INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

DESIGNING AND PERFORMANCE EVALUATION OF ADVANCED TRUST BASED AODV AND DSR ROUTING PROTOCOL

Praveen[1], Vikas Kuchhal[2]

[1]Research scholar, [2]Asst. Prof.
B.M.I.E.T, Sonepat, Haryana,

Abstract: *A dynamic local network i.e. MANETs is formed by a set of mobile wireless nodes. These networks do not have any central control infrastructure. This kind of network can be formed and integrated together. Also, they can be divided into separate networks without depending on any fixed infrastructure management. In this kind of network, each mobile node acts as a router instead of acting just as a host. These nodes also transmit and receive packets to and from other nodes. These features make MANETs to be more robust to security threats. Because the probability of eavesdropping, spoofing denial of service and impersonation attacks increases, MANETs need to be a trust model. So, trust management in MANETs has made variety applications such as security routing. In development of trust management system in MANETs, the highest focus is on developing secure routing protocols based on trust. In this work, we have presented two routing protocols TAODV (Trust based Ad-hoc On Demand Distance Vector Routing) and Modified TDSR (Trust based Dynamic Source Routing). All the input parameters i.e. Total number of nodes, Index of source node, Index of destination node, Node transmission range, Node X-coordinates and Node Y-coordinates and Nodes trust values are same for both of the methods as given in Table 1. Hop-by-hop method is used to find the route in TAODV method and Dijkstra algorithm is used in TDSR method for the same. Also, output parameter i.e. trusted Path Distance, Trusted Path hops, Trusted Path Cost, Trusted Path and computational time are calculated to evaluate the performance of both methods. MATLAB R2013a has been used as an implementation platform.*

Keywords: *MANET, TAODV, Modified TDSR, Dijkstra algorithm .*

1. INTRODUCTION

A mobile ad hoc network is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another device that is immediately within their radio range. Main characteristics of mobile ad hoc network are:

- Dynamic topology- the nodes in the network can move arbitrarily, the topology of the network also changes.
- The bandwidth of the link is constrained and the capacity of the network is also varies tremendously. Because of the dynamic topology, the output of each relay node will vary with the time and then the link capacity will change with the link change.
- Power limitation in mobile devices is a serious factor. Because of the mobility characteristic of the network, devices use battery as their power supply. As a result, the advanced power conservation techniques are very necessary in designing a system.
- The security is limited in physical aspect. The mobile network is easier to be attacked than the fixed network.

Overcoming the weakness in security and the new security trouble in wireless network is on demand. Wireless networks are classified into two categories:

- Infrastructure networks and
- Ad Hoc networks

1.1 Infrastructure networks

An Access Point (AP) represents a central coordinator for every node. Any node can be joining the network via AP. In addition, AP organizes the connection between the Basic Set Services (BSSs) so that the route is ready when it is needed. Major drawback of using an infrastructure network is the large overhead of maintaining the routing tables

1.2 Ad Hoc networks

Ad Hoc networks are remarkable for not depending on any fixed infrastructure to communicate. The main challenge for such networks is the development of robust protocols able to cope with the high probability of topology changes and wireless impairments in place.

A MANET is a collection of mobile nodes sharing a wireless channel without any centralized control or established communication backbone. MANET has dynamic topology and every mobile node has limited resources such as battery, Processing power and on-board memory. This kind of infrastructure-less network is very useful in situation in which ordinary wired networks is not feasible like battlefields, natural disasters etc.

Nowadays, with the immense growth in wireless network applications like handheld computers, PDAs and cell phones, researchers are encouraged to improve the network services and performance. One of the challenging design issues in wireless Ad Hoc networks is supporting mobility in Mobile Ad Hoc Networks (MANETs). The mobility of nodes in MANETs increases the complexity of the routing protocols and the degree of connection's flexibility. However, the flexibility of allowing nodes to join, leave, and transfer data to the network pose security challenges.

MANET (Mobile Ad hoc Networks) ae mobile wireless networks without fixed infrastructure. In an ad hoc network, each node is at the same time a router and a terminal, and is free to change its position with any speed and at any time. Many applications are possible: battlefields, conferences, urgency services.

Although the security requirements are different from one application to another, they are not negligible in most cases. Unfortunately, ad hoc networks are particularly vulnerable due mainly to their lack of infrastructure. Other reasons could be: high mobility, wireless links, Umited bandwidths, lack of boundaries, short lifetime batteries and weak capacity of equipments [1].

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Current ad hoc network security research works can be classified into two principal categories according to their main problematic: the distribution and management of keys and the authentication scheme, and the security of various routing protocols.

Secure routing protocols is a crucial area towards security of MANET. The routing solutions for conventional networks are not sufficient to work efficiently in ad-hoc environment. Most of the existing work [2] in the area of secure routing protocols in an ad hoc network is based on key management, heavy encryption techniques or on continuous promiscuous monitoring of the neighbors. These approaches for making ad hoc routing secure are expensive in terms of network bandwidth as they introduce a heavy traffic load to exchange and verify keys, they also consume lots of nodes' energy and come at the cost of computational complexity of encryption techniques thus they do not fit well for MANET.

Mobile Ad Hoc Network (MANET) is an infrastructure-less network, consisting of a set of mobile nodes without any support of base stations or access points. The mobile nodes are free to change their position with any speed and at any time, and they play the role of terminals and routers allowing hop by hop communication among nodes outside wireless transmission range.

For lack of network infrastructure, the nodes have to communicate cooperatively. Cooperation at the network layer means routing and forwarding packets. Some nodes may deviate from the protocol for selfish or malicious reasons, these nodes are called misbehaving nodes. Selfish nodes wish to use system services while taking an advantage of saving their resources by deviating from regular routing and forwarding. Malicious nodes wish to mount an attack to either a specific node or the network as whole. Both selfish and malicious nodes disrupt the routing protocol operation and reduce the network throughput. This brings up the need for secure routing protocols, where the Routing protocols must cope with such selfish and malicious behavior [3].

MANETs are wireless mobile node systems that dynamically self-organize in arbitrary/ temporary network topologies. A wireless mobile hosts group dynamically establishes a network on the fly, without any communication infrastructure. However, this network architecture and topology are liable to attack internally and externally [4]. Hence, the ultimate goal for MANET security is providing services like authentication, confidentiality, anonymity, integrity, and availability. A weakness in security systems is vulnerability. A system can be vulnerable to unauthorized data manipulation as it does not verify user identity before ensuring data access. MANETs are more vulnerable than wired networks.

2. RELATED WORK

We can characterized the life cycle of mobile ad hoc network into first, second and third generation. Present ad hoc network are considered the third generation. The first generation of ad hoc network can be traced back to 1970's. In 1970's, these are called Packet Radio Network (PRNET). The Defense Advanced Research Project Agency (DARPA) initiated research of using packet- switched radio communication to provide reliable communication between computers and urbanized PRNET. Basically PRNET uses the combination of Areal Location of Hazardous Atmospheres (ALOHA) and Carrier Sense Multiple Access (CSMA) for multiple access and distance vector routing.

The PRNET is then evolved into the Survivable Adaptive Radio Network (SURAN) in the early 1980's. SURAN provides some benefits by improving the radio performance (making them smaller, cheaper and power thrifty). This SURAN also provides resilience to electronic attacks.

Around the same time, United State Department of Defense (DOD) continued funding for programs such Globe Mobile Information System (GloMo) and Near Term Digital Radio (NTDR). GloMo make use of CSMA/CA and TDMA molds, and provides self-organizing and self-healing network (i.e. ATM over wireless, Satellite Communication Network). The NTDR make use of clustering and link state routing and organized an ad hoc network. NTDR is worn by US Army. This is the only "real" ad hoc network in use. By the growing interest in the ad hoc networks, a various other great developments takes place in 1990's. The functioning group of MANET is born in Internet Engineering Task Force (IETF) who worked to standardized routing protocols for MANET and gives rise to the development of various mobile devices like PDA's , palmtops, notebooks, etc . Meanwhile the Development of Standard IEEE 802.11 (i.e. WLAN's) benefited the ad hoc network. Some other standards are also developed that provide benefits to the MANET like Bluetooth and HIPERLAN.

3. PROPOSED METHODOLOGY

In this section we have presented the existing algorithm (AODV) and proposed algorithm (TDSR).

3.1 Implementation steps of AODV:

1. Declaration of some input parameters
   - Total number of nodes
   - Number of source node
   - Number of destination node
   - Node transmission range
   - Nodes x coordinates
   - Nodes y coordinates
   - Nodes trust values
2. Plotting of network topology
3. Declaration of outer loops according to total number of nodes
4. Plotting of current node position according to x-y coordinates
5. Assignment of a number according to current loop to the current node
6. Declaration of inner loops according to total number of nodes
7. Calculation of distance information between two nodes
8. Check if distance is less than maximum transmission range
9. Calculation of average trust values
10. Connection of current node with each other
11. Allocation of distance to another variable.
12. Finding the cost and path from source to destination using hop-by-hop routing by selecting the next hop with the highest trust value.
    - Declaration of empty matrix for required path
    - Assigning of source node as 1st point of path

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

- Checking of real trust value using source, destination node and trust value
- Checking if path exists between source and destination node
- Declaration of a counter for neighbors
- Declaration of a counter path
- Declaration of empty vector of neighbors and trust values
- Declaration of outer loops according to total number of nodes
- Allocation of real trust values to a new variable (empty vector of neighbors and trust values)
- Sorting of trust values in descending order
- Declaration of current trust value as next hop with the highest trust value
- Checking if current source node and current trust value is same or not (if both are not same for current source node and current trust value)
- Checking of real trust value using source, destination node and trust value
- Checking if path exists between source and destination node
- Calculation of average cost of the path

13. Routing by selecting the next hop with the highest trust value
14. Calculation of number of hopes involved in the path
15. Calculation of total distance for whole path
16. Declaration of a loop according to number of hopes involved in the path
17. Display of final selected path

3.2 Implementation steps of TDSR:

1. Declaration of some input parameters
   - Total number of nodes
   - Number of source node
   - Number of destination node
   - Node transmission range
   - Nodes x coordinates
   - Nodes y coordinates
   - Nodes trust values
2. Plotting of network topology
3. Declaration of outer loops according to total number of nodes
4. Plotting of current node position according to x-y coordinates
5. Assignment of a number according to current loop to the current node
6. Declaration of inner loops according to total number of nodes
7. Calculation of distance information between two nodes
8. Check if distance is less than maximum transmission range
9. Calculation of average trust values
10. Connection of current node with each other
11. Allocation of distance to another variable.
    - Finding the cost and path from source to destination using Dijkstra algorithm
    - Check if first element of trust matrix is a real value
    - Calculation of current distance of path
    - Declaration of first node as parent node
    - Exploration and analyzing the whole graph
    - Updation of distance of path
    - Updation of distance of path
    - Back-tracing of the shortest-path
    - Calculation of the cost according the distance matrix
12. Calculation of the final cost
13. Calculation of number of hopes involved in the path
14. Calculation of total distance for whole path
15. Declaration of a loop according to number of hopes involved in the path
16. Display of final selected path

4. EXPERIMENTAL RESULTS

In this section, we have presented two routing protocols TAODV (Trust based Ad-hoc On Demand Distance Vector Routing) and Modified TDSR (Trust based Dynamic Source Routing). All the input parameters i.e. Total number of nodes, Index of source node, Index of destination node, Node transmission range, Node X-coordinates and Node Y-coordinates and Nodes trust values are same for both of the methods as given in Table 1. Hop-by-hop method is used to find the route in TAODV method and Dijkstra algorithm is used in TDSR method for the same.

Table 1: Input Parameters and their values

Parametrs/Routing Protocol	**TAODV and TDSR**
Total number of nodes/hopes used	10
Index of source node	1
Index of destination node	10
Node transmission range	5
Node X-coordinates	1,2,3,4,8,6,7,9,10,10
Node Y-coordinates	6,2,5,8,5,1,10,2,8,5
Nodes Trust Value	1,1,0.7,0.4,0.1,0.1,0.1 ,1,1,1

There are 4 snapshots below showing the network topologies and and values of output parameters for both methods. Figure 1 is the snapshot of shortest route selected by TAODV protocol. Figure 2 is the snapshot of output parameters i.e. Trusted Path Distance, Trusted Path hops, Trusted Path Cost and Trusted Path TAODV protocol. Figure 3 is the snapshot of shortest route selected by TDSR protocol. Figure 4 is the snapshot of output parameters i.e. Trusted Path Distance, Trusted Path hops, Trusted Path Cost and Trusted Path for TDSR protocol. Also, the values of output parameters have been given in Table 2. These values for both methods are also presented graphically. Figure 5 is the snapshot of comparison of Distance of path selected. Figure 6 is the snapshot of comparison of number of hopes used. Figure 7 is the snapshot of comparison of path cost. Figure 8 is the snapshot of comparison of computation time.

Volume 4, Issue VII, July 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

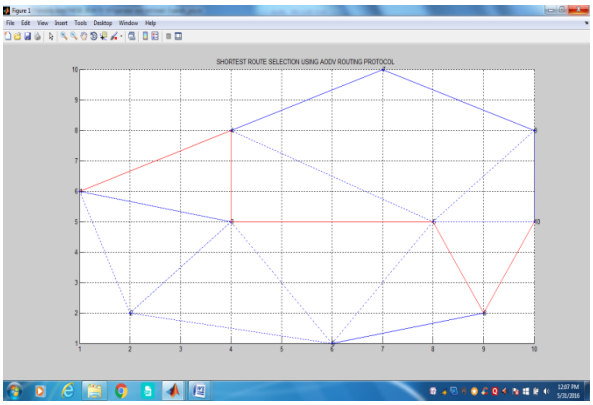

Figure 1: snapshot of shortest route selected by TAODV protocol.

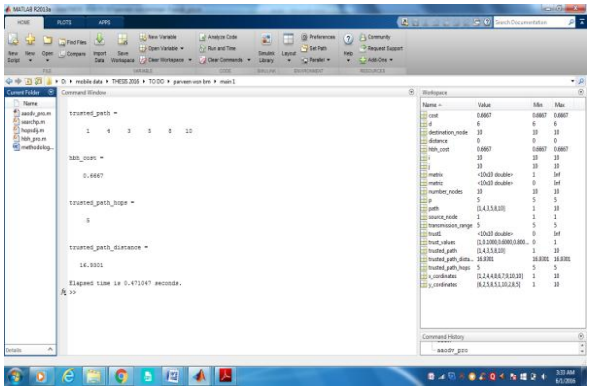

Figure 2: snapshot of output parameters i.e. Trusted Path Distance, Trusted Path hops, Trusted Path Cost and Trusted Path TAODV protocol

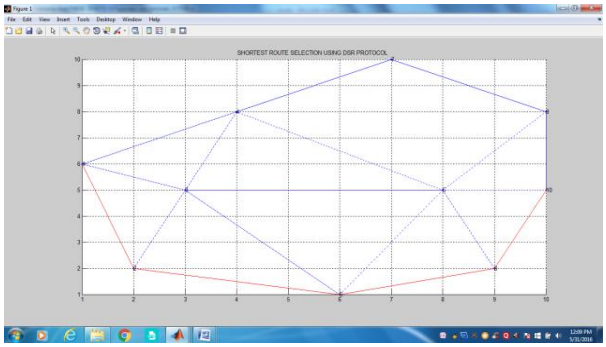

Figure 3: snapshot of shortest route selected by TDSR protocol

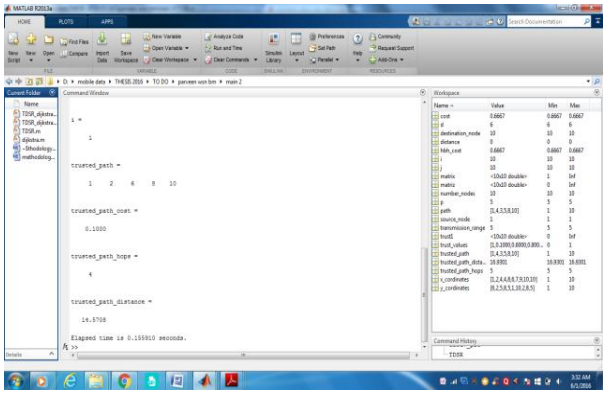

Figure 4: snapshot of output parameters i.e. Trusted Path Distance, Trusted Path hops, Trusted Path Cost and Trusted Path for TDSR protocol

Table 2: Comparison of TDSR and TAODV routing protocol

Parameters/ Algorithm	TAODV	TDSR
Trusted Path Distance	16.9301	14.5708
Trusted Path hops used	5	4
Trusted Path Cost	0.6667	0.1000
Trusted Path	1-4-3-5-8-10	1 -2-6-8-10
Computational time	0.471047	0.171371

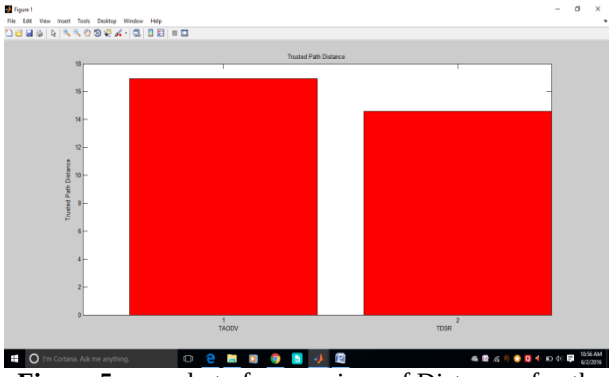

Figure 5: snapshot of comparison of Distance of path selected

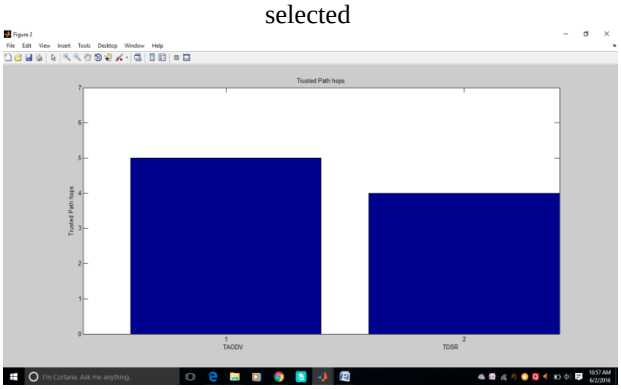

Figure 6: snapshot of comparison of number of hopes used

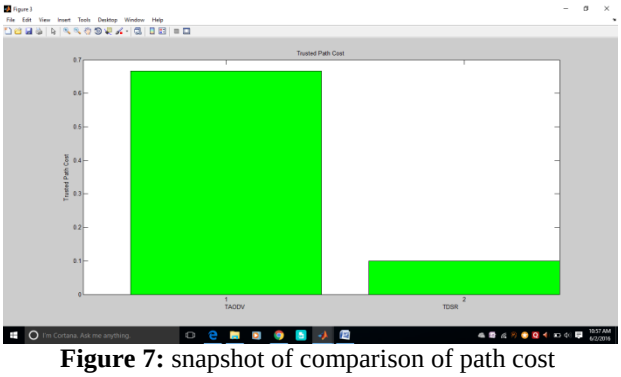

Figure 7: snapshot of comparison of path cost

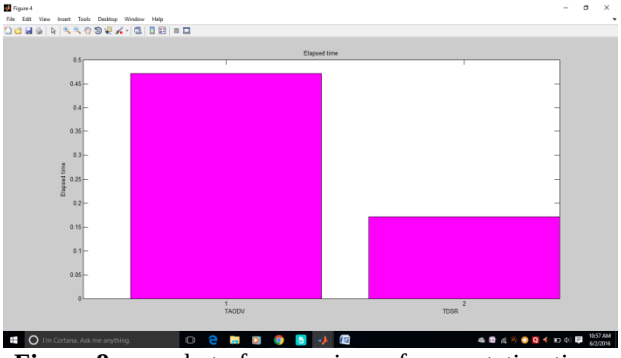

Figure 8: snapshot of comparison of computation time

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

5. CONCLUSION

The inherent nature of MANETs provokes the appearance of new security hazards, while some existing weaknesses in wired networks are emphasized. To secure MANET from such hazards notion of trust has come in the field of MANET security. Trust is a more complex subject in physiological environment and it is influencing of assumptions, expectations, behaviors, environments, and other factors. In an advanced wireless network, trust is desirable for all routing protocols to secure data transmission. An enormous volume of important information communicates over the wireless network using trusted dynamic routing protocol, which is the enhancement of the DSR (Dynamic Source Routing) protocol to improve trust. It can be concluded from the experimental results that Modified TDSR protocol is much efficient in finding the shortest from source node to destination node as compared to TAODV protocol. The proof of above statement is Trusted Path Distance, Trusted Path hops, Trusted Path Cost, Trusted Path and computation time. The value of all the five parameters for Modified TDSR protocol is much optimized as compared to TAODV protocol.

References

[1] Xiaoyun Xue and Jean Leneutre, "A TRUST-BASED ROUTING PROTOCOL FOR AD HOC NETWORKS," INFRES department, ENSTParis - CNRSLTCI-UMR5141, 46 rue Barrault 75634 Paris Cedex 13.

[2] Deepika Kukreja, Umang Singh, and B. V. R. Reddy, "A Survey of Trust Based Routing Protocols in MANETs," Journal of Advances in Computer Networks, Vol. 1, No. 4, December 2013

[3] Ahmed M. Abd El-Haleem and Ihab A. Ali, "TRIDNT: THE TRUST-BASED ROUTING PROTOCol WITH CONTROLLED DEGREE OF NODE SELFISHNESS FOR MANET," International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.

[4] N SATHEESH, Dr. K. PRASADH, "TRUST BASED AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL AGAINST WORMHOLE ATTACK," Journal of Theoretical and Applied Information Technology 31st December 2014. Vol.70 No.3

[5] Mohana, N.K. Srinath, Amit L.K, "Trust Based Routing Algorithms for Mobile Ad-hoc Network," ISSN 2250-2459, Volume 2, Issue 8, August 2012

[6] Chi Zhang, Xiaoyan Zhu, Yang Song and Yuguang Fang, "A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks," This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2010 proceedings.