ENHANCED T-AODV ROUTING PROTOCOL IN WIRELESS NETWORKS

Nagisetty.Rachana, CSE, NIT Andhra Pradesh, Kandi.Sreeja, Nagisetty.Abhinaya, IT , NIT Raipur and
BKSP.Kumar Raju Alluri, CSE, NIT Andhra Pradesh

***Abstract*—Wireless networks are prone to a variety of attacks due to their open nature. In this paper, we have proposed a new algorithm for Trust embedded Ad-hoc On Demand Distance Vector (iT-AODV). Also, an extension for iT-AODV is introduced to withstand multiple attacks by malicious nodes (eT-AODV). Through experimental results, the proposed approach proved the network efficiency in terms of improved packet delivery ratio, hop by hop cost, trusted path distance and number of nodes to the destination. Simulation results show that the proposed scheme performs better than T-AODV.**

Keywords—Routing;Malicious nodes;Trust ;Attacks

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of network devices which are connected through the wireless links. Wireless Ad-hoc networks are self-organizing, rapidly deployable and require no fixed infrastructure. Fig.1. shows one such MANET. The use of a wireless network enables enterprises to avoid the costly process of introducing cables into buildings. Wireless networks use radio waves to connect devices such as laptops to the Internet. They are comprised of wireless nodes, which must cooperate in order to dynamically establish communications using limited network management and administration [1].

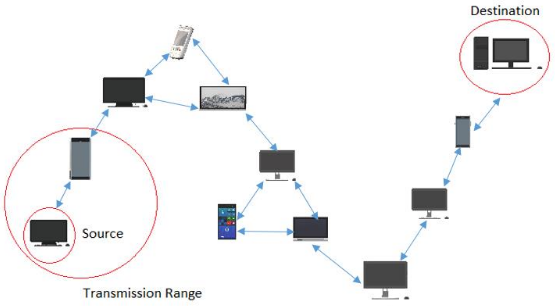

Fig. 1: Mobile Ad-hoc Network

The performance of wireless networks is highly dependent on routing protocols. Fig.2 shows routing protocols. (1) Proactive routing Protocol (2) Reactive routing Protocol and (3) Hybrid routing Protocol. AODV is a popular routing protocol for wireless networks. It is a reactive protocol in which the routes are created only when they are needed i.e., when they are requested by source nodes. Network nodes that need connections broadcast a request for connection. The remaining AODV nodes forward the message and record the node that requested a connection. Thus, they create a series of temporary routes back to the requesting node.

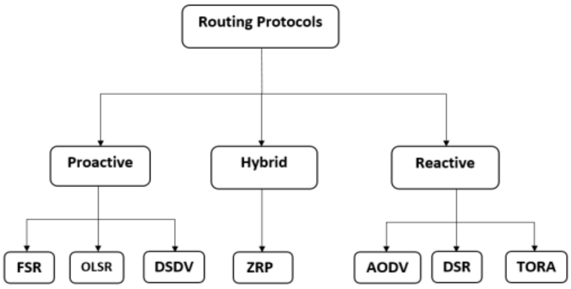

Fig. 2: ROUTING PROTOCOLS IN MANET

This protocol establishes routes to destinations on demand and supports both unicast and multicast routing. AODV utilizes routing tables to store routing information. The route table in AODV stores destinationaddr, next-hop, destseqno, hopcount, lifetime.

<destinationaddr, next-hop, destseqno, hopcount, lifetime>

Each node in this network relays on its neighbours for routing and message forwarding. However, neighbour based communication without any trust worthiness creates a major vulnerability in security related aspects of the network. In this type of environment, trust value plays a crucial role in all of the network activities. So, Ad hoc network is also defined as trusted network. To achieve this, existing AODV routing protocol has been modified in order to adapt the trust based communication feature known as trust embedded ad hoc on-demand distance vector (T-AODV). T-AODV concentrates on node trust. In T-AODV, the following parameters are stored. This routing table also contains trust value of the node.

<destinationaddr, next-hop, destseqno, hopcount, lifetime, nodetrust>

A. *Problem Definition*

In MANET, all nodes are free to join and leave the network. All intermediate nodes between a source and destination take part in routing. A node sends packets to all the nodes in its transmission range. Due to these characteristics, each node can easily gain access to the other node packets or inject fault packets to the network. Therefore, securing MANET against malicious behaviour and nodes, became one of the most important challenges [2]. Malicious nodes launch security attacks in the network and lead to damage the different network functions such as routing, energy and data aggregation. But T-AODV does not take the presence of malicious nodes in network into consideration. We need to establish secure route between source and destination with less probability of having malicious nodes.

B. *Proposed Approach*

In this paper, we propose a new algorithm based on Trust based AODV protocol and we call it as improved TAODV (i.e. iT-AODV). An extension for iT-AODV is also introduced (eT-AODV) based on trust method to secure against attacks such as Gray hole attack, Routing loop attack, Packet insertion, Packet drop and Packet modification. eT-AODV ignores malicious nodes encountered in the path to ensure secure communication. Detection of malicious node is done based on trust value of the node.

II. RELATED WORK

In recent years, security issues in Ad-hoc networks have drawn considerable attention. There have been number of research efforts done to address the security needs for MANETs [1][11]. Recommendation and reputation models have been proposed to enhance security in MANETs. Over the past few years, even if some secure methods have been designed to find an end-to-end secure routes, they fail to protect the network from malicious nodes acting in collusion.

According to some researchers, trust is a set of relations among entities that participate in a protocol [3]. These relations are based on the confirmation generated by the previous interactions within a protocol. In general, if the interactions have been reliable to the protocol, then trust will accumulate between these entities. Trust has also been defined as the degree of belief about the behavior of other entities or agents.

Biswas et.al [9] proposed a solution to detect and prevent black hole attacks for each single and co-operative node. Within the network every node have three parameters for checking its trust rank, remaining power and stability issue. If the rank of the node is zero, then consider it as black hole node.

In [10], Hansi Mayadunna proposed a new model for the detection of malicious node. This model considers only the black hole attack to detect malicious node. Also, trust value calculation includes direct and indirect trust which is an overhead to the node.

Buchegger et.al [5] proposed a protocol named CONFIDANT to encourage the node cooperation and punish misbehaving nodes. Wang et al [6] has proposed a trust-based incentive model for selfpolicing mobile ad hoc networks to reduce impact of false recommendation on the accuracy of trust values. Maltz D et.al [2] analyzed the use of on-demand behavior in different routing protocols proposed for use in multi-hop wireless adhoc networks.

Subramaniam et.al [7] presents Trust based AODV protocol. In their work, node selection process is performed before routing. Trust and energy are measured before nodes are chosen for routing and threshold value is outlined clearly. Node's trust and energy levels are beyond threshold for considering it in the routing process. Estahbanati et.al [8] introduced Hidden Markov Model (HMM) as trust model that relies on Markov chain trust. The main focus of the paper is choosing the suitable route based on the measured trust value.

Xia Li et.al [4] proposed a new model to quantify trust level of the nodes in MANET. They have defined a new computation function in which the effect of different direct experiences can be adjusted individually. To combine the direct and indirect trust values from others, they have modeled a new trust relation equation. But in their research, there are issues with various misleading attacks.

It can be deduced that most of the trust based models calculate node trust instead of path trust. Also, these models include only few attacks to detect malicious node. Consideration of these two aspects would lead to a better model.

III. PROPOSED WORK

Basically T-AODV tends to calculate the trust of a
node based on direct and indirect trust of the nodes which
is an overhead to the node. Instead, trust of the path can be
calculated. This motivation led us to design a new algorithm for T-AODV. Essentially all routing protocols in Ad-hoc community tend to find the shortest path irrespective of the presence of any malicious node in that path. A path free from malicious node is more important than the shortest path. This inspired us to design extended T-AODV routing protocol.

Many trust management schemes are devised to detect misbehaving nodes such as malicious nodes [11]. Specific attacks are described as follows:

• Routing loop attacks: A malicious node may modify routing packets in such a way that they do not reach the intended destination.

• Packet drop: Irrespective of queue status, a malicious node drops packets.

• Packet insertion: A node which is malicious may insert packets with incorrect routing information.

• Grayhole attacks: A malicious node may selectively drop packets, as a special case of a black hole attack. For example, they may forward routing packets but not data packets.

• Packet modification: A node which is malicious may modify packets with incorrect routing information.

A. *Design of The Proposed Algorithm*

The fact that Ad-hoc nodes are characterized by low level of trust among themselves, motivated us to design a secure algorithm based on internal spying and verification. Basic T-AODV invloves calculation of direct and indirect trust of a node which is burden to the node. We proposed an algorithm to overcome this drawback. Here, every node has a self-evaluated trust. Trust is calculated for every pair of nodes. The trust always lies in the range of 0 and 1. The steps for iT-AODV are given in Algorithm 1.

Algorithm-1 takes x,y coordinates of nodes, trust of the nodes, source node and destination node as parameters. A node initially calculates the distance to every node in the network. The nodes which are in transmission range of a node are called reachable nodes. For every path between a node and its reachable nodes, trust values are calculated using equation-1.

$$\mathbf{trust\ (i,j)=(Z(i)+Z(j))/2} \qquad (1)$$

Algorithm 1 Proposed iT-AODV

```
procedure iT-AODV($x, y, Z, sor, dest$)
  for <p=1:n> do
    for <q=1:n> do
      $dt \leftarrow sqrt((x(i) - x(j))^2 + (y(i) - y(j))^2)$
      if $dt \le R$ then
        $trust(i, j) \leftarrow (Z(i) + Z(j))/2$
        $matriz(i, j) \leftarrow dt$
      else
        $trust(i,j) \leftarrow inf$
        $matriz(i,j) \leftarrow inf$
      end if
    end for
  end for
  [$path, cost$] $\leftarrow hop\_by\_hop(sor,des, trust)$
end procedure
```

The path which is having more trust value is considered to be reliable. The function hop-by-hop takes the parameters source, destination, path trust matrix as input. It returns the trusted path between source and destination and its average cost. In the proposed algorithm eT-AODV, we extended the proposed iT-AODV protocol to incorporate the security needed to counter the malicious attack. The steps for eT-AODV are given in Algorithm 2.

In algorithm eT-AODV, we have five different scenarios for a node to act as malicious (step-5). Step-7 considers packet modification. Step-10 deals with grayhole attack which drops one data packet. Trust value is decreased for both packet drop and for acting as malicious node. Step-13 handles packet drop. Number of packets dropped by the node varies from 1 to no. of packets it received i.e., it can drop all plackets (Black hole Attack). Step-16 considers packet insertion. Step-20 covers routing loop attack. In this case, packet never reaches destination. Therefore, output parameters are not obtained.

Algorithm 2 Proposed extended T-AODV

```
1: Fix the no: of nodes
2: Assign x and y co-ordinates randomly for all nodes
3: Assign initial trust in the range 0:7-1 for all nodes randomly.
4: [$path, cost$] = $iT - AODV (x, y, Z, sor, des)$
5: for <d=2:length(path)> do
6:    $c \leftarrow path(d)$
7:    if Packet modification at c then
8:        $Z(c) \leftarrow Z(c) - 0.1$
9:    end if
10:   if Grayhole attack at c then
11:       $Z(c) \leftarrow Z(c) - 0.1$
12:   end if
13:   if Packet drop at c then
14:       $Z(c) \leftarrow Z(c) - (dropped\_packets(c)/np)$
15:   end if
16:   if Packet insertion at c then
17:       $np \leftarrow np + 1$
18:       $Z(c) \leftarrow Z(c) - 0.1$
19:   end if
20:   if Routing loop attack at c then
21:       $Z(c) \leftarrow Z(c) - 0.1$
22:   end if
23:   if $Z(c) < 0$ then
24:       $Z(c) \leftarrow 0$
25:   end if
26:   $hop\_by\_hop\_cost \leftarrow cost$
27:   $trusted\_path\_hops \leftarrow length(path) - 1$
28:   for <d=1:length(path)-1> do
29:       $trusted\_path\_distance \leftarrow trusted\_path\_distance + matriz(path(d-1), path(d))$
30:   end for
31:   for <y=1:n> do
32:       $dp \leftarrow dp + dropped\_packets(y)$
33:   end for
34: end for
```

Trust value of node of the node is made zero if it becomes negative (step-23). Hop By Hop cost, trusted path hops, trusted path distance and dropped packets are calculated in step-26, step-27, Step-28 and Step-31 respectively.

IV. SIMULATION AND RESULTS

We have used MATLAB for our simulation. We have carried out the simulation for two different models. We defined a region of 200 units by 200 units and placed the nodes randomly within that region. The parameters for the model are as shown in the Table 1. For better accuracy, 1000 iterations are run for each node. After each iteration, trust array gets modified. At the end of each iteration, eT-AODV gives hop by hop cost, trusted path distance, total number of dropped packets, and number of hops in the trusted path. The trust array we get at the end of 999th iteration is accurate. Taking this trust array as input, the final results are obtained.

TABLE 1: SIMULATION PARAMETERS

Independent variable	**Set of Parameters Compared**			
No.of nodes	Dropped packets	Trusted path distance	Hop by Hop cost	Trusted path hops

We have varied the number of nodes in the network from 10 to 200 and compared our eT-AODV protocol with iT-AODV in various aspects.

Fig.3 shows the comparison between no. of nodes and total no. of dropped packets in the trusted path. We can observe that eT-AODV performs better than iT-AODV with reduced number of dropped packets most of the time. The possible explanation for this is that, eT-AODV selects the path frees from malicious nodes resulting in lesser no. of dropped packets.

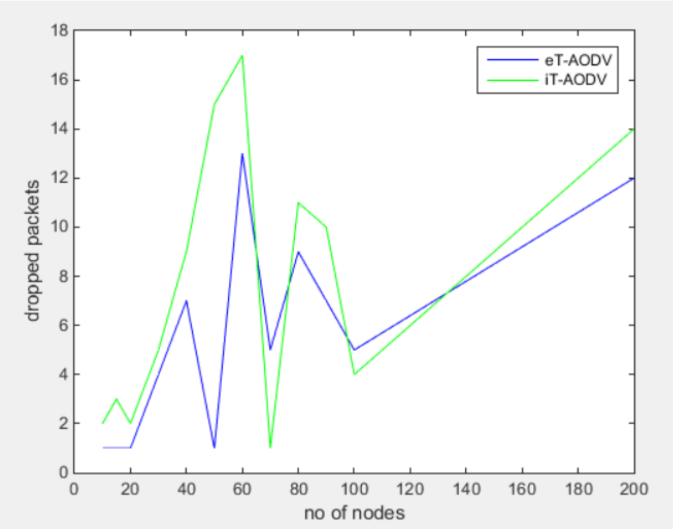

Fig 3: COMPARISION BETWEEN NO OF NODES AND DROPPEDD PACKETS

Fig.4 shows the comparison between no. of nodes and hop-by-hop cost in the trusted path. It can be noticed that eT-AODV performs better than iT-AODV with lower hop-by-hop cost most of the time. This is due to path selection which is free from malicious nodes in eT-AODV resulting low hop-by-hop cost.

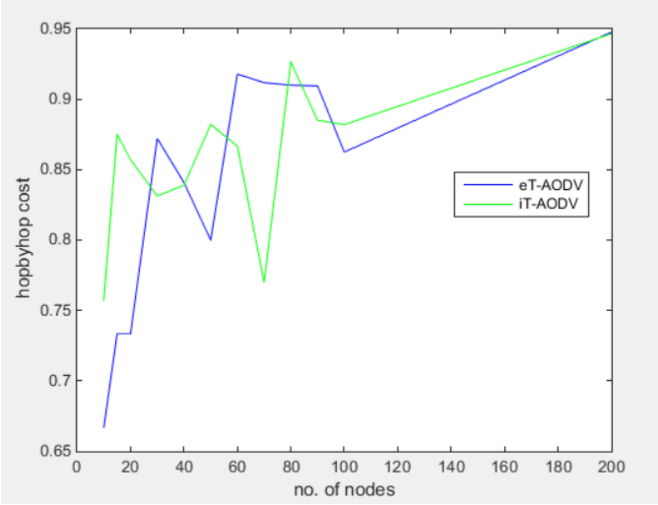

Fig. 4: NO OF NODES AND HOP BY HOP COST CORELATION

Fig.5 shows the correlation between no. of nodes and distance from source to destination in the trusted path. We can observe that most of the time eT-AODV performs better than iT-AODV with lower trusted path distance. This could be because eT-AODV selects the path free from malicious nodes resulting in low trusted path distance.

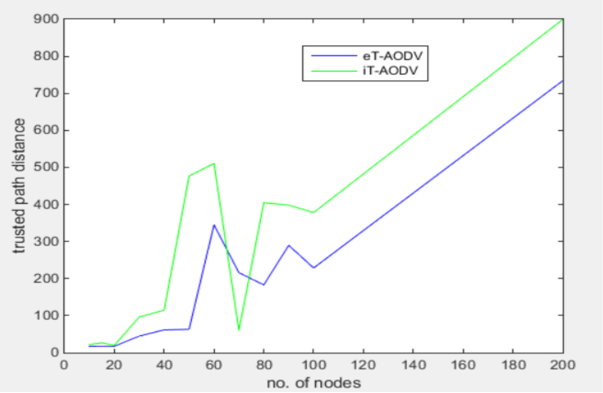

Fig. 5: CORELATION BETWEEN NO OF NODES AND TRUSTED PATH DISTANCE

Fig.6 shows the comparison between no. of nodes and number of hops in between source and destination in the trusted path. We can perceive that most of the time eT-AODV performs better than iT-AODV with lower trusted path hops. The possible explanation for this is that, eT-AODV selects the path free from malicious nodes resulting in lower number of hops.

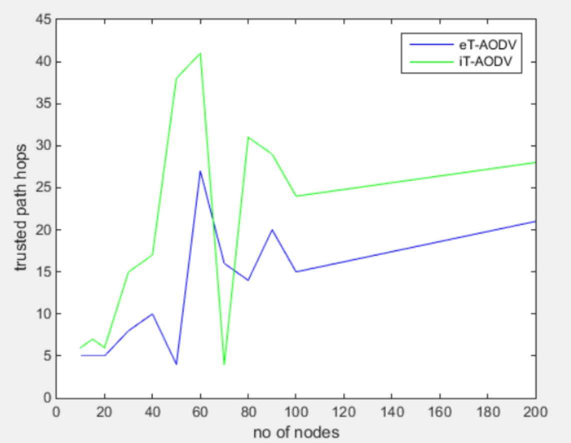

Fig. 6: NO OF NODES AND TRUSTED PATH HOPS COMPARISON

V. CONCLUSION

Trust is a multidimensional, complex and context- dependent concept. In this paper, we proposed a new algorithm for T-AODV (iT-AODV) which selects best path from source to destination based on path trust. Also, we proposed a new MANET routing algorithm called Enhanced T-AODV which is basically an extension to iT-AODV that incorporates a malicious node detection mechanism to enhance its security. The proposed algorithm was implemented and simulated using MATLAB. Each node is given a trust value and this value is associated with the possibility of the node to act as malicious. Any malicious entity, trying to inject wrong routing information or dropping the data packets or modifying the packets, is effectively singled out. With the inclusion of malicious node detection mechanism, it is expected that using eT-AODV would result in better performance in terms of total no. of dropped packets in the path, trusted path hops, trusted path distance and hop by hop cost compared to iT-AODV. Therefore, it can be concluded that eT-AODV does provide enhanced security with minimal impact to performance.

VI. REFERENCES

[1] Swain, Jhum, Binod Kumar Pattanayak, and Bibudhendu Pati.

”Study and analysis of routing issues in MANET.” Inventive Com- munication and Computational Technologies (ICICCT), 2017 Inter- national Conference on. IEEE, 2017.

[2] Maltz David A., et al. ”The effects of on-demand behavior in routing protocols for multihop wireless ad hoc networks.” IEEE Journal on Selected areas in Communications 17.8 (1999): 1439-1453

[3] Patel, Meenakshi, and Sanjay Sharma. ”Detection of malicious attack in manet a behavioral approach.” Advance Computing Con- ference (IACC), 2013 IEEE 3rd International. IEEE, 2013.

[4] Xia Li, Jill Slay and Shaokai Yu, Evaluating trust in mobile ad hoc networks.

[5] Buchegger Sonja and Jean-Yves Le Boudec. A robust reputation sys- tem for mobile ad-hoc networks. No. LCA-REPORT-2003-006.2003

[6] Wang A Trust Approach for Node Cooperation in MANET, H.

Zhang et al. (Eds.): MSN 2007, LNCS 4864, pp. 481 491, 2007.

[7] Subramanian Sridhar, and Baskaran Ramachandran. ”Trust based scheme for QoS assurance in mobile ad-hoc networks.” arXiv preprint arXiv:1202.1664 (2012).

[8] Estahbanati Maryam Miri, Mehdi Rasti, and Seyyed Mostafa Safavi Hamami. ”A mobile ad hoc network routing based on energy and Markov chain trust.” Telecommunications (IST), 2014 7th Interna- tional Symposium on. IEEE, 2014.

[9] Biswas Suparna, Tanumoy Nag, and Sarmistha Neogy. ”Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET.” Applications and Innovations in Mobile Computing (AIMoC), 2014. IEEE, 2014.

[10] Mayadunna, Hansi, et al. ”Improving trusted routing by identify- ing malicious nodes in a MANET using reinforcement learning.” Advances in ICT for Emerging Regions (ICTer), 2017 Seventeenth International Conference on. IEEE, 2017.

[11] Cho, Jin-Hee, Ananthram Swami, and Ray Chen. ”A survey on trust management for mobile ad hoc networks.” IEEE Communications Surveys and Tutorials 13.4 (2011): 562-583.