack

1. INTRODUCTION

In MANETS, due to mobility of nodes, there is no predefined Infrastructure. Since it is a dynamic environment, nodes may enter or leave the network at any time without taking part in the data transmission. All nodes must coordinate each other to enable communication which requires each node to be more intelligent so that it can function both as a network host for transmitting and receiving data and as a network router for routing packets from other nodes. Hence evaluating proposed ITV for each node enables a secured communication between the nodes in a MANET environment. The security features which are needed for secure data communication in MANETS are:

- Data Integrity between source node and destination node
- End-to-End Authentication from source node to destination node
- End-to-End non repudiation for source and destination nodes
- Protecting data from Internal and External attacks in the network
- Maintaining data confidentiality throughout the network

In the forthcoming chapters, how the proposed protocol AT-AODV support the necessary authentication in a MANET environment is discussed.

2. RELATED WORK

Bhalaji *et al*. (2008) proposed a new trust establishment among nodes to overcome the packet dropping attack using DSR routing protocol. The results obtained are compared with DSR for dropped data packets ratio between the total drops and malicious drops which seems satisfactory.

Kartheesn and Srivatsa (2012) proposed a combined data security using three policies such as Integrity, authentication and confidentiality. Integrity is provided by calculating trust indexes of the nodes,

Corresponding Author: Sumathi, A., Department of Information Technology, MIT Campus, Anna University, Chennai, India

authentication is provided by using Distributed Certificate Authority (DCA) technique and confidentiality is provided by an RSA based novel encryption mechanism.

Sakthivel and Radha (2011) suggested an algorithmic approach for misbehaving node detection and isolation by maintaining a counter which increments every time when node misconduct is detected and when the counter crosses the limit value it is labeled as malicious. The percentage of selfish nodes present in the network was also monitored.

Suganthi and Tamilarasi (2012) proposed cooperation of nodes between intermediate nodes for route discovery and transmission of pockets between source and destination. The impact of malicious node on the Optimised Link State Routing (OLSR) protocol is observed such that the throughput degrades when the network is attacked by malicious nodes.

Manikandan and Manimegalai (2012) investigated a study modification of AODV and DSR routing protocol implementation with regard to mitigating attacks and intrusion detection. This study also proposes routing protocol which predicts and handle the attacks by malicious node isolation.

3. OVERVIEW OF PROPOSED ROUTING PROTOCOL AT-AODV

3.1. Need for Trust and ITV Evaluation in MANETS

The characteristics of Trust can be given as follows (Ramana *et al*., 2010):

- Trust is subjective
- Trust is not transitive. (i.e.,) X trusts Y and Y trusts Z but it does not imply that X trust Z
- Trust is dynamic not static

Since it is dynamic, for making a decision upon each node, an ITV computation for each node is a must. The following section describes how an ITV value is calculated and used with the AODV routing protocol in MANETS.

Now in the proposed protocol E-AODV, it is assumed that the query request success rate of a node i can be calculated based on the neighbouring node which had received the broadcast message from the source node successfully and it can be given as $q_r\ s_i$. The query response failure of a node i can be calculated based on the neighbouring nodes which do not receive the broadcast message from the source node and it can be given as $q_r\ f_i$. Hence the query request for node i is:

$$q_r(i) = \sum \frac{q_r s_i - q_r f_i}{q_r s_i + q_r f_i} \quad (1)$$

Here it is assumed that the request and response for a node is given as $r_q = 0.1$ and $r_p = 0.1$ and K = a constant value depending upon the maximum rate of packets to be transmitted in Kbytes.

Now the data query request success of a node i can be calculated based on the successful data transmission towards the destination and it can be given as $dq_r s_i$ and the data query response failure of a node i can be calculated based on the failure of data transmission towards the destination and it can be given as $dq_r f_i$.

The data query request for node i can be given as:

$$dqr(i) = \sum \frac{dq_r s(i) - dq_r f(i)}{dq_r s(i) + dq_r f(i)} \quad (2)$$

Now the intermediate trust value can be calculated as:

$$ITV(i) = \frac{\sum [r_q * q_r(i)] + [r_p * dq_r(i)]}{k} \quad (3)$$

3.2. AT-AODV Route Request and Route Response

Adhoc On Demand Distance Vector (AODV) routing protocol implements the routing only on demand which is issued by the source node for data transmission. The source node and the intermediate nodes stores the neighbouring nodes information such as next hop information corresponding to each flow for data packet transmission.

A routing phase of an AODV in MANET consists of a route request message which is broadcasted by the source nodes to all other nodes to find an unknown route. At first all nodes are initialized in MANETS by each node having its own unique IP, MAC and sequence number. The nodes send signal to find the number of other nodes within range. The synchronization between nodes takes place and the neighbour's list for each node is maintained in the Routing Information Table (RIT).

3.3. AT-AODV Path Selection Phase

For each node in the neighbour's list we calculate the ITV of that node. From the calculated ITV neighbour nodes, the node which contains the highest ITV has priority is selected as an AT-path (Authenticated Trust based path) for data transmission. This is called as first hop AT-path. From the selected node, the ITV values are calculated for next authentic nodes and second hop AT path is found. Similarly the AT-path is found for all intermediate nodes between source and destination nodes. Finally an AT-path is found between source and destination nodes. If the ITV falls beyond the threshold value 0.5, then that particular node will not be selected for data transmission and is isolated as a malicious node which is discussed in **Table 1**.

3.4. AT-AODV Error Routing Phase

Suppose if a link breakage occurs between the intermediate authenticated nodes (or) any packet drop occurs in the intermediate nodes at the time of transmitting packets then a route error message will be invoked from that node with the Error-id and that node will be immediately removed from the AT-path as well as in the RIT as an authenticated node. Here it is assumed that a packet drop occur when a node becomes a misbehavior node which can be due to network error. So for avoiding such misbehaving nodes it is removed from the AT-path and RIT at the time of transmission. Now the proposed ITV calculation is explained using an example as shown in **Fig. 1**.

Consider the **Fig. 1** with 7 nodes of which ITV has to be calculated for node 1 which has 3 neighbour nodes:

$$q_r(1) = 3 - 0/3 + 0 = 1$$
$$dq_r(1) = 1000 - 100/1000 + 100 = 0.82$$
$$ITV(1) = (0.1 \times 1) + (0.1 \times 0.82)/K = 0.1 + 0.82/k$$
$$\text{Hence } ITV(1) = 0.92$$

Here according to the proposed protocol AT-AODV, the nodes are selected based on the highest Intermediate Trust Value among the neighbour nodes for data transmission and is depicted in **Fig. 1**. Here node 6 has a lowest ITV 0.3 which is considered as a malicious node as per the decision making **Table 1** and is avoided for data transmission. But AODV does not have the capability of finding a malicious node and hence packet delivery decreases.

4. RESULTS

Here NS-2 simulator tool is used to simulate the proposed protocol. Both the AODV and AT-AODV protocols are implemented in NS2, 2. 34 version and had made comparisons between the protocols. Here 50 nodes are selected which are arranged in a MANET topology of network area 2000×2000 meters. Using the nam simulator trace files the various parameters such as throughput, packet delivery ratio, node density and blackhole attack are analyzed. The various parameters used are shown in **Table 2**.

Table 1. ITV decision making

S.No.	ITV of a node	Decision making for AT-path selection
1	≥0. 7	Accept with higher priority
2	≥0.5 and <0.7	Accept with less priority
3	<0.5	Maintained in black list and isolate as malicious node

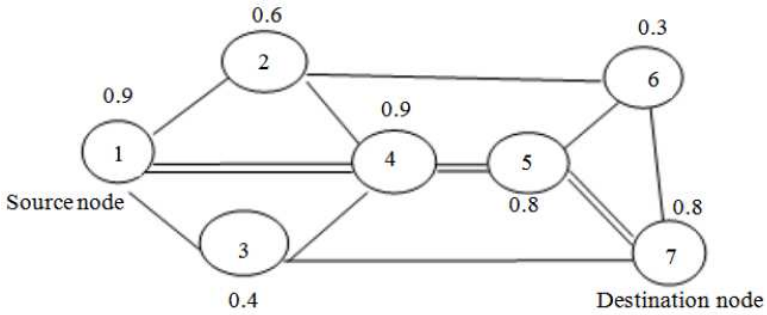

Fig. 1. Implementation of AT-AODV with example diagram

Table 2. Parameters used

Parameters	Assumptions
Simulator tool	NS-2 (version 2.34)
No. of nodes	50
Minimum delay required	2 CBR units
Maximum delay required	7 CBR units
Minimum bandwidth required	4 CBR units
Network area	2000x2000 meters
Transmission range	250 meters
MAC layer protocol	IEEE 802.11
Protocol	AODV, AT-AODV
No. of packets	1000

5. DISCUSSION

Suresh and Duraisamy (2011) have proposed a reputation scheme in which the reputation is evaluated to find the trust value of the node. Mangai and Tamilarasi (2011) proposed an Improved Location aided Cluster based Routing Protocol which provides high delivery ratio with the Intrusion Detection Systems which is specifically designed for GPS enabled MANETS. Suganthi and Tamilarasi (2012) investigate the degradation of QOS under an attack by a small group of malicious node on the Optimized Link State Routing Protocol. Boukerche and Ren (2008) proposed a Generalized Reputation Evaluation to prevent from malicious nodes. No specific type of attack model is discussed.

The **Fig. 2** represent a screenshot of Intermediate trust values calculated in the proposed AT-AODV network. The proposed routing protocol AT-AODV chooses an authentic trust based secure path, so the packet loss is less and the packet delivery ratio is high when compared to that of AODV routing protocol which is shown in **Fig. 3**. Since the proposed protocol AT-AODV chooses a reliable and authentic path than AODV, the throughput performance of AT-AODV is better at all of time intervals as shown in **Fig. 4**.Initially the number of malicious nodes is high, but in case of AODV, it does not contain any trust and authentication enforcement, so the same level of malicious node retains. But in case of AT-AODV, at the first stage itself we authentic nodes only if it possesss unique ids. Without unique id, it is considered as a malicious node and it is not considered for data transmission. So the graph becomes decreasing incase of AT-AODV which is shown in **Fig. 5**.

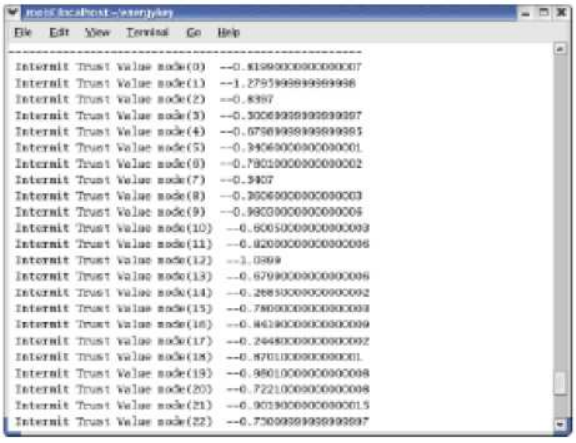

Fig. 2. Screenshot of ITV obtained for proposed AT-AODV

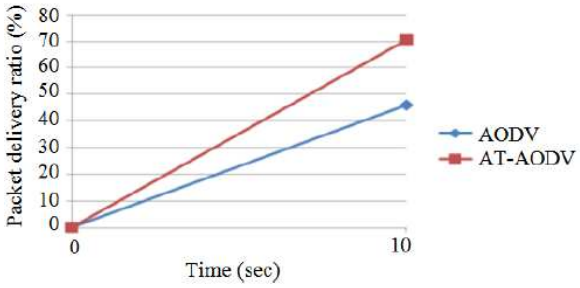

Fig. 3. Comparision of PDR

In AT-AODV, a node which does not possess the unique ids is considered as an unauthentic node. At this stage, an unauthentic node is considered as a malicious node and isolated from the network for data transmission. The percentage of malicious noes that are isolated with the help of ITV from the network portrays the strength of the authenticated protocol AT-AODV in detecting malicious behaviour which is shown in **Fig. 6**.

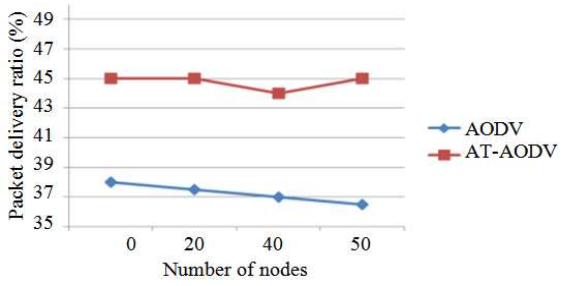

Fig. 4. Comparision of throughput

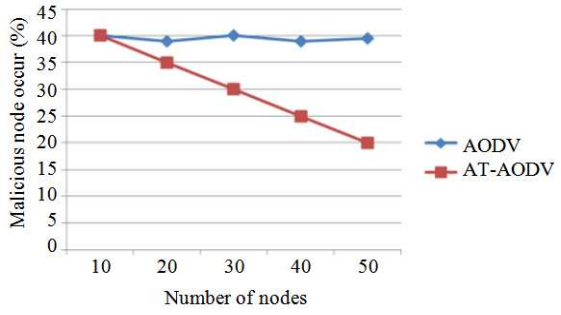

Fig. 5. Comparision of malicious node occur

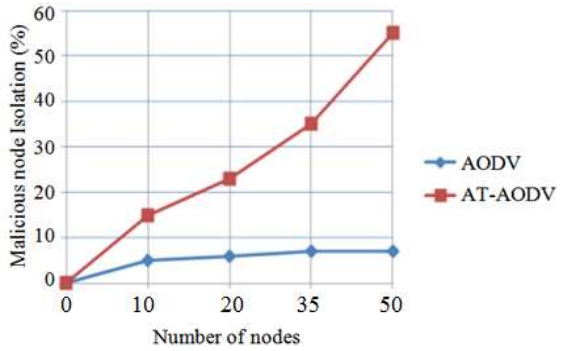

Fig. 5. Comparision of malicious node occur

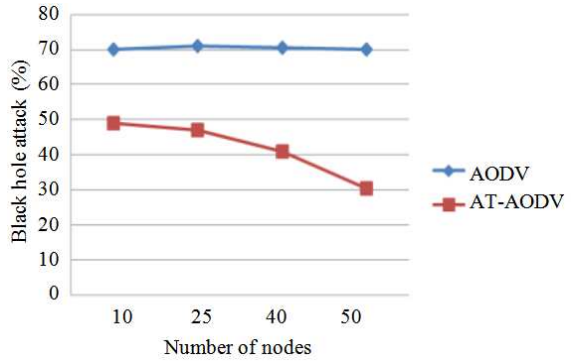

Fig. 7. Comparision of blackhole attack

In the proposed AT-AODV routing protocol, using unique ids, ITV for each node is evaluated and malicious nodes are eliminated. So no node can act as a black node with the intention of intercepting packets. Hence black node attack percentage is reduced in AT-AODV but not in AODV which is shown in **Fig. 7**.

6. CONCLUSION

Hence for detecting misbehaving and selfish nodes between the intermediate nodes the Intermediate Trust Value (ITV) for each node which depends on the value of successful packet delivery rate is evaluated in the network, so that malicious nodes are isolated. A threshold value is maintained and if the ITV of a node falls below the threshold value, it is considered as a malicious node and is avoided for data communication in a MANET network. Simulation results are evaluated under black hole attack such that no node can act as a black node with the intention of intercepting packets and hence proved. Simulation results also prove that our proposed Authenticated Trust based AODV protocol (AT-AODV) performs well in malicious nodes isolation and packet delivery ratio is also increased. Future work can be extended for finding node SINR (Signal to Noise Interference Ratio) value, node capacity value, analyzing of link utilization metric and attaining an energy constrained and a congestion controlled network.

7. REFERENCES

Bhalaji, N., S. Banerjee and A. Shanmugam, 2008. A Novel Routing Technique against Packet Dropping Attack in Adhoc Networks. J. Comput. Sci., 4: 538-544. DOI: 10.3844/jcssp.2008.538.544

Boukerche, A. and Y. Ren, 2008. A Security Management Scheme using a Novel Computational Reputation Model for Wireless and Mobile Ad Hoc Networks. Proceedings of the 5th ACM symposium on Performance Evaluation of Wireless Ad hoc, Sensor and Ubiquitous Networks, Oct. 27-31, ACM New York, pp: 88-95. DOI: 10.1145/1454609.1454628

Kartheesn, L. and S.K. Srivatsa, 2012. A policy based scheme for combined data security in mobile ad hoc networks. J. Comput. Sci., 8: 1397-1406. DOI: 10.3844/jcssp.2012.1397.1406

Mangai, S. and A. Tamilarasi, 2011. An improved location aided cluster based routing protocol with intrusion detection system in mobile ad hoc networks. J. Comput. Sci., 7: 505-511. DOI: 10.3844/jcssp.2011.505.511

Manikandan, S.P. and R. Manimegalai, 2012. Survey on mobile ad hoc network attacks and mitigation using routing protocols. Am. J. Applied Sci., 9: 1796-1801. DOI: 10.3844/ajassp.2012.1796.1801

Ramana, K.S., A.A. Chari and N. Kasiviswanth, 2010. A survey on trust management for mobile adhoc networks. Int. J. Netw. Security Applic., 2: 75-85.

Sakthivel, U. and S. Radha, 2011. Misbehaving node detection in mobile ad hoc networks using multi hop acknowledgement scheme. J. Comput. Sci., 7: 723-730. DOI: 10.3844/jcssp.2011.723.730

Suganthi, P. and A. Tamilarasi, 2012. Impact of malicious nodes under different route refresh intervals in adhoc network. Am. J. Applied Sci., 9: 18-23. DOI: 10.3844/ajassp.2012.18.23

Suresh, A. and K. Duraiswamy, 2011. Mobile ad hoc network security for reactive routing protocol with node reputation scheme. J. Comput. Sci., 9: 242-249. DOI: 10.3844/jcssp.2011.242.249