Journal of Computer Science Engineering and Software Testing

Volume 3 Issue 1

Performance Analysis of TS-AODV and MTS-AODV Routing Protocols in MANET

K. Thamizhmaran
Department of ECE, FEAT, Annamalai University, Annamalai Nagar, Tamilnadu, India
E-mail: tamil10_happy@rediff.com

Abstract

A Mobile Ad-hoc Network (MANET) is a group of wireless nodes that are communicating with each other within radio range without help of infrastructure based or any centralized administration. As the nodes are mobile so topology changes frequently that leads to link failure and lack of infrastructure support and resource constraint is the key issue that causes dishonest and non co-operative nodes. There are finding a route to destination, new route discovery is initiated. The frequent discoveries lead to more network congestion. To avoid this multipath routing protocols have been proposed to find multiple routes to destination and switch on to alternate secondary path in case of route broken and its provide better routing performance and security. In this technical research paper attempt to compare the performance of two reactive routing protocols for MANETs that is Trusted Secure Ad-hoc On-Demand Distance Vector (TS-AODV) and Modified Trusted Secure Ad-hoc On-Demand Distance Vector (MTS-AODV). TS-AODV is on-demand gateway discovery protocol where a mobile device of MANET gets connected to gateway. MTS-AODV is based on the node routing behaviour and identifying the attacks such as flooding, black hole, gray hole and denial of service attacks in MANET. MTS-AODV using the Intrusion Detection system (IDS) and trust based routing, the performance results are analysed by varying simulation time. Furthermore, all the above mentioned protocols are compared based on several important performance metrics which are packet delivery ratio, end-to-end delay and average energy.

Keywords*: MANET, IDS, TS-AODV, MTS-AODV, PDR, delay, energy*

INTRODUCTION

The recent trends in wireless communication network have changed the lives of human beings. The new wireless technologies create a potential for the next generation MANET and applications. Wireless technologies such as Bluetooth or the 802.11 standards enable mobile devices to establish a MANET by connecting dynamically through the wireless medium without any centralised structure. MANET is a network having dynamic topology that consists of mobile nodes without base Station or centralized

control. All mobile nodes perform functioning of routers that search and maintain routes to other nodes in the network. Difficulty in ad-hoc network is that for communication with other nodes, a node must be in the transmission range of base station but sometimes a node moves and network fails [1, 2]. MANET has solved this problem as in MANET nodes follow multihop pattern for communicating with other nodes. Routing is the process of moving information across internet work from source to destination by selecting best outgoing path that a packet has to take in internetwork. To perform this, a set of routing protocols needed that uses metrics to find optimal path for a packet to travel. Routing protocols designing goals are optimality, simplicity, low overhead, robustness, reliability and flexibility. Route request and Route reply messages are used to discover and store the paths found from the source to destination. After finding the paths, shortest path is selected by the source node. Paths discovered by shortest path algorithm cause problems like congestion problems as the centre of network carry more traffic, this results in poor performance [3, 4]. The main goals of multipath routing protocols are to maintain reliable communication, to reduce routing overhead by use of secondary paths, to ensure load balancing, to improve quality of service, to avoid the additional route discovery overhead. The major focus of the routing is the performance and the efficiency of the protocol in the presence of a dynamic network environment. The routing protocol has to overcome the security pitfalls to utilize the potentials of the MANET. A secure routing is challenging due to the security vulnerabilities present in the active network.

BACKROUND WORK

This work evolves the previous work that has been undergone in this field. An implementation study of AODV routing protocol was done by Das, *et al*. (2000). Improvement and analysis of multipath routing protocol AOMDV based on CMMBCR was done by Yin-jun Yang (2011). A node disjoint multipath routing method based on AODV protocol for MANET was done by Lal, *et al*. (2012). Increased throughput for load based channel aware routing in MANETs with reusable paths was done by Ayyasamy (2012). Specification based intrusion detection for unmanned aircraft systems was done by Mitchell (2012). A survey of attacks on MANET routing protocols was done by Tayal (2013). Review on MANET routing protocols and challenges was done by Habib (2013). A survey of intrusion detection in wireless network applications was done by Mitchell (2014). Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems was done by Mitchell (2015). Trusted secure ad-hoc on-demand multipath distance vector routing in

MANET was analysis by Abrar Omar Alkhamisi (2016) [5, 6].

EXISTING METHOD

TS-AODV (Trusted Secure Adhoc On-demand Distance Vector Routing Protocol)

In AODV, when a route is needed from source to destination, then source starts a route discovery process by flooding a RREQ for destination. With the help of sequence numbers, RREQs are uniquely identified so that duplicate RREQs can be identified and discarded. When a non-duplicate RREQ is received then intermediate node records previous hop and search for a fresh route entry to the destination in routing table. If fresh route is present then the node sends a RREP to the source but if fresh route is not present, it rebroadcasts the RREQ [7]. The routing information is updated by a node only if a RREP contains either a larger destination sequence number than previous one or a route with less hop count found. TS-AODV routing process with the help of IDS and trust-based routing, the attack identification and isolation in TS-AODV are carried out in two phases of routing such as route discovery phase and data forwarding phase. The trust obtained from IDS is applied in the routing decision-making about propagating RREQ packet of the source and selecting the trust based router for data forwarding. Trust based route discovery process initially, each node assigns the trust value as 'one' to its neighboring nodes. According to the routing activities of these nodes, the IDS measure the original trust value and inform the network layer. The route discovery process is carried out based on the trust value to isolate the flooding attacker activity [8, 9]. Prior to rebroadcasting the received RREQ packet to the neighbors, every node checks for the trust value of the source that has broadcasted the RREQ packet. If the trust value is lesser than the threshold, then the RREQ packet from the corresponding source is dropped to block the flooding activity of the attacker. For instance, in the trust value of the source node is maintained by its neighboring nodes such as A, B, and C. The trust value of the source node is different in various neighboring nodes due to the network collisions. The trust value of the source node is very less, so these nodes do not forward the RREQ packet of the source node into the network. Trust based data forwarding process data forwarding process is carried out based on the trust value to isolate the activity of black hole and the gray whole attacker. Prior to forwarding the data packet to the router, every node checks for the trust value of the router. The trust value of the router indicates the reliability of data delivery through it. If the trust value is low, the current data transmission through the malicious router is blocked. Subsequently, the trusted router from the routing table is accessed to resume data transmission through it. For instance, the trust value of

the node B is higher than node A, and so the source node selects router B for further data forwarding. Thus, the IDS and the trust based TS-AOMDV protocol improve the routing performance and security in MANET.

PROPOSED METHOD

MTS-AODV (Modified Trusted Secure Adhoc On-demand Distance Vector Routing Protocol)

In this proposed work TS-AODV, when a route is needed from source to destination, then source starts a route discovery process by flooding a RREQ for destination. With the help of sequence numbers, RREQs are uniquely identified so that duplicate RREQs can be identified and discarded. When a non-duplicate RREQ is received then intermediate node records previous hop and search for a fresh route entry to the destination in routing table [10]. If fresh route is present then the node sends a RREP to the source but if fresh route is not present, it rebroadcasts the RREQ. The routing information is updated by a node only if a RREP contains either a larger destination sequence number than previous one or a route with less hop count found. MTS-AODV routing process with the help of IDS and trust-based routing, the attack identification and isolation in MTS-AODV are carried out in two phases of routing such as route discovery phase and data forwarding phase. Trust Based Route Discovery Process Initially, each node assigns the trust value as 'one' to its neighboring nodes. Prior to rebroadcasting the received RREQ packet to the neighbors, every node checks for the trust value of the source that has broadcasted the RREQ packet. If the trust value is lesser than the threshold, then the RREQ packet from the corresponding source is dropped to block the flooding activity of the attacker. For instance, in the trust value of the source node is maintained by its neighboring nodes such as A, B, and C. The trust value of the source node is different in various neighboring nodes due to the network collisions. The trust value of the source node is very less, so these nodes do not forward the RREQ packet of the source node into the network. For instance, the trust value of the node B is higher than node A, and so the source node selects router B for further data forwarding. Thus, the IDS and the trust based MTS-AODV protocol improve the routing performance and security in MANET.

EXPERIMENTAL SETUP

The NS-2 which is a discrete event driven simulator developed at UC Berkeley is used in this simulation process. Network Simulator NS-2 is useful in designing new protocols, comparison of different protocols and for evaluating the traffic. A scenario file is taken as input in the NS-2 simulation process that shows the motion of each node and the originating packets by each node. The simulation models are

built using the NS-2 version 2.34 and it is run under bandwidth of 40 MHZ.

Table 1: *Simulation Parameters.*

Parameter	Values
Simulation area	800*800
Number of nodes	50, 100, 150, 200
Average speed of	0–25 meter/second
Mobility model	Random waypoint
Number of packets	40
Constant bit rate	2 (packets/second)
Packet size	512 bytes
Node beacon	0.5 (seconds)
MAC protocol	802.11 DCF
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	500 sec

RESULTS AND DISCUSSION

The results for the above mentioned simulation experiment is shown with the help of graphs. In this section the comparison of TS-AODV and MTS-AODV is made and the metrics used for the analysis of results are packet delivery ratio and end to end delay, energy.

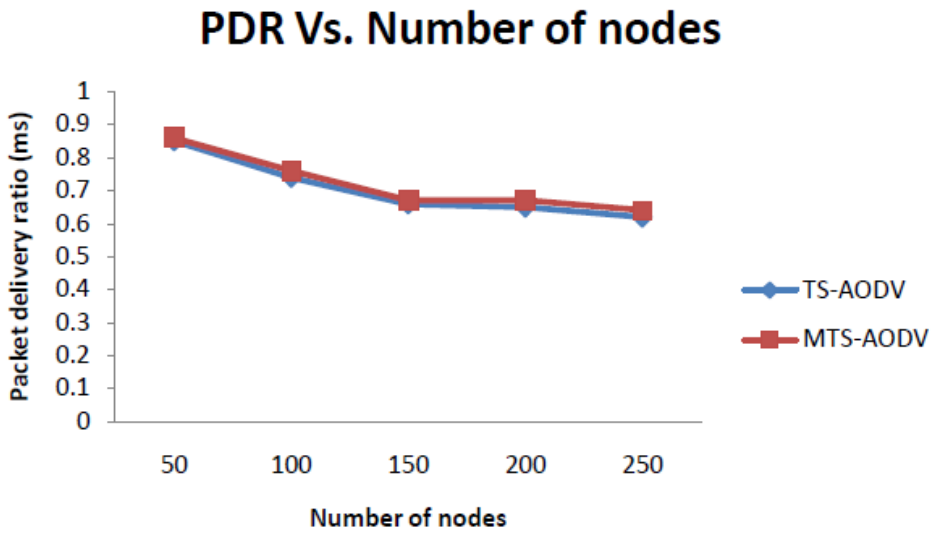

Fig. 1: *Packet Delivery Ratio vs. Number of Nodes.*

It is observed from Figure 1 that when compared with TS-AODV algorithm, MTS-AODV increases the delivery ratio above 85% with the increase in the number of nodes from 50 to 250. As the proposed algorithm finds maximum secure and lowest link failed route with minimum retransmit packets frequently, it is possible to increase the delivery ratio.

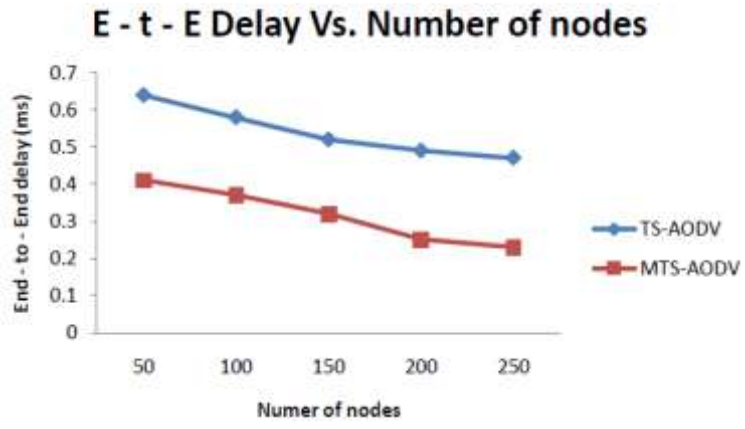

Fig. 2: *End-to-End Delay vs. Number of Nodes.*

MTS-AODV has the lowest delay in comparison with TS-AODV, when there are 1 meter to 800 meters of transmission ranges. When the transmission range increases, the connectivity among the nodes also increases, which enables the

proposed method to identify more number of alternate secondary paths which in turn reduces the delay. Figure 2 describes the decrease in delay obtained by the proposed MTS-AOSV when there are 50 to 250 nodes.

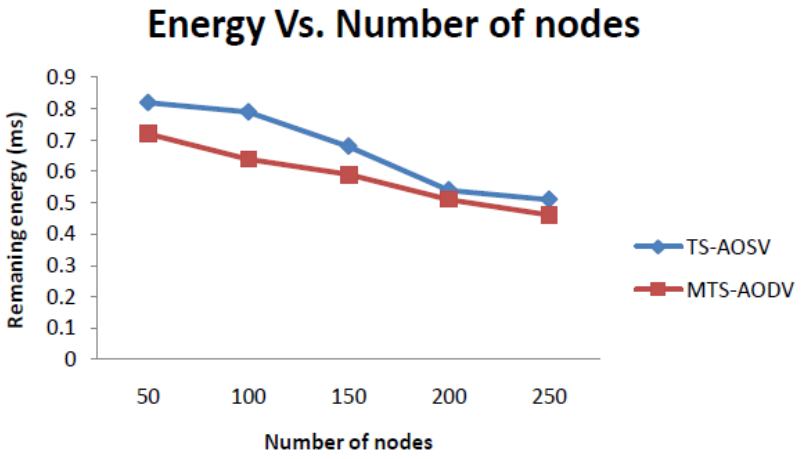

Fig. 3: *Energy vs. Number of Nodes.*

Figure 3 shows the graph of the remaining energy when the topology is size 800 m, the number of nodes increased from 50 to 250. The proposed MTS-AODV increases the remaining energy with the increasing topology size compared to TS-AODV and MTS-AODV.

CONCLUSION AND FUTURE WORK

MTS-AODV, the multipath enhancement to TS-AODV was designed generally for highly dynamic ad hoc networks where link fails and route breaks occur frequently. The comparison was done on basis of packet delivery ratio, end-to-end delay, and energy. On the basis of simulation results it is concluded that MTS-AOMDV is better than TS-AODV. MTS-AODV outperforms TS-AODV due its ability to discover alternate routes when a current link fails. Although MTS-AODV incurs more routing overheads because of flooding the network and packet delays due its alternate route discovery process, it is very much efficient in case of packet delivery for the same reason. MTS-AODV proves to be more efficient than TS-AODV as it provides better throughput. Finally the conclusion is that when network load increases MTSAOMDV is a better on-demand routing protocol than TS-AODV as it gives better statistics for packet delivery and throughput were implementing via network simulator 2. To increase the merits of this research work, there is a plan to investigate the following issues in our future research.

The same concept can be applied in satellite to increase delivery ratio and reduce delay in the route and also to save more energy. The performance of MTS-AODV can be tested in real time network environment.

REFERENCES

1. Das, et al. An implementation study of AODV routing protocol. *Wireless Communication and Networking Conference*. 2000; 3: 1003-1008p.
2. Lal, et al. A node disjoint multipath routing method based on AODV protocol for MANET. *IEEE 26th international Conference on Data Object Identifier*. 2012; 309-405p.
3. Ayyasamy, Venkatachalapathy. Increased throughput for load based channel aware routing in manets with reusable paths. *International Journal of Computer Applications*. 2012; 40(2): 20-23p.
4. Mitchell, Chen. Specification based intrusion detection for unmanned aircraft systems. *Proceedings of the first ACM MANET workshop on Airborne Networks and Communications*. 2012; 31-36p.
5. Tayal, Gupta. A survey of attacks on MANET routing protocols. *International Journal of Innovative Research in Science, Engineering and Technology*. 2013; 2(6): 2280-2285p.
6. Habib, et al. Review on MANET routing protocols and challenges. *IEEE Student Conference on Research and Development SCORED*. 2013; 529-533p.
7. Mitchell, Chen. A survey of intrusion detection in wireless network applications. *Computer Communications*. 2014; 42: 1-23p.
8. Mitchell, Chen. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. *In Dependable and Secure Computing, IEEE Transactions*. 2015; 12(1): 16-30p.
9. Abrar Omar Alkhamisi, Seyed M Buhari. Trusted secure adhoc on-demand multipath distance vector routing in MANET. *IEEE 30th International Conference on Advanced Information Networking and Applications*. 2016.
10. Yin-jun Yang, Xue-ming Wang. Improvement and analysis of multipath routing protocol AOMDV based on CMMBCR. *Wireless Communications, Network and Mobile Computing, 7th International Conference on Digital Object Identifier*. 2016; 1-4p.