IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-2 E-ISSN: 2347-2693

Trust based Multipath Routing Scheme (TMAODV)

Nikhat Raza Khan[1*], Sanjay Sharma[2], P.S. Patheja[3]

[1*]Department of Computer Science and Engineering, Mewar University, Chittorgarh, India
[2]Department of M.C.A, Maulana Azad National Institute of Technology, Bhopal, India
[3]Department of Computer Science and Engineering, Vellore Institute of Technology, Bhopal, India

**Corresponding Author: nikhat.raza@gmail.com +919826087555*

Available online at: www.ijcseonline.org

Received: 22/Jan/2018, Revised: 31/Jan/2018, Accepted: 13/Feb/2018, Published: 28/Feb/2018

Abstract— Malicious nodes in MANETS can make considerable damage. As basic routing protocols does not provide any strong security against internal attacks nodes, they can easily become part of network and degrade the performance by launching attack.In this work, the main focus is to develop a method of security in communications between ad-hoc network nodes. This proposed model i.e Trust based Multipath Routing Protocol Scheme (TMAODV), firstly calculates transmission cost and then trust factor is calculated on the basis of number of packets forward and dropped. For this a new data structure is added into neighborhood table. Secondly, a different computation factors like Optimal Traffic Ratio, Remaining Energy value and transmission cost is calculated and this data structure is stored by routing table.

Keywords— MANET,TMAODV, Optimal Traffic Ratio, Transmission Cost, Remaining Energy

I. Introduction

There are different kinds of attack exists which can be imposed by internal attackers e. g. rushing attack, blackhole attack, neighbor attack, jellyfish attack etc. [6]. Here, the packet dropping attack by malicious nodes is considered for both MAODV and PUMA protocols. These malicious nodes shows normal activity (doesn't drop or alter any control packet) to become part of data packet paths. It does not drop or alter any control packet required by MAODV and PUMA for their working. Due to this activity it becomes difficult to locate its presence in network. When it becomes the part of route i.e. data packet forwarding mechanism, upon receiving the data packet, it drops the data packets instead of forwarding it to next node in data packet route. This data packet dropper malicious node causes less packet delivery ratio in both MAODV and PUMA.

To address and avoid packet dropper malicious nodes in MAODV, authors proposed trust based security (TMAODV). TMAODV elects shortest trustworthy path from available paths. Trust values are used along with hop count to evaluate the trust of the path. As discussed earlier there exists two kind of trust calculations: Recommendation (indirect) based trust calculation and non-recommendation (direct) based trust calculation. In recommendation based trust calculation, node uses its own knowledge and second hand information obtained from other nodes to derive final trust. Indirect trust calculation needs extra control packet exchange between nodes to obtain second hand information. This extra control packet exchange between nodes may incur additional communication cost for trust exchange. In direct trust calculation, node simply uses its direct observations to evaluate the trust values of other nodes.

II. Methodology

This trust based security model uses direct trust calculation method in which nodes evaluates trust using the history of direct interactions between them. In this model, positive and negative responses are used as observable factors for assessing trust. In MANET, promiscuous mode allows nodes to monitor its neighbors. This mode allows node to listen every message transmitted by the nodes which are within its transmission range. To record positive and negative responses and to calculate trust, an extra table is maintained at each node. This table is further used for secure route construction. The proposed mechanism is explained in detail as following:

A. Trust evaluation with direct observation

To keep the track of neighboring node an extra data structure (neighbour table) is added at each node. This table is used by each node to calculate the belief (trust) of its neighboring node. For the path trust calculation and path selection, this table is referred.

Node	**FCount (α)**	**DCount (β)**	**Belief**

Neighbour Table for Trust based Model

In above figure, the first column indicates the node id of neighbor node, the second column Fcount indicates the counts of data packets successfully forwarded by the that node third column indicates the counts of data packets dropped by the next node and belief column indicates trust values calculated for corresponding node. In promiscuous mode each node listens the packet transmitted by its neighbor node. When node forwards data packet to next node (except receiver) in data path, it expects the next node to forward that data packet. When that next node forwards data packet its Į count is increased by one otherwise its ù count increased by one. When node forwards the data packet to next node on the data packet route, it adds that nodes entry in neighbour table and starts observing its behaviour in terms of α and β. As end tree node in MAODV doesn't forward data, for the accurate calculation of α and β, an extra control packet is used, which is only sent by end tree node to previous node only once.

The Algorithm of this model is as:

Algorithm 1: α, β and belief Calculation in MAODV

```
Input: forward(packet):executed at each node when it forwards packet to next node
if(packet_type==data_packet)then
node = neighbour_lookup(next_node in datapath);
if(node!=null)then
Then
node(forward_count)=node(forward_count)+1;
else
neighbour_add(node);
node(forward_count)=1;
node(receive_count)=0;
End if
End if
Input: tap(packet):executed at each node when it listens packet transmitted by its neighbor
if(packet_type==data_packet) then
node=neighbourwatch_lookup(packet forwarder node);
if (node!=null) then
node(recieve_count)=node(recieve_count)+1;
else
 neighbour_add(node);
 node(receive_count)=1;
node(forward_count)=0;
end if
 end if
Input: cal():executed at each node at regular interval
α=0;
 β=0;
node=first_node in neighbour table;
while (node) do
α=node(receive_count);
β=node(forward_count) − node(receive_count);
belief = α /  (α+ β+1);
insert(α β and belief in neighbour table);
node=next_node in neighbour table;
end while
Algorithm 1: To Setup Route
Input: Control Packets (CP)
Initialize: $T_c$=0;
Broadcast Control Packets;
If received by neighbours
Then
Store in Routing Neighbourhood Table (N-Table)
Calculate Transmission Cost $T_c = \frac{1}{p\times q}$
Else if node is destination
Then
Set $T_c$=0;
Broadcast it to Neighbours.
End if
Else
Find Neighbours
End if
```

The trust of neighboring nodes is evaluated in terms of trust values at each node. These values are calculated using Į and ù values at regular interval. In proposed security, the direct trust between node i and j is calculated using Bayesian inference (expectation of beta distribution) [18]

$$T_{ij} = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij} + 1}$$

Where T_{ij} is the trust calculated by node i for node j. α_{ij} is the number of data packets forwarded by node j which has been sent by node i to it. β_{ij} is the number of data packets not forwarded by node j which has been sent by node i to it. As data packet transmission continues in network these trust values are updated at regular intervals.

III. Results and Discussion

In this work, two protocols AOMDV and TMAODV are implemented using NS-2 simulator. TMAODV is trust based multipath protocol where trust of a path is calculated on the

basis of nodes' communication that is packet forward and dropped by a node. These protocols are simulated in the area 1000x1000 m^2. Implementation is done using different scenarios to test the performance of the protocols.
The scenarios implemented for testing are as given below:

A. *Scenario1: Varying Nodes*

To test the performance of the protocols 50, 100, 150 and 200 nodes are deployed in the area of 1000x1000 m^2 with maximum speed of 50m/s. Simulation is carried out using CBR traffic with maximum 40 connections. Other parameters are as given in the table 1.

Table 1: Simulation Setup

Simulation Parameters	**Values**
Area	1000x1000
No. of nodes	50,100,150,200
Speed	0~50m/s
Traffic	CBR
Packet Size	1000 bytes
Packet Rate	250k/s
Pause Time	500s
Simulation Time	1000s
Max Connection	40
Routing Protocol	AOMDV & EMPSO

Results Parameters:

a. Packet Delivery Ratio: This trust based protocol (TMAODV) performs better than AOMDV and achieves 67% improvement in Packet Delivery Ratio. The comparison of these protocols by varying nodes is as given in table 2.

Table 2: Packet Delivery Ratio

	PDR			
	50	100	150	200
AOMDV	23.0701	23.508	34.3308	33.9252
TAOMDV	90.831	86.931	88.39	85.311

Figure 1 shows the performance of both protocols. This figure also shows that PDR increases with the increase number of nodes and more than AOMDV.

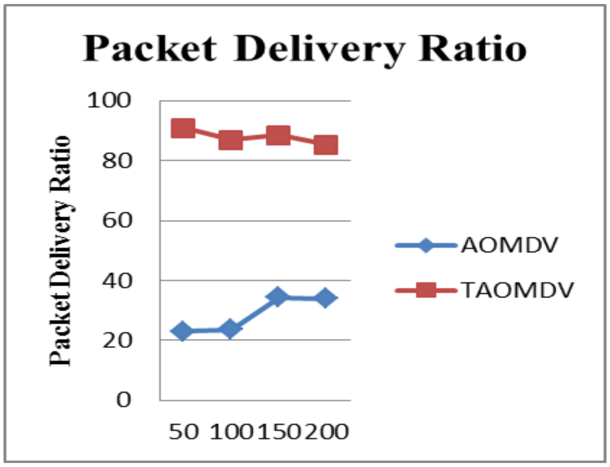

Figure 1: Packet Delivery Ratio (Scenario-1)

b. Overhead: This trust based protocol (TMAODV) performs better than AOMDV and achieves 41% improvement in Overhead. The comparison of these protocols by varying nodes is as given in table 3.

Table 3: Overhead

	Overhead			
	50	100	150	200
AOMDV	15.431	32.664	26.28	26.407
TAOMDV	9.352	12.378	16.361	19.726

Figure 2 shows the performance of both protocols. This figure shows that Overhead increases with the increase number of nodes but less than AOMDV.

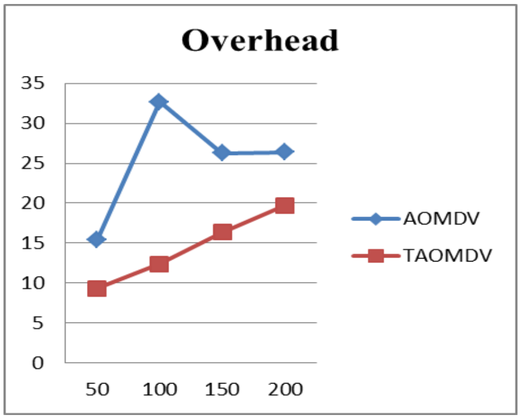

Figure 2: Overhead (Scenario-1)

c. Delay: This trust based protocol (TMAODV) performs better than AOMDV and achieves 28% improvement in

Delay. The comparison of these protocols by varying nodes is as given in table 4.

Table 4: Delay

	Delay			
	50	100	150	200
AOMDV	0.07	0.06	0.04	0.05
TAOMDV	0.04	0.06	0.02	0.04

Figure 3 shows the performance of both protocols. This figure shows that Delay increases with the increase number of nodes but less than AOMDV.

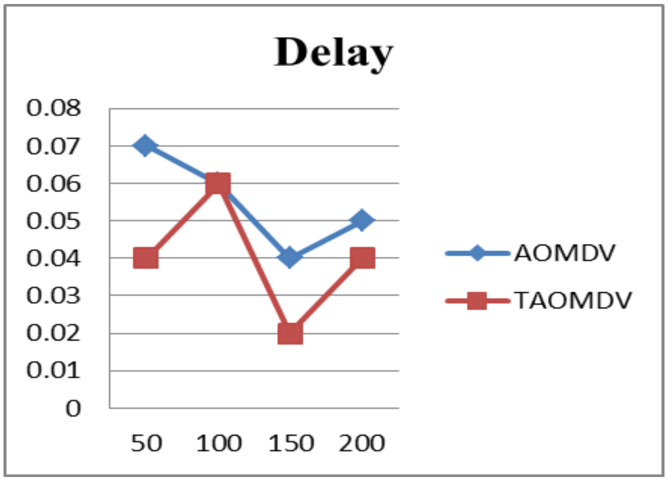

Figure 3: Delay (Scenario-1)

d. Throughput: This trust based protocol (TMAODV) performs better than AOMDV and achieves 39% improvement in Delay. The comparison of these protocols by varying nodes is as given in table 5.

Table 5: Throughput

	Throughput			
	50	**100**	**150**	**200**
AOMDV	51.55	56.54	47.59	59.18
TAOMDV	93.38	89.48	92.36	84.32

Figure 4 shows the performance of both protocols. This figure shows that Throughput increases with the increase number of nodes and more than AOMDV.

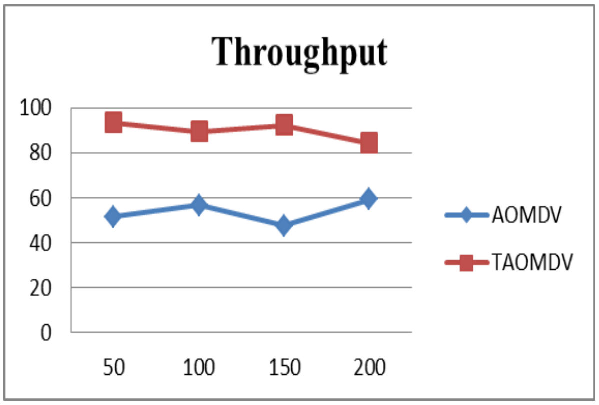

Figure 4: Throughput (Scenario-1)

e. Total Energy Consumption: This trust based protocol (TMAODV) performs better than AOMDV and achieves 8% improvement in Delay. The comparison of these protocols by varying nodes is as given in table 6.

Table 6: Total Energy Consumption

	Total Energy			
	50	**100**	**150**	**200**
AOMDV	4896.06	9764.28	14869.5	19835.8
TAOMDV	4173.37	9328.18	13845.3	18023.3

Figure 5 shows the performance of both protocols. This figure shows that Total Energy consumption increases by increasing number of nodes but less than AOMDV.

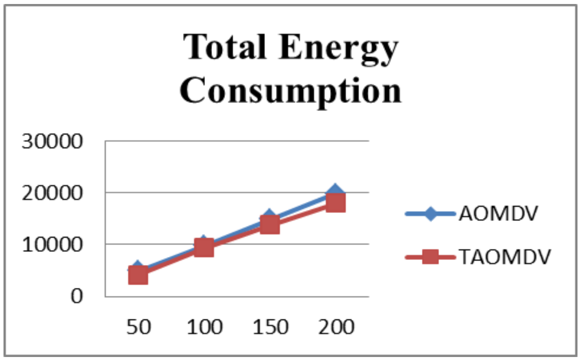

Figure 5: Total Energy Consumption (Scenario-1)

B. Scenario2: Varying Packet Size

To test the performance of the protocols 50 nodes are deployed in the area of 1000x1000 m^2 with maximum speed of 50m/s and by varying packet size from 200 to 1000 bytes. Simulation is carried out using CBR traffic with maximum 40 connections. Other parameters are as given in the table 7.

Table 7: Simulation Setup

Simulation Parameters	Values
Area	1000x1000
No. of nodes	50
Speed	0~50m/s
Traffic	CBR
Packet Size	200,400,600,800,1000 bytes
Packet Rate	250k/s
Pause Time	500s
Simulation Time	1000s
Max Connection	40

Results Parameters:

a. Packet Delivery Ratio: This trust based protocol (TMAODV) performs better than AOMDV and achieves 50% improvement in Packet Delivery Ratio. The comparison of these protocols by varying packet size is as given in table 8.

Table 8: Packet Delivery Ratio

	PDR				
	200	400	600	800	1000
AOMDV	49.2347	28.3298	25.6825	18.4943	23.0701
TAOMDV	51.361	55.289	58.371	60.335	90.831

Figure 6 shows the performance of both protocols. This figure also shows that PDR increases with the increase in packet size and more than AOMDV.

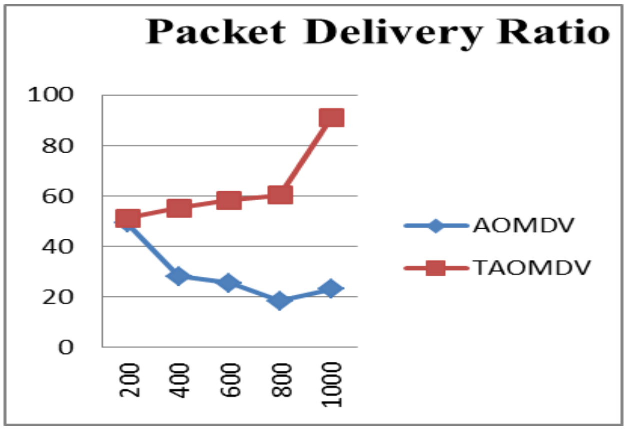

Figure 6: Packet Delivery Ratio (Scenario-2)

b. Overhead: This trust based protocol (TMAODV) performs better than AOMDV and achieves 13% improvement in Overhead only in case of 800 and 1000 Packet size. The comparison of these protocols by varying packet size is as given in table 9.

Table 9: Overhead

	Overhead				
	200	400	600	800	1000
AOMDV	5.582	7.855	7.424	14.884	15.431
TAOMDV	16.375	15.753	13.027	10.836	9.352

Figure 7: shows the performance of both protocols. This figure shows that Overhead decreases with the increasing packet size and is less than AOMDV in case of 800 and 1000 packet size.

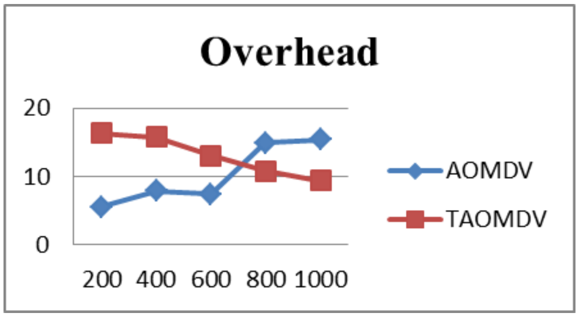

Figure 7: Overhead (Scenario-2)

c. Delay: This trust based protocol (TMAODV) performs better than AOMDV and achieves 8% improvement in Delay. The comparison of these protocols by varying packet size is as given in table 10.

Table 10: Delay

	Delay				
	200	400	600	800	1000
AOMDV	0.02	0.02	0.02	0.02	0.07
TAOMDV	0.02	0.02	0.03	0.05	0.04

Figure 8 shows the performance of both protocols. This figure shows that Delay decreases with the increasing packet size and is less than AOMDV in case of 1000 packet size.

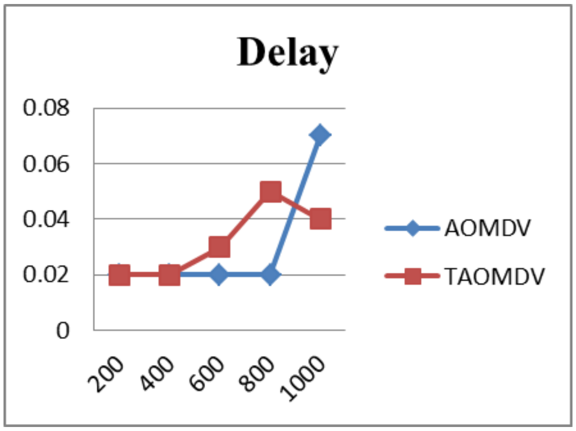

Figure 8: Delay (Scenario-2)

d. Throughput: This trust based protocol (TMAODV) performs better than AOMDV and achieves 31% improvement in Throughput. The comparison of these protocols by varying packet size is as given in table 11.

Table 11: Throughput

	Throughput				
	200	400	600	800	1000
AOMDV	33.54	36.15	60.13	41.9	51.55
TAOMDV	38.27	58.38	70.03	81.71	93.38

Figure 9: shows the performance of both protocols. This figure shows that Throughput increases with the increasing packet size and is more than AOMDV.

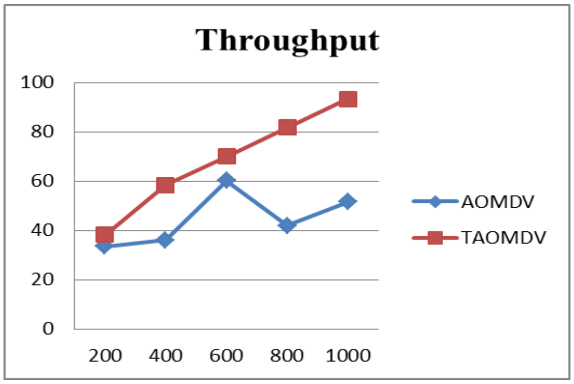

Figure 9: Throughput (Scenario-2)

e. Total Energy Consumption: This trust based protocol (TMAODV) performs better than AOMDV and achieves 14% improvement in Total Energy Consumption. The comparison of these protocols by varying packet size is as given in table 12.

Table 12: Total Energy Consumption

	Total Energy				
	200	400	600	800	1000
AOMDV	4992.59	4866.33	4823.25	4778.94	4896.06
TAOMDV	4538.41	4235.39	3972.85	3836.47	4173.37

Figure 10 : shows the performance of both protocols. This figure shows that Total Energy Consumption decreases with the increasing packet size and is less than AOMDV.

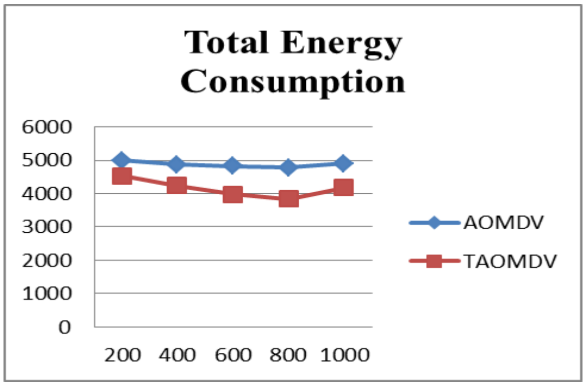

Figure 10 Total Energy Consumption (Scenario-2)

C. Scenario 3: Varying Speed

To test the performance of the protocols 50 nodes are deployed in the area of 1000x1000 m^2 with varying speed by 10, 20, 30,40 and 50m/s with fixed packet size of 1000 bytes. Simulation is carried out using CBR traffic with maximum 40 connections. Other parameters are as given in the table 13.

Table 13: Simulation Setup

Simulation Parameters	Values
Area	1000x1000
No. of nodes	50
Speed	10,20,30,40,50 m/s
Traffic	CBR
Packet Size	1000 bytes
Packet Rate	250k/s
Pause Time	500s
Simulation Time	1000s
Max Connection	40

Results Parameters

a. Packet Delivery Ratio: This trust based protocol (TMAODV) performs better than AOMDV and achieves 73% improvement in Packet Delivery Ratio. The comparison of these protocols by varying node speed is as given in table 14.

Table 14: Packet Delivery Ratio

	Packet Delivery Ratio				
	10	20	30	40	50
AOMDV	23.3564	10.2126	27.8491	19.4062	14.9668
TAOMDV	65.3821	69.371	71.271	79.836	82.474

Figure 11 shows the performance of both protocols.
This figure shows that PDR increases with the increasing speed and is more than AOMDV.

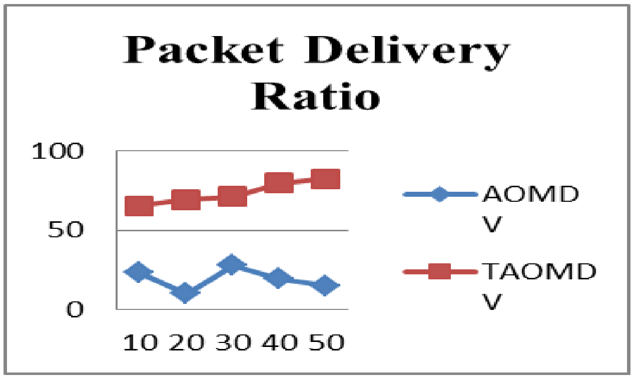

Figure 11: Packet Delivery Ratio (Scenario-3)

b. Overhead: This trust based protocol (TMAODV) performs better than AOMDV and achieves 42%

improvement in Overhead. The comparison of these protocols by varying node speed is as given in table 15.

Table 15: Overhead

	Overhead				
	10	20	30	40	50
AOMDV	9.269	23.539	8.17	13.07	15.545
TAOMDV	5.382	5.937	7.03	7.402	9.482

Figure 12 shows the performance of both protocols. This figure shows that Overhead increases with the increasing speed and is less than AOMDV.

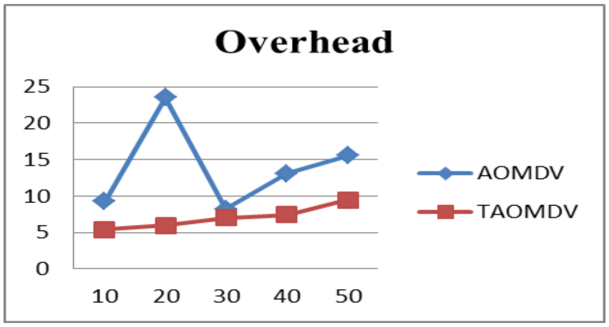

Figure 12: Overhead (Scenario-3)

c. Delay: This trust based protocol (TMAODV) performs better than AOMDV and achieves 16% improvement in Delay. The comparison of these protocols by varying node speed is as given in table 16.

Table 16: Delay

	Total Energy				
	10	20	30	40	50
AOMDV	4988.97	4837.62	5057.01	5047.23	5012.22
TAOMDV	4793.27	4638.84	4884.42	4936.87	4993.65

Figure 13: shows the performance of both protocols. This figure shows that Delay increases with the increasing speed and is less than AOMDV.

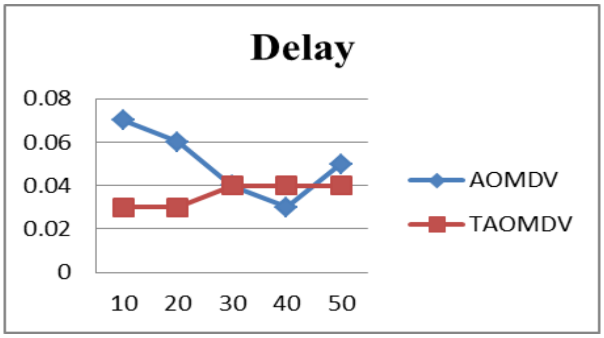

Figure 13: Delay (Scenario-3)

d. Throughput: This trust based protocol (TMAODV) performs better than AOMDV and achieves 26% improvement in Throughput. The comparison of these protocols by varying node speed is as given in table 16.

Table 16: Throughput

	Throughput				
	10	20	30	40	50
AOMDV	77.9	40.63	80.91	50.17	46.04
TAOMDV	75.38	79.37	80.99	82.37	84.72

Figure 14: shows the performance of both protocols. This figure shows that Throughput increases with the increasing speed and is more than AOMDV.

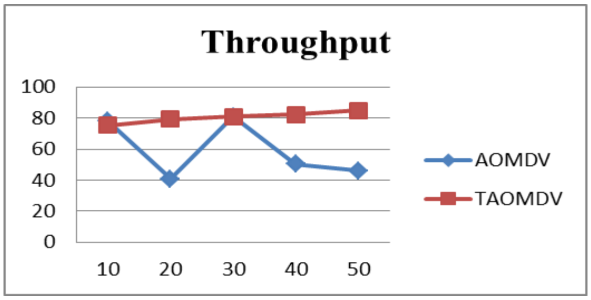

Figure 14: Throughput (Scenario-3)

e. Total Energy Consumption: This trust based protocol (TMAODV) performs better than AOMDV and achieves 2% improvement in Total Energy Consumption. The comparison of these protocols by varying node speed is as given in table 17.

Table 17: Total Energy Consumption

	Delay				
	10	20	30	40	50
AOMDV	0.07		0.04	0.03	0.05
TAOMDV	0.03	0.03	0.04	0.04	0.04

Figure 15: shows the performance of both protocols. This figure shows that Total Energy Consumption increases with the increasing speed and is less than AOMDV.

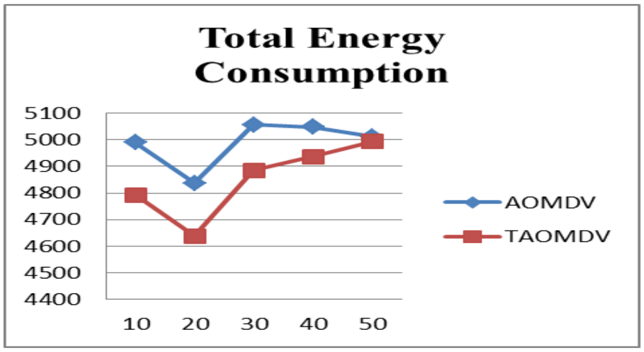

Figure 15: Total Energy Consumption (Scenario-3)

IV. Conclusion

In this research work, the analysis of the base protocol which is based on Security Multipath Routing Scheme with Path Trust Mechanism is done. This protocol is implemented and tested on three different scenarios where its performance is measured in terms of different parameters. The resultant parameters show that this trust based protocol performs better than AOMDV in all aspects. So, this protocol will be used in further work to enhance the performance of Mobile Ad hoc Network in terms of security.

Acknowledgment

I am indebted to my thesis supervisor Dr. Sanjay Sharma Prof. & head dept. of MCA MANIT, Bhopal for all their guidance and help. Their kind encouragement and motivation during the preparation of this thesis is highly appreciated.

I wish to express my heartiest regards to my Co- supervisor Prof Dr. Pushpinder Singh Patheja, Associate Professor, Vellore Institute of Technology Bhopal, who assisted me and provided help throughout my research work.

I express my appreciation and gratitude to all my family members for their encouragement, moral support, understanding and patience throughout the span of research work..

References

[1] Kush, A., Taneja, S., & Sharma, D. (2010). Energy efficient routing for MANET. 2010 International Conference on Methods and Models in Computer Science (ICM2CS-2010).

[2] Guodong, W., Gang, W., & Jun, Z. (2010). ELGR: An Energy-efficiency and Load-balanced Geographic Routing Algorithm for Lossy Mobile Ad Hoc Networks. Chinese Journal of Aeronautics, 23(3), 334-340.

[3] Fareena, N., Mala, A. S., & Ramar, K. (2012). Mobility Based Energy Efficient Multicast Protocol for MANET. Procedia Engineering, 38, 2473-2483.

[4] Jamali, S., Rezaei, L., & Gudakahriz, S. J. (2013). An Energy-efficient Routing Protocol for MANETs: a Particle Swarm Optimization Approach. Journal of Applied Research and Technology, 11(6), 803-812.

[5] Choukri, A., Habbani, A., & Koutbi, M. E. (2014). An energy efficient clustering algorithm for MANETs. 2014 International Conference on Multimedia Computing and Systems (ICMCS).

[6] S.S. Basurra, M. De Vos, J. Padget, Y. Ji, T. Lewis, S. Armour,(2014). Energy Efficient Zone based Routing Protocol for MANETs, Ad Hoc Networks (2014)

[7] Choudhury, D., Kar, D., Biswas, K. R, Saha, H. (2015). Energy efficient routing in mobile ad-hoc networks. 2015 International Conference and Workshop on Computing and Communication (IEMCON).

[8] Das, S. K., & Tripathi, S. (2015). Energy Efficient Routing Protocol for MANET Based on Vague Set Measurement Technique. Procedia Computer Science, 58, 348-355.

[9] Divya, M., Subasree, S., & Sakthivel, N. (2015). Performance Analysis of Efficient Energy Routing Protocols in MANET. Procedia Computer Science, 57, 890-897.

[10] Patil, M., Naik, S. R., Nikam, V. B., & Joshi, K. K. (2015). Extended ECDSR protocol for energy efficient MANET. 2015 International Conference on Advanced Computing and Communication Systems.

[11] Sara, Z., & Rachida, M. (2015). Energy-Efficient Inter-Domain Routing Protocol for MANETs. Procedia Computer Science, 52, 1059-1064.

[12] Sumathi, K., & Priyadharshini, A. (2015). Energy Optimization in Manets Using On-demand Routing Protocol. Procedia Computer Science, 47, 460-470.

[13]ashkaar, M., & Sharma, P. (2016). Enhanced energy efficient AODV routing protocol for MANET. 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS).

[14] Dodke, S., Mane, P. B., & Vanjale, M. (2016). A survey on energy efficient routing protocol for MANET. 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT).

[15] Kaliappan, M., Augustine, S., & Paramasivan, B. (2016). Enhancing energy efficiency and load balancing in mobile ad hoc network using dynamic genetic algorithms. Journal of Network and Computer Applications, 73, 35-43.

[16] Kuo, W., & CHU, S. (2016). Energy Efficiency Optimization for Mobile Ad Hoc Networks. IEEE Access, 4, 928-940.

[17] Logambal, R., & Chitra, K. (2016). Energy efficient hierarchical routing algorithm in MANETs. 2016 IEEE International Conference on Advances in Computer Applications (ICACA).

[18] Tiwari, A., & Kaur, I. (2017). Performance evaluaron of energy efficient for MANET using AODV routing protocol. 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT).

[19] Zahary, A., & Ayesh, A. (2010). An analytical review for multipath routing in Mobile Ad Hoc Networks. International Journal of Ad Hoc and Ubiquitous Computing, 5(2), 69.

[20] Savitha, K., & Chandrasekar, C. (2013). An energy aware enhanced AODV routing protocol in MANET. International Journal of Communication Networks and Distributed Systems, 10(3), 233.

[21] Singh, R., & Gupta, S. (2014). EE-AODV: Energy Efficient AODV routing protocol by Optimizing route selection process . International Journal of Research in Computer and Communication Technology, 3(1), 158-163.

[22] Jain, H. R., & Sharma, S. K. (2014). Improved energy efficient secure multipath AODV routing protocol for MANET. 2014 International Conference on Advances in Engineering & Technology Research (ICAETR - 2014).

[23] Kanakala, S., Ananthula, V. R., & Vempaty, P. (2014). Energy-Efficient Cluster Based Routing Protocol in Mobile Ad Hoc Networks Using Network Coding. Journal of Computer Networks and Communications, 2014, 1-12.

[24] Jabbar, W. A., Ismail, M., & Nordin, R. (2014). On the Performance of the Current MANET Routing Protocols for VoIP, HTTP, and FTP Applications. Journal of Computer Networks and Communications, 2014, 1-16.

[25] Kaur, N., & Singh, T. (2015). Improving Performance of MANETs using Multi-Criteria Multipath Routing Protocol . International Journal of Computer Applications, 112(8), 36-41.

[26] Agrawal, H., Johri, P., & Kumar, A. (2015). Emerging trends in energy efficient routing protocols. International Conference on Computing, Communication & Automation.

[27] Mohapatra, S. K., Mahapatra, S. K., Kanoje, L., & Behera, S. (2015). A Low Energy consumed routing multipath protocol in MANETS. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).

[28] Peng, S., Chen, Y., Chang, R., & Chang, J. (2015). An Energy-Aware Random Multi-path Routing Protocol for MANETs. 2015 IEEE International Conference on Smart City/SocialCom/Sustain Com (Smart City)

[29] Tong, M., Chen, Y., Chen, F., Wu, X., & Shou, G. (2015). An Energy-Efficient Multipath Routing Algorithm Based on Ant Colony Optimization for Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 11(6), 642189.

[30] Tiwari, S. (2016). An Energy Saving Multipath AODV Routing Protocol In MANET. International Journal Of Engineering And Computer Science.

[31] Lutimath, N. M., L, S., & Naikodi, C. (2016). Energy Aware Multipath AODV Routing Protocol for Mobile Ad hoc Network. International Journal of Engineering Research , 5(4), 790 -991.

[32] Periyasamy, P., & Karthikeyan, E. (2016). End-to-End Link Reliable Energy Efficient Multipath Routing for Mobile Ad Hoc Networks. Wireless Personal Communications, 92(3), 825-841.

[33] Iqbal, Z., Khan, S., Mehmood, A., Lloret, J., & Alrajeh, N. A. (2016). Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks. Journal of Sensors, 2016, 1-18.

[34] Jayavenkatesan, & Mariappan, A. (2017). ENERGY EFFICIENT MULTIPATH ROUTING FOR MANET BASED ON HYBRID ACO-FDRPSO . International Journal of Pure and Applied Mathematic, 115(6), 185 -191.

[35] Tareq, M., Alsaqour, R., Abdelhaq, M., & Uddin, M. (2017). Mobile Ad Hoc Network Energy Cost Algorithm Based on Artificial Bee Colony. Wireless Communications and Mobile Computing, 2017, 1-14

[36] M.Selladevi1, S. Duraisamy, Survey Paper on Various Security Attacks In Mobile Ad Hoc Network International Journal of Computer Sciences and Engineering, Volume-6, Issue-1 E-ISSN: 2347-2693, 2018.

Authors Profile

Dr Sanjay Sharma presently working in dept. of mathematics and computer application, MANIT, Bhopal as a Professor and Head. His experiences is more then 24 years in teaching and Research field. He has published 31 Paper in International Journals. 10 Paper National Journal, 09 Paper in the National Level Conference. 10 Paper in International Level Conference. He is a member of Computer Society of India (CSI),IEEE, and IDES. His specialization in Computer Networks, Big Data Analytics, Wireless Communication & Mobile Ad-hoc Networks, Next Generation Networks & IPv6.

DR. Pushpendra singh Patheja is currently working in Vellore Institute of Technology, Bhopal As a n Associate Professor dept. of CSE. His experience is more then 22yrs. In the field of teaching and Research. He has published more then 70 National and International papers . He is a member of various research organisation, his specialization is computer network, Big Data, Adhoc Network.

Mrs. Nikhat Raza Khan is completed of Masters in technology dept. of computer science and Engineering in year 2009from MANIT, Bhopal. He is currently pursuing Ph.D. and currently working as Research Scholar in Department of Computer Sciences, She is a member of EEE & IEEE computer society since 2017, She has published more than 30 research papers in reputed internatisnal journals. Her main research work focuses on Mobile adhoc network, Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics, IoT and Computational Intelligence based education. she has 13 years of teaching experience and 3 years of Research Experience.