Topology Adjustment of Effective Communication Model using Fuzzy Controller for MANET

V. Rajesh Kannan[*] & Dr. A. Charles[1]

[*]Research Scholar & AP, Department of ECE, Annamalai University, India. kannan.813@gmail.com

[1]Assistant Professor, Department of ECE, Annamalai University, India. maryarputhamcharles@gmail.com

*corresponding [*]Author

Abstract

Treads of today research uncertainty environment and natural situation if focussed in Mobile Ad hoc Networks, a Big challenges to develop routing protocol that can meet different application needs and optimize routing paths according to the topology change in mobile ad hoc networks. The continuous transmission of small packet is called beacon packet, that advertises the presence of a base station and the mobile units sense the beacons and attempt to establish a wireless connections. Basing their forwarding decisions only on the local topology, geographic routing protocols have drawn a lot of attentions in recent years. MANET nodes square measure distinguished by their restricted resources like multipath communication, end-to-end delay, routing conjunction, remaining energy, bandwidth and storage. MANET routing is serious issue as a result of topology. In this emerging research article developed with my pervious published paper and proposed multipath work with three different topology size, three different set of nodes, three different set of malicious nodes with various parameters such as packet delivery ratio, throughput, routing overhead, packet loss, delay and remaining energy via Network Simulator 2 (NS2).

Keywords: Multi-path, Attack, Energy, Routing Protocols, NS2.

I. INTRODUCTION

Ad hoc self organization, self configuration and self healing because no network will operates they will occur any problem in network simple self reconfigured this is multi-hop wireless network. In MANET each node act as both host and route in autonomous behavior, any time a node can join or leave from the network due to making the network topology dynamic in nature. All nodes have identical (same) features with similar responsibility and capabilities and hence it forms a completely symmetric environment due to mobile nodes are characterized with less memory, power and light weight features. Basically mobile ad hoc router model designed three different types (per established connection for proactive, on-demand connection established for reactive and both concept available in hybrid routing protocols) for sharing information between devices in non fixed network Multipath importance techniques using alternative multiple path in network which can elide provide such as tolerance increase bandwidth and improving security, the multiple path computing joint and disjoined between nodes in the network, extension of research is going recent years in multipath fading communication based on some criteria like minimum cost, minimum weight, maximum forwarding capability, maximum receiving capability, minimum link breakage path etc.

II. PROBLEM IDENTIFICATION

This research work we discussed our previous work called ad hoc on demand distance vector with fuzzy controller, the above design focused on increased delivery ratio with help of fuzzy logic (fuzzy logic reduced number of retransmission and reduced used energy). The dynamic nature of MANETs requires the routing protocols to refresh the routing tables frequently while they suffer from transmission congestion which are the results of the broadcasting nature of radio transmission. Since a node in a MANET cannot directly communicate with the nodes outside its communication range, a packet may have to be routed through intermediate nodes to reach the destination. It also becomes essential to monitor the constraints in intermediate nodes (multi-hop routing). Consequently, an efficient routing approach may generate route failures. The simplest scheme of routing in MANET is the one to find a route without malicious nodes. In this research aims provide an unbreakable route to improved remaining energy for the way of secured transmission. Hence, a new routing algorithm named, Ad hoc on-demand Distance Vector with help of Fuzzy Controller (FC-AODV) is proposed.

Algorithm:

Procedural Steps of EA3ACK Algorithm

- FC-AODV processing starts with fuzzy controller.
- Hello packet transmission from source to destination through intermediate nodes.
- Destination node sends ACK message to source node in same route through intermediate nodes.
- If source node receives this acknowledgement packet within a predefined time period, then data transmission will be start.
- If node A does not receive this acknowledgement packet within a predefined time period, then the intermediate nodes are marked as malicious nodes, otherwise data transmission is started.
- Transmit the data in the alternate path to the destination, and go to step1.

III. SIMULATION PARAMETER

Part of this work in this section, we simulate using proposed protocol with below mentioned parameter values an open environment is evaluated, the simulations are carried out using network simulator (NS 2.34). Initially nodes are placed at certain specific locations, the simulation parameters are specified below.

Table 1 Simulation parameters

Parameter	Values
Simulation area	600m*600m
Number of nodes	75 & 150
Number of packets sender	25
Constant bit rate	4 (packets/second)

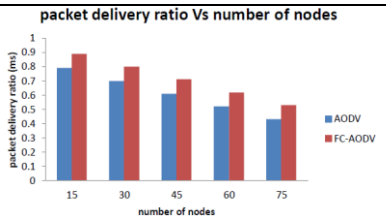
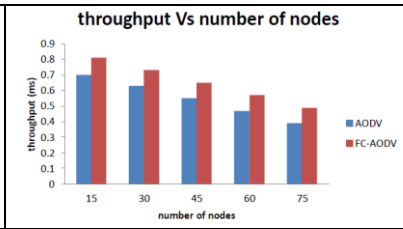
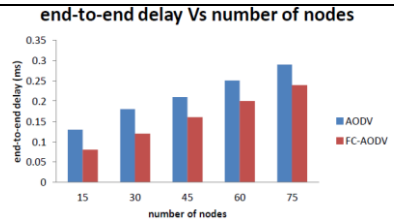
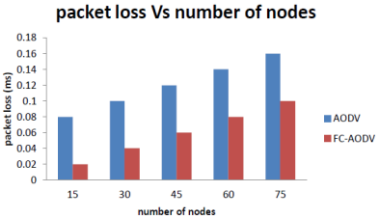
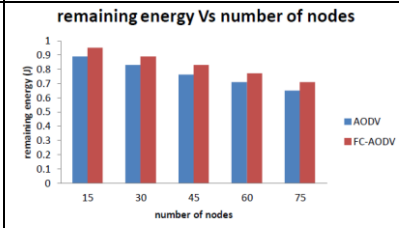
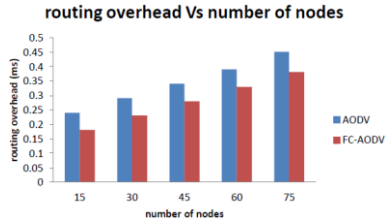
Packet size	512 bytes
Initial energy/node	100 joules
Antenna model	Omni directional
Simulation time	500 sec
Malicious node	8, 12 & 16

IV. RESULT AND DISCUSSION

In this section we discussed results and discussion of existing and proposed methods with five different parameters via NS 2, this manuscript tested with nine different scenarios.

Table 2 Results of Parameter Values (SA=600m, NN=75 & MN=8)

Packet Delivery Ratio					
PDR / NN	15	30	45	60	75
AODV	0.79	0.70	0.61	0.52	0.43
FC-AODV	0.89	0.80	0.71	0.62	0.53
Throughput					
Throughput / NN	15	30	45	60	75
AODV	0.70	0.63	0.55	0.47	0.39
FC-AODV	0.81	0.73	0.65	0.57	0.49
End-to-end Delay					
Delay / NN	15	30	45	60	75
AODV	0.13	0.18	0.21	0.25	0.29
FC-AODV	0.08	0.12	0.16	0.20	0.24
Packet Loss					
Packet loss / NN	15	30	45	60	75
AODV	0.08	0.10	0.12	0.14	0.16
FC-AODV	0.02	0.04	0.06	0.08	0.10
Remaining Energy					
Remaining Energy / NN	15	30	45	60	75
AODV	0.89	0.83	0.76	0.71	0.65
FC-AODV	0.95	0.89	0.83	0.77	0.71
Routing Overhead					
Routing Overhead / NN	15	30	45	60	75
AODV	0.24	0.29	0.34	0.39	0.45
FC-AODV	0.18	0.23	0.28	0.33	0.38

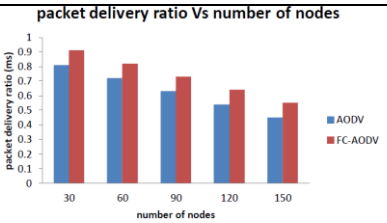
		
1 (a) PDR Vs NN	**1 (b) throughput Vs NN**	**1 (c) end-to end delay Vs NN**
		
1 (d) packet loss Vs NN	**1 (e) end-to end delay Vs NN**	**1 (f) end-to end delay Vs NN**

Simulation results are obtained by varying the number of nodes from 15 to 75. The performances of the proposed FC-AODV and the existing AODV compared. Fig. 1(a) and Table 2 show the proposed model with improved packet delivery ratio, when number of malicious nodes is increased from 1 to 8 when compared to the existing method. It is clear that proposed scheme surpasses AODV performance by 10%, is able to detect malicious in the presence of receiver collision, limited transmission power, and false misbehaviour report and collusion attacks. Fig. 1(b) and Table 2 compare the throughput performance using two algorithms. Result of Fig. 1(b) shows that FC-AODV has increase average throughput by 9.8% compared to the existing method. Proposed algorithm to increases number of active nodes and to identify avoid malicious nodes, it is capable of finding the minimum link failed unbreakable short route between the source to destination and also increase number of successfully deliver packets without malicious node than existing method. Calculate end-to-end delay with varying number of malicious node using FC algorithm, performance comparison of the proposed and the existing methods is shown in Fig. 1(c) and Table 2. It is observed from Fig. 1(c), the proposed model decreases the average delay by 5.2% than AODV protocol with the increase in the number of malicious nodes from 1 to 8 out of 75 nodes. If the malicious node is detected, the FC algorithm finds alternate shortest route between the sender and receiver, because of FC algorithm to allow strongest node transmit without traffic route in the network. The impact of delay on packet loss is analysed using the two algorithms and the simulation results are shown in Fig. 1(d) and Table 2. From the simulation results it is understood that the proposed algorithm reduced an average losses by 6% than existing design. The proposed algorithm is capable of finding unbreakable shortest path to reduce data loss while transmitting and receiving packets. Fig. 1(e) shows that suggested system reduces utilization energy when the number of malicious nodes varied compared to the existing system. It is clear that the proposed design increases the average remaining energy by 6.2% with the increasing nodes 15 to 75 than AODV, due to increases duration of time period of acknowledgments than other acknowledgments it is possible to increases remaining energy. Fig. 1(f) and Table 2 compare the routing overhead performance

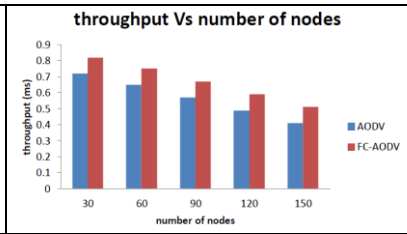
of the proposed FC-AODV and existing acknowledgement based AODV schemes. FC-AODV has reduced routing overhead with the number of malicious nodes from 1 to 8 when compared to the existing method as show in Fig. 1(f). Suggested new method has the reduce average routing overhead by 6.2% than AODV, although FC-AODV requires public and private key at all acknowledgement process.

Table 3 Results of Parameter Values (SA=600m, NN=150 & MN=8)

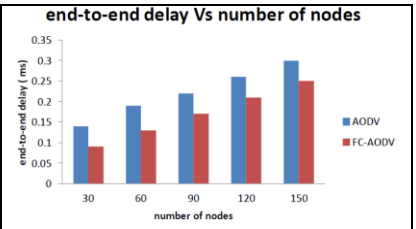
Packet Delivery Ratio					
PDR / NN	30	60	90	120	150
AODV	0.81	0.72	0.63	0.54	0.45
FC-AODV	0.91	0.82	0.73	0.64	0.55
Throughput					
Throughput / NN	30	60	90	120	150
AODV	0.72	0.65	0.57	0.49	0.41
FC-AODV	0.82	0.75	0.67	0.59	0.51
End-to-end Delay					
Delay / NN	30	60	90	120	150
AODV	0.14	0.19	0.22	0.26	0.30
FC-AODV	0.09	0.13	0.17	0.21	0.25
Packet Loss					
Packet loss / NN	30	60	90	120	150
AODV	0.10	0.12	0.14	0.16	0.18
FC-AODV	0.04	0.06	0.08	0.10	0.12
Remaining Energy					
Remaining Energy / NN	30	60	90	120	150
AODV	0.86	0.80	0.73	0.68	0.62
FC-AODV	0.92	0.86	0.80	0.74	0.67
Routing Overhead					
Routing Overhead / NN	30	60	90	120	150
AODV	0.26	0.31	0.36	0.41	0.47
FC-AODV	0.20	0.25	0.30	0.35	0.40



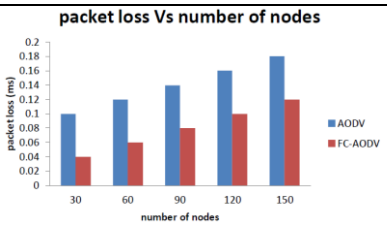
2 (a) PDR Vs NN



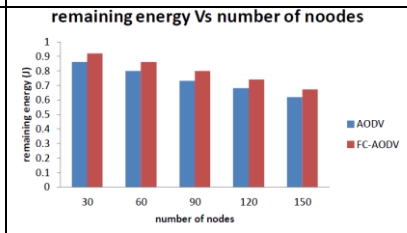
2 (b) throughput Vs NN



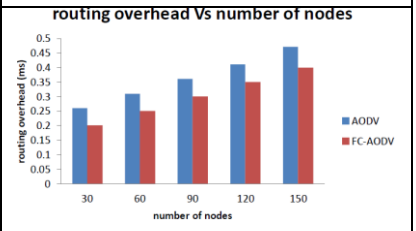
2 (c) end-to end delay Vs NN



2 (d) packet loss Vs NN



2 (e) remaining energy Vs NN



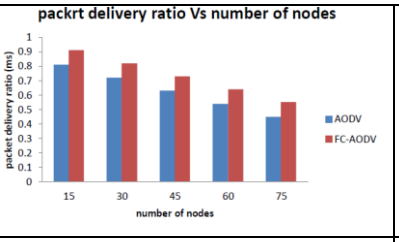
2 (f) routing overhead Vs NN

The result obtained is given in Table 3 and Fig. 2(a), Fig. 2(b), 2(c), 2(d), 2(e) and 2(e) the malicious node is varied from 1 to 8 out of 150 and simulation is carried out to calculate the packet delivery ratio using proposed and existing methods. It is clear from the simulation results of Fig. 2(a) that the FC-AODV has the maximized average packet delivery ratio 10% than AODV with topology size 600m * 600m. Result of Fig. 2(b) shows that FC-AODV has increase average throughput by 10% compared to the existing method. Proposed algorithm to increases number of active nodes and to identify avoid malicious nodes, it is capable of finding the minimum link failed unbreakable short route between the sources to destination. It is observed from Fig. 2(c), the proposed model decreases the average delay by 6.2% than AODV protocol with the increase in the number of malicious nodes from 1 to 8 out of 150 nodes. Simulation results are shown in Fig. 2(d) and Table 3. From the simulation results it is understood that the proposed algorithm reduced an average losses by 6% than existing design. Fig. 2(e) it is clear that the proposed design increases the average remaining energy by 6% with the increasing nodes 30 to 150 than AODV. Fig. 2(f) and Table 3 FC-AODV has reduced routing overhead with the number of malicious nodes from 1 to 8 when compared to the existing method as show in Fig. 2(f). Suggested new method has the reduce average routing overhead by 6.2% than AODV.

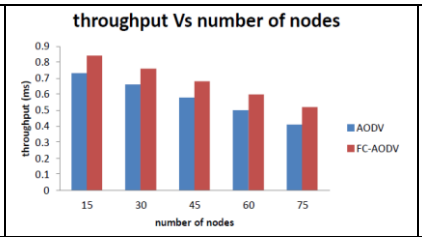
Table 4 Results of Parameter Values (SA=600m, NN=75 & MN=12)

Packet Delivery Ratio					
PDR / NN	15	30	45	60	75
AODV	0.81	0.72	0.63	0.54	0.45
FC-AODV	0.91	0.82	0.73	0.64	0.55
Throughput					
Throughput / NN	15	30	45	60	75
AODV	0.73	0.66	0.58	0.50	0.41
FC-AODV	0.84	0.76	0.68	0.60	0.52

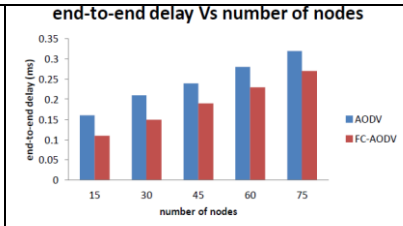
End-to-end Delay					
Delay / NN	15	30	45	60	75
AODV	0.16	0.21	0.24	0.28	0.32
FC-AODV	0.11	0.15	0.19	0.23	0.27
Packet Loss					
Packet loss / NN	15	30	45	60	75
AODV	0.11	0.13	0.15	0.17	0.19
FC-AODV	0.05	0.07	0.09	0.11	0.13
Remaining Energy					
Remaining Energy / NN	15	30	45	60	75
AODV	0.84	0.78	0.71	0.66	0.60
FC-AODV	0.90	0.84	0.78	0.72	0.66
Routing Overhead					
Routing Overhead / NN	15	30	45	60	75
AODV	0.26	0.31	0.36	0.41	0.47
FC-AODV	0.19	0.24	0.29	0.34	0.39



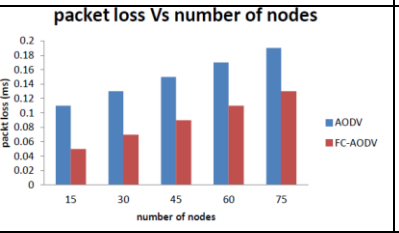
3 (a) PDR Vs NN



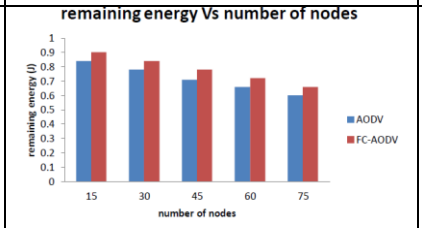
3 (b) throughput Vs NN



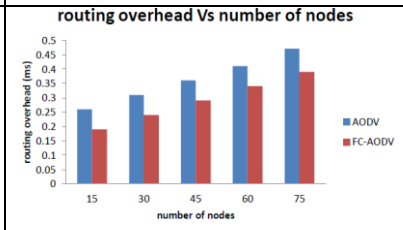
3 (c) end-to-end delay Vs NN



3 (d) packet loss Vs NN



3 (a) remaining energy Vs NN



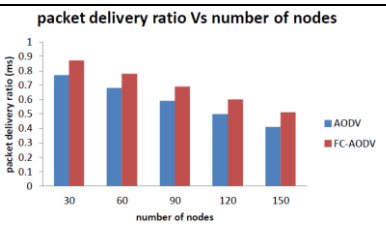
3 (a) routing overhead Vs NN

Above simulation outcomes performances of the proposed FC-AODV and the existing AODV compared with 600m*600m using 12 malicious nodes out of 75 nodes, Fig. 3(a) and Table 3 it is clear that proposed scheme surpasses traditional model performance by 10%, Result of Fig. 3(b) shows that FC-AODV has increase average throughput by 10.4% compared to the existing method. Proposed algorithm to increases number of active nodes and to identify avoid malicious nodes, it is observed from Fig. 3(c) proposed model decreases the average delay by 5% than AODV protocol with the increase in the number of malicious nodes from 1 to 12 out of 75 nodes. FC algorithm finds alternate shortest route between the sender and receiver, because of FC algorithm to allow strongest node transmit without traffic route in the network. Fig. 3(d) and Table 4 from the simulation results it is understood that

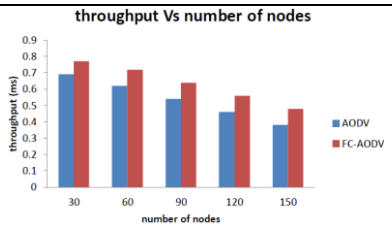
the proposed algorithm reduced an average losses by 6% than existing design. The proposed algorithm is capable of finding unbreakable shortest path to reduce data loss while transmitting and receiving packets. Fig. 3(e) shows that suggested system reduces utilization energy when the number of malicious nodes varied compared to the existing system. It is clear that the proposed design increases the average remaining energy by 6.2% with the increasing nodes 15 to 75 than AODV, due to increases duration of time period of acknowledgments than other acknowledgments it is possible to increases remaining energy. FC-AODV has reduced routing overhead with the number of malicious nodes from 1 to 12 when compared to the existing method as show in Fig. 3(f). Suggested new method has the reduce average routing overhead by 7.2% than AODV.

Table 5 Results of Parameter Values (SA=600m, NN=150 & MN=12)

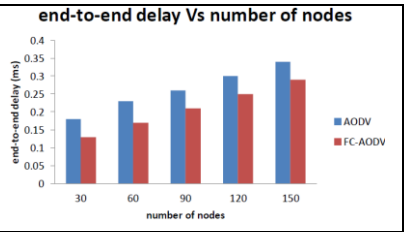
Packet Delivery Ratio					
PDR / NN	30	60	90	120	150
AODV	0.77	0.68	0.59	0.50	0.41
FC-AODV	0.87	0.78	0.69	0.60	0.51
Throughput					
Throughput / NN	30	60	90	120	150
AODV	0.69	0.62	0.54	0.46	0.38
FC-AODV	0.77	0.72	0.64	0.56	0.48
End-to-end Delay					
Delay / NN	30	60	90	120	150
AODV	0.18	0.23	0.26	0.30	0.34
FC-AODV	0.13	0.17	0.21	0.25	0.29
Packet Loss					
Packet loss / NN	30	60	90	120	150
AODV	0.14	0.16	0.18	0.20	0.22
FC-AODV	0.07	0.10	0.12	0.14	0.16
Remaining Energy					
Remaining Energy / NN	30	60	90	120	150
AODV	0.81	0.75	0.68	0.63	0.57
FC-AODV	0.87	0.81	0.75	0.69	0.62
Routing Overhead					
Routing Overhead / NN	30	60	90	120	150
AODV	0.28	0.33	0.38	0.43	0.49
FC-AODV	0.22	0.27	0.32	0.37	0.42



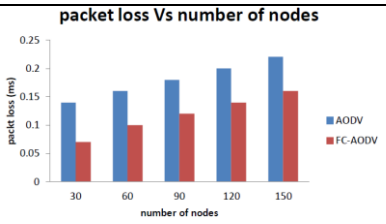
4 (a) PDR Vs NN



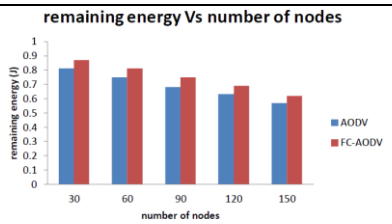
4 (b) throughput Vs NN



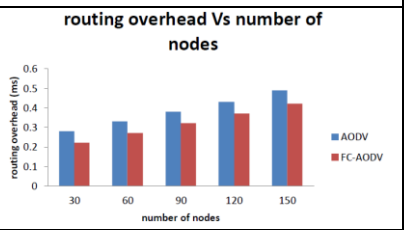
4 (c) end-to-end delay Vs NN



4 (d) packet loss Vs NN



4 (e) remaining energy Vs NN



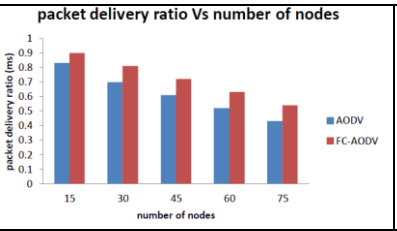
4 (f) PDR Vs NN

Table 5 and Fig. 4(a) packet delivery ratio, Fig. 4(b) throughput, Fig. 4(c) end-to-end delay, Fig. 4(d) packet loss, Fig. 4(e) remaining energy and Fig. 4(f) routing overhead the malicious node is varied from 1 to 12 out of 150 using topology area is 600m*600m and simulation is carried out to calculate the all the parameters using proposed and existing method. Fig. 4(a) that the FC-AODV has the maximized average packet delivery ratio 10% than AODV, result of Fig. 4(b) shows that FC-AODV has increase average throughput by 10.4% compared to the existing method. It is observed from Fig. 4(c), the proposed model decreases the average delay by 5.2% than AODV protocol, simulation results are shown in Fig. 4(d) and Table 5. From the simulation results it is understood that the proposed algorithm reduced an average losses by 5.4% than existing design. Fig. 4(e) it is clear that the proposed design increases the average remaining energy by 6% with the increasing nodes 30 to 150 than AODV. Fig. 4(f) and Table 5 FC-AODV has reduced routing overhead with the number of malicious nodes from 1 to 12 when compared to the existing method as show in Fig. 4(f). Suggested new method has the reduce average routing overhead by 5.2% than AODV.

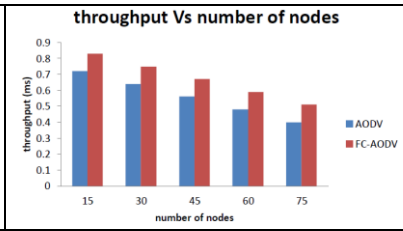
Table 6 Results of Parameter Values (SA=600m, NN=75 & MN=16)

Packet Delivery Ratio					
PDR / NN	15	30	45	60	75
AODV	0.83	0.70	0.61	0.52	0.43
FC-AODV	0.90	0.81	0.72	0.63	0.54
Throughput					
Throughput / NN	15	30	45	60	75
AODV	0.72	0.64	0.56	0.48	0.40
FC-AODV	0.83	0.75	0.67	0.59	0.51
End-to-end Delay					
Delay / NN	15	30	45	60	75
AODV	0.18	0.23	0.26	0.30	0.35

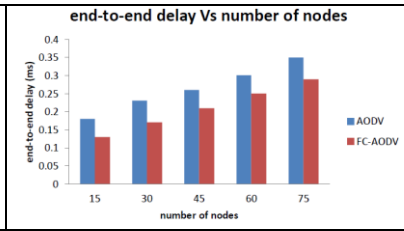
FC-AODV	0.13	0.17	0.21	0.25	0.29
Packet Loss					
Packet loss / NN	15	30	45	60	75
AODV	0.13	0.15	0.17	0.19	0.21
FC-AODV	0.09	0.11	0.13	0.15	0.17
Remaining Energy					
Remaining Energy / NN	15	30	45	60	75
AODV	0.80	0.74	0.67	0.62	0.56
FC-AODV	0.88	0.82	0.76	0.70	0.64
Routing Overhead					
Routing Overhead / NN	15	30	45	60	75
AODV	0.28	0.33	0.38	0.43	0.49
FC-AODV	0.21	0.26	0.31	0.36	0.41



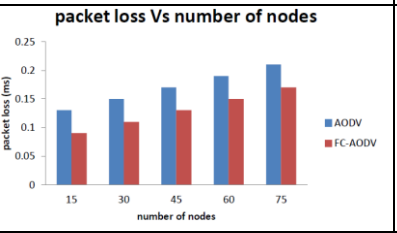
5 (a) PDR Vs NN



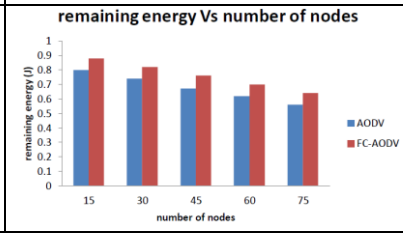
5 (b) throughput Vs NN



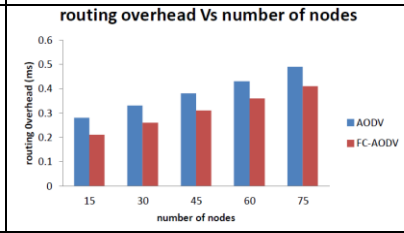
5 (c) end-to-end delay Vs NN



5 (d) packet loss Vs NN



5 (e) remaining energy Vs NN



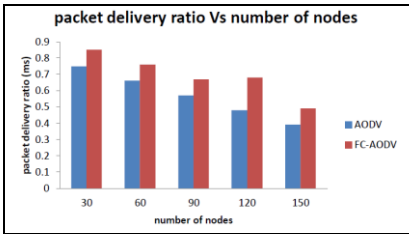
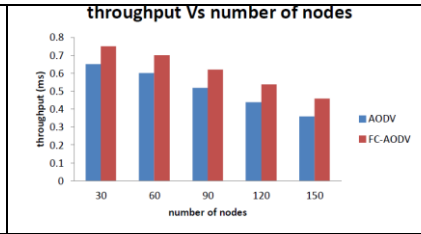
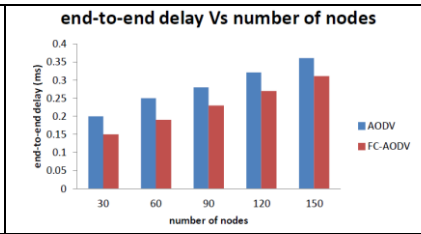
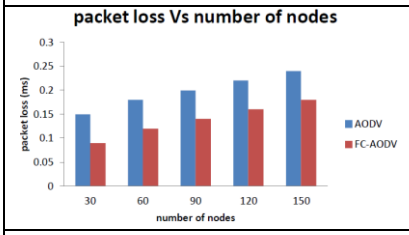
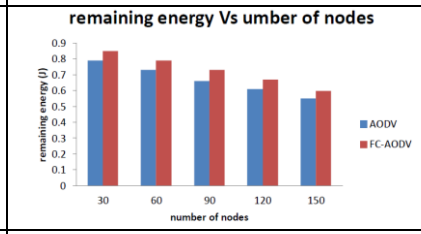
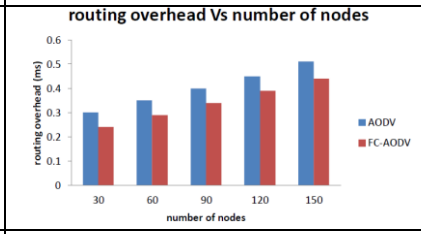
5 (f) routing overhead Vs NN

Performances of the proposed FC-AODV and the existing AODV compared with 600m*600m using 16 malicious nodes out of 75 nodes, Fig. 5(a) and Table 6 it is clear that proposed scheme surpasses traditional model performance by 10.2%, Result of Fig. 5(b) shows that FC-AODV has increase average throughput by 11% compared to the existing method. Proposed algorithm to increases number of active nodes and to identify avoid malicious nodes, it is observed from Fig. 5(c) proposed model decreases the average delay by 5.4% than AODV protocol with the increase in the number of malicious nodes from 1 to 16 out of 75 nodes. FC algorithm finds alternate shortest route between the sender and receiver, because of FC algorithm to allow strongest node transmit without traffic route in the network. Fig. 5(d) and Table 6 from the simulation results it is understood that the proposed algorithm reduced an average losses by 4% than existing design. The proposed algorithm is capable of finding unbreakable shortest path to reduce data loss while transmitting and receiving packets. Fig. 5(e) shows that suggested system reduces utilization energy when the number of

malicious nodes varied compared to the existing system. It is clear that the proposed design increases the average remaining energy by 8.2% with the increasing nodes 15 to 75 than AODV, due to increases duration of time period of acknowledgments than other acknowledgments it is possible to increases remaining energy. FC-AODV has reduced routing overhead with the number of malicious nodes from 1 to 16 when compared to the existing method as show in Fig. 5(f). Suggested new method has the reduce average routing overhead by 7.2% than AODV.

Table 7 Results of Parameter Values (SA=600m, NN=150 & MN=16)

Packet Delivery Ratio					
PDR / NN	30	60	90	120	150
AODV	0.75	0.66	0.57	0.48	0.39
FC-AODV	0.85	0.76	0.67	0.68	0.49
Throughput					
Throughput / NN	30	60	90	120	150
AODV	0.65	0.60	0.52	0.44	0.36
FC-AODV	0.75	0.70	0.62	0.54	0.46
End-to-end Delay					
Delay / NN	30	60	90	120	150
AODV	0.20	0.25	0.28	0.32	0.36
FC-AODV	0.15	0.19	0.23	0.27	0.31
Packet Loss					
Packet loss / NN	30	60	90	120	150
AODV	0.15	0.18	0.20	0.22	0.24
FC-AODV	0.09	0.12	0.14	0.16	0.18
Remaining Energy					
Remaining Energy / NN	30	60	90	120	150
AODV	0.79	0.73	0.66	0.61	0.55
FC-AODV	0.85	0.79	0.73	0.67	0.60
Routing Overhead					
Routing Overhead / NN	30	60	90	120	150
AODV	0.30	0.35	0.40	0.45	0.51
FC-AODV	0.24	0.29	0.34	0.39	0.44

		
6 (a) PDR Vs NN	**6 (b) throughput Vs NN**	**6 (c) end-to-end delay Vs NN**
		
6 (d) packet loss Vs NN	**6 (e) remaining energy Vs NN**	**6 (f) routing overhead Vs NN**

The result obtained is given in Table 7 and Fig. 6(a), Fig. 6(b), 6(c), 6(d), 6(e) and 6(f) the malicious node is varied from 1 to 16 out of 150 and simulation is carried out to calculate the packet delivery ratio using proposed and existing methods. It is clear from the simulation results of Fig. 6(a) that the FC-AODV has the maximized average packet delivery ratio 10% than AODV with topology size 600m * 600m. Result of Fig. 6(b) shows that FC-AODV has increase average throughput by 10% compared to the existing method. Proposed algorithm to increases number of active nodes and to identify avoid malicious nodes, it is capable of finding the minimum link failed unbreakable short route between the sources to destination. It is observed from Fig. 6(c), the proposed model decreases the average delay by 5.2% than AODV protocol with the increase in the number of malicious nodes from 1 to 16 out of 150 nodes. Simulation results are shown in Fig. 6(d) and Table 7. From the simulation results it is understood that the proposed algorithm reduced an average losses by 6% than existing design. Fig. 6(e) it is clear that the proposed design increases the average remaining energy by 5.8% with the increasing nodes 30 to 150 than AODV. Fig. 6(f) and Table 7 FC-AODV has reduced routing overhead with the number of malicious nodes from 1 to 16 when compared to the existing method as show in Fig. 6(f). Suggested new method has the reduce average routing overhead by 6.2% than AODV.

From all the above figures and tables it is clear that the comparison of the proposed FC-AODV with the conventional routing protocol and other existing acknowledgement based IDS schemes, shows the packet deliver ratio, throughput and remaining energy increased, end-to-end delay, packet loss and routing overhead decrease with the increase in the number of malicious nodes.

V. SUMMARY

In this manuscript, it is clear that misbehaver attacking for multi-path routing has always been a major threat to the security in MANETs during the transmission drop (or) attack the packet, if wireless communication is done without acknowledgement. In this research, a proposed routing protocol named FC-AODV is proposed with fuzzy controller. The simulation results propose FC-AODV algorithm as compared with the existing AODV

algorithm in different scenarios through the network simulation 2. This developed model ability to detect misbehaviour nodes with improves average packet delivery ratio for all the three scenarios by 12.4%, improved average throughput for three scenarios by 10.27% than the existing routing protocol and reduced average end-to-end delay for all the three scenarios by 5.37%, reduced packet loss average packet loss for all the three scenarios by 5.57% also solve weakness of existing method, result of all the scenarios clearly shows propose system still increased average remaining energy by 6.4% than existing method and reduce average routing overhead by 6.37 compared to the existing routing protocol. We plan to investigate the following issues in our future research. 1) The same concept can be applied in satellite to reduce more congestion in the route and also to save more energy. 2) The possibilities of adopting the shortest path algorithm to eliminate the requirement of redistributed; can be examined. 3) The performance of FC-AODV can be tested in real time network environment Instead of software simulation.

References

1. G.Forman and J.Zahorjan, (1994) "Mobile Wireless Computing", IEEE Spectrum, Vol. 27, No. 4, pp. 38-47.
2. Basagni.S, et al, (2003) "Ad Hoc Networking", IEEE Press Wiley, Vol. 6, No. 2, pp. 46-55.
3. Douglas S.J.DE Couto, Daniel Aguayo, John Bicket and Robert Morris (2005) "A High-Throughput Path Metric for Multi-Hop Wireless Routing, Wireless Networks, Vol. 11, pp. 419–434.
4. Burmester, M. and de Medeiros, B. (2009), On the Security of Route Discovery in MANETs, IEEE Transactions on Mobile Computing, Vol. 8, No. 9, 1180-1188.
5. Zafar, H., Harle, D., Andonovic, I., and Khawaja, Y., (2009), Performance Evaluation of Shortest Multipath Source Routing Scheme, IET Communications, Vol. 3, No. 5, pp. 700-713.
6. Mohammed, Tarique., Kemal, E.T., Sasan, Adibi., and Shervin, Erfani., (2009), Survey of multipath routing protocols for mobile ad hoc networks, Journal of Network and Computer Applications, Vol. 32, No. 6, pp. 1125-1143.
7. A. Jameli, et al (2009) "Comparative Analysis of Ad Hoc Networks Routing Protocols for Multimedia Streaming", IEEE, Vol. 3, No. 1, pp. 22-45.
8. R Ahlswede, et al (2010) "Network information flow", IEEE transactions on information theory, Vol. 56, No. 12, pp. 5893-5905.
9. Jiazi Yi., Asmaa Adnane., Sylvain David., and Benoît Parrein., (2011), Multipath optimized link state routing for mobile ad hoc networks, Ad hoc Networks, Vol. 9, No. 1, pp. 28-47.
10. K. Prabu, et al (2012) "A Survey of Wireless Ad hoc Network for MANET", IJARCS, Vol. 3, No. 7, pp. 279-283.
11. K. Thamizhmaran, R. Santosh Kumar Mahto, and V. Sanjesh Kumar Tripathi, (2012) "Performance Analysis of Secure Routing Protocols in MANET", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, No. 9, pp. 651-654.
12. May Zin Oo, and Mazliza Othman, (2012), Analytical Studies of Interaction between Mobility Models and Single-Multi Paths Routing Protocols in Mobile Ad hoc Networks, Wireless Personal Communication, Vol. 64, No. 2, pp. 379–402.

13. K. Thamizhmaran, A. D. Arivazhagan and M. Anitha, "Co-operative analysis of proactive and reactive protocols using dijkstra's algorithm", 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO), pp. 1-6, Jan. 2015
14. K. Thamizhmaran and M. Anitha (2015) "A Survey of Routing Protocols in Mobile Ad hoc Network, International Journal of Applied Engineering Research, Vol. 10, No. 1, pp. 490-496.
15. K. Prabu and K. Thamizhmaran (2016) "Detecting misbehaving nodes in MANET using EA3ACK algorithm, Global Journal of Pure and Applied Mathematics, Vol. 12, No. 4, pp.1-6.
16. Farooq Aftab, Zhongshan Zhang and Adeel Ahmad (2017) "Self-Organization Based Clustering in MANETs Using Zone Based Group Mobility", IEEE Translations and content mining, Vol. 5.
17. K.Thamizhmaran., M. Anitha and Alamelunachippan (2017) "Performance Analysis of On-demand Routing Protocol for MANET Using EA3ACK Algorithm", International Journal of Mobile Network Design and Innovation, Vol. 7, No. 2, pp. 88-100.
18. Gautam, M. and Mahajan, A.R. (2017), A secure and trust based on-demand multipath routing scheme for self-organized mobile ad hoc networks, Wireless Networks, Vol. 23, No. 8, pp. 2455-2472.
19. K.Thamizhmaran., M. Anitha and Alamelunachippan (2017) "Performance Analysis of Energy-Efficient Enhanced Adaptive 3-Acknowledgement (EE-EA3ACK) Using ECC in MANET" ARPN Journal of Engineering and Applied Sciences, Vol. 12, No. 9, pp. 2901-2912.
20. K.Thamizhmaran, M. Anitha and Alamelunachippan (2017) "Comparison and Parameter Adjustment of Topology Based (S-EA3ACK) for MANETs", International Journal of Control Theory and Application, Vol. 10, No. 30, pp. 423-436.
21. Gautam, M. and Mahajan, A.R. (2017), A secure and trust based on-demand multipath routing scheme for self-organized mobile ad hoc networks, Wireless Networks, Vol. 23, No. 8, pp. 2455-2472.
22. Thamizhmaran K (2017) Modified ABR (M-ABR) routing protocol with multi-cost parameters for effective communication in MANETs. IJARCS, Vol. 8, No. 1, pp. 288-291.
23. Akram Kout., Said Labed., Salim Chikhi., and El Bay Bourennane., (2018), AODVCS, a new bio-inspired routing protocol based on cuckoo search algorithm for mobile ad hoc networks, Wireless Network, Vol. 24, No. 9, pp. 2509-2519.
24. K. Thamizhmaran, M. Anitha and Alamelunachippan (2018) "Reduced End-To-End Delay for Manets using SHSP-EA3ACK Algorithm", I-Manager Journal on Communication Engineering and Systems, Vol. 7, No. 3, pp. 9-15.
25. L. Femila and M. Marsaline Beno (2019) "Optimizing Transmission Power and Energy Efficient Routing Protocol in MANETs, Wireless Personal Communication, Vol. 106, pp. 1041-1056.
26. K. Anish Pon Yamini, K. Suthendran and T. Arivoli (2019) "Enhancement of Energy Efficiency using a Transition State MAC Protocol for MANET", Computer Networks, Vol. 155, No. 1, pp. 110-118.
27. Y. Harold Robinson, E. Golden Julie, Krishnan Saravanan, Raghvendra Kumar and Le Hoang So (2019) "FD-AOMDV: fault-tolerant disjoint ad-hoc on-demand multipath distance

vector routing algorithm in mobile ad-hoc networks", Journal of Ambient Intelligence and Humanized Computing, Vol. 10, pp. 4455–4472.

28. J. Deepa and J. Sutha (2019) "A new energy based power aware routing method for MANETs", Cluster Computing, Vol. 22, pp. 13317–13324.
29. N.S. Saba Farheen and Anuj Jain (2020) "Improved routing in MANET with optimized multi path routing fine tuned with hybrid modeling", Journal of King Saud University Computer and Information Sciences, Vol. 32, No. 6, pp. 700-708.
30. K.Thamizhmaran (2020) "IOT supported security considerations for network" WSEAS Transactions on Communications, Vol.19, pp. 113-123.
31. K.Thamizhmaran (2020) "Secure Three Acknowledgements Based Quality Routing Protocol for WSN", Journal of Optoelectronics and Communication, Vol. 2, No. 3, pp. 1-5.
32. R. Thiagarajan, M. Rajesh Babu & M. Moorthi (2021) "Quality of Service based Ad hoc On-demand Multipath Distance Vector Routing protocol in mobile ad hoc network", Journal of Ambient Intelligence and Humanized Computing, Vol. 12, pp. 4957–4965.
33. Yutao Liu, Yue Li, Yimeng Zhao and Chunhui Zhang (2021) "Research on MAC Protocols in Cluster-Based Ad Hoc Networks" Wireless Communications and Mobile Computing, 23, 1-12.
34. Saleh A. Alghamdi (2022) "Cuckoo Energy Efficient Load Balancing On-Demand Multipath Routing Protocol", Arabian Journal for Science and Engineering, Vol. 47, pp. 1321-1335.
35. K.Thamizhmaran, "Comparative Study of Energy Efficient Routing Protocols in MANET", WSEAS Transaction, Vol. 21, 2022.