CLUSTER NODE SELECTION IN MANET USING FC BASED ON-DEMAND ROUTING PROTOCOL (FCH-AODV)

[1]V. Rajesh Kannan* and [2]Dr. A. Charles
[1]Research Scholar, Dept. of ECE, Annamalai University, India.
[2]Assistant Professor, Dept of ECE, Annamalai University, India.

Email ID: *kannan.813@gmail.com, charlesgceb@gmail.com

***Corresponding Author**

Abstract – Many of developed researchers focused in the field of ad hoc temporary network because of this only network is effectively communication from source to destination in the time of un-avoidance or natural issues. Mobile Ad hoc Networks (MANET) affects for many challenging issue such as multipath routing, wasted energy, wasted bandwidth, attacks, drop, loss etc. Multipath is one of un-avoided concept of MANET they lead to easy communication between two nodes using intermediate hops due to problem of obstacle in active path or network this types of topology is very flexible share information through different paths. Part of in this work implemented Cluster Head based On-Demand Routing Protocol called Cluster Head based Ad hoc On-Demand Distance Routing Protocol using Fuzzy Controller (FCH-AODV) they work path selection routing between source and destination via active intermediate nodes for mobile network specially developed to aware head node compare to existing Ad hoc On-Demand Distance Routing Protocol (AODV), and tested using NS2.

Keywords: MANET, Multipath Routing, Cluster Head, Security, Fuzzy Controller, NS2.

Doi: 10.31838/ecb/2023.12.6.259

Introduction

In no other field these developments have been more evident than in field of wireless technology. Though wireless systems have existed since the 1980's, it is only in recent times that wireless systems have started to make in-roads into all aspects of human life. Mobile Ad hoc Network (MANET) is advanced wireless communication networks. MANET appeared in the 1970s with the Packet Radio Network (PRNET) program of the Defense Advanced Research Projects Agency (DARPA). Initially designed for tactical networks, MANET has benefited from a growing interest in the research community since the 1980s. Indeed, since no fixed infrastructure manages the network, the MANET experiences several problems, such as frequent disconnections of links, hidden nodes, varying topology due to mobility, more interference and limited bandwidth due to the shared medium, and quick power consumption on the mobile nodes. Every networking functions, such as formative the network topology, multiple accesses, and routing of data over the most suitable paths are to be performed in a spread way. These tasks are particularly difficult due to the restricted communication bandwidth offered in the wireless channel. These networks operate without the support of any fixed infrastructure or centralized administration (i.e. Infrastructure less Networks) and are completely self-organizing and self-configuring as in figure 1 Nodes are connected dynamically and in an arbitrary manner to form a network, depending on their transmission ranges and positions. Nodes can communicate directly with all nodes within transmission range. As transmission ranges are limited, two nodes may not be able to communicate directly and they must rely on other nodes to forward their packets. Different types of ad hoc networks like Mobile Ad hoc Network (MANET), Wireless Mesh Network (WMN), Wireless Sensor Networks (WSN) and Vehicular Ad hoc Networks (VANET) etc. In recent years, the interest in ad hoc networks has grown due to the availability of wireless communication devices that its capability to work in the ISM bands. While designing an ad hoc network in particular we are concerned with the capabilities and limitations that the physical layer imposes on the network performance. Each of the nodes has a wireless interface and communicates with each other over either radio or infrared. Laptop computers and Personal Digital Assistants (PDA) that communicate directly with each other are some of the examples of nodes in an ad hoc network. Nodes in the ad hoc network are often mobile, but can also consist of stationary nodes, such as access points to the internet. Figure 1 shows a simple MANET with three nodes. The outermost nodes are not within transmitter range of each other. However the middle node can be used to forward packets between the outermost nodes. The middle node is acting as a router and these three nodes have formed an ad hoc network.

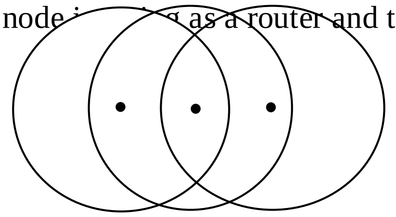

Figure 1 A Simple MANET

MANET does not use any centralized administration. This is to ensure that the network won't collapse just because one of the mobile nodes moves out of transmitter range of the others. Nodes should be able to enter/leave the network as they wish. Because of the transmission range limit of the nodes, multiple hops may be needed to reach other nodes. Every node wishing to participate in an ad hoc network must be willing to forward packets to other nodes. Thus each node in a MANET can act as both a host and a router to receive and forward packets, and it can randomly move around, leave the network or switch off. Moreover, new nodes may join the network unexpectedly. MANET takes advantages of the nature of the wireless communication medium. In other words, in a wired network the physical cabling is done a priori restricting the connection topology of the nodes, this restriction is not present in the wireless domain and, provided that two nodes are within transmitter range of each other, an instantaneous link between them may form. These characteristics make a MANET an unstable network where links between nodes frequently break. In such dynamic topologies, each node is responsible for establishing connections with neighbour nodes and for relaying packets on behalf of other nodes, and therefore, temporary networks can be set up with no or limited infrastructure support. Due to these properties, MANET has great application potential in various scenarios, such as battle field communication and disaster recovery. Application scenarios of MANET include disaster relief, personal communication in battlefields, vehicle-to-vehicle communication in automated highway systems, emergency services, personal entertainment and mobile conferencing.

Characteristics of MANET: MANET has several distinct characteristics that make them quite different from conventional cellular networks.

✓ ***Dynamic topologies:*** Nodes are free to move arbitrarily at different speeds. It is difficult to predict a node's movement and its trajectory. Therefore, the network topology may change randomly and unpredictably

✓ ***Limited bandwidth:*** Wireless links have lower capacity than wired networks. Nowadays however, some standards offer better data rates comparable to those of Ethernet (e.g., WiMAX). Additionally, the throughput in wireless communication is affected by the conditions of the environment, fading, noise or interference.

✓ ***Energy-constrained:*** In a MANET, nodes may rely on limited batteries as source of energy. Nodes do not have enough transmitting power to reach all nodes in the network. This restricts the nodes communication to only the neighbouring nodes.

✓ ***Limitations of the medium:*** In a wireless network, it is not possible to transmit and to listen at the same time. Message loss is mainly due to collisions and interference.

✓ ***Limited physical security:*** In MANETs, data packets travel across the air. Hence, it is relatively easy for an intruder to every data packets by operating in promiscuous mode and by using a packet sniffer. Nodes may also be affected by intentional jamming or denial of service (DoS) attacks.

Challenges of MANET Network: A number of challenges are given below which affect the MANET. Figure 2 depicts assorted MANET challenge where security related challenge is at application layer, quality of service at transport layer, routing at network layer, power control at link/application layer.

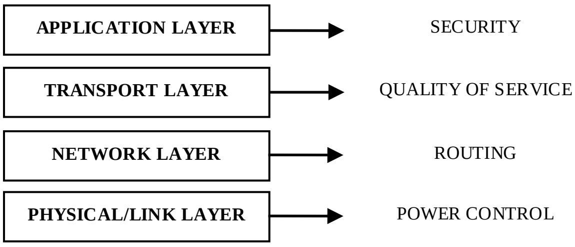

Figure 2 MANET Challenges at different layer

✓ ***Application Layer:*** The application layer with which a user interacts is application-specific. All the other layers are used to create a seamless interface for the networking needs of the application layer. The functionalities of the other layers change on the basis of requirement of application. There are Numbers of identifications like communication partners, privacy quality of service, user authentication, and a number of constraints on data syntax are identified. The application services provided by application layer are file transfers, e-mail and network software services.

✓ ***Transport Layer:*** The transport layer is accountable for end-to-end connection establishment, end-to-end data packet delivery, congestion control, and flow control. Transport protocols help to create communication sessions between computers and that reliable data movement between computers is guaranteed.

- ✓ ***Network Layer:*** In MANET the source and the destination are not in the direct transmission/reception range of each other. Multi-hop forwarding is used for the nodes that are not in direct communication range. Such indirect communication through multi-hop forwarding is called routing. Set up and maintain of routes from a source to any desired destination is the responsibility of the network layer. The network layer needs sufficient information about the topology of the communication network to provide efficient routes. There are two main function of the network layer: route discovery and route maintenance. Route discovery is used to find a route from a source to a destination, although route maintenance is used to maintain an existing route as the topology changes suitable to node mobility.
- ✓ ***Physical Layer:*** The physical layer is the modem hardware in simple terms. Electronics parts of the physical layer are the antenna and the transmitter/receiver as an e.g. in a wireless node. Main functions are Modulation and coding of the physical layer. IEEE protocols at physical layer are:
  - o To transmit data at 10 Mbps 802.3 (Ethernet) is used which is a logical bus network. To every computer on the network, data is transmitted.
  - o To transmit data at 4Mbps or 16bps 802.5 (Token Ring) is used which is a logical ring network. Each computer is branching of hub so it resembles more like star.
  - o 802.4 (Token Passing) uses a token-passing scheme which is a bus layout. Computers that are addressed respond all the received data. A token that travels the network determine which computer is capable to broadcast.
- ✓ ***Link Layer:*** The limited bandwidth of the wireless channel combined with radio propagation loss and the broadcast nature of radio transmission make communication over a wireless channel inherently unreliable. Link-layer protocols are used to add information bits to the data bits to protect them against channel errors. Forward error correction protocols add controlled redundancy to the data, in order to enable reliable transmission of data over unreliable channels. Typical channel coding systems contain a source code, to reduce redundancy from the data, followed by a channel coder that adds controlled redundancy to the compressed data.

Basically, routing protocols are often generally classified into three varieties as Table–Driven routing protocol, On-Demand routing protocol and Hybrid routing protocol.

- ✓ ***Table Driven / Proactive:*** Proactive routing protocols acquire routing information periodically and store them in one or more routing tables. The differences among the protocols in this class are routing structure, number of tables, frequency of updates, use of hello messages and the existence of a central node.

- ✓ ***On-Demand / Reactive:*** Reactive routing protocols discover or maintain a route as needed. This reduces overhead that is created by proactive protocols. Flooding strategy is used to discover a route. Reactive routing protocols can be classified into two groups: source routing and hop by hop routing.

- ✓ ***Hybrid***: This protocols exhibit both reactive and proactive features. Proactive strategy is used to discover and maintain routes to nearby nodes, while routes to far away nodes are discovered reactively. Consequently, overheads and delay that are introduced by proactive protocols and reactive protocols, respectively, are minimized.

Problem with Routing in MANET: Routing is the most fundamental research issue in MANET and must deal with limitations of power, bandwidth, and mobility of nodes. Some of the problems with routing in MANET are as follows: Asymmetric links, Routing Overhead, Interference and Dynamic Topology.

Experimental

Network wide routing in MANETs is a vital task of transferring data from a source to the destination. The dynamic nature of MANETs requires the routing protocols to refresh the routing tables frequently while they suffer from transmission congestion during multipath 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. 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. This research article aims to provide an unbreakable multipath route in cluster Head for MANET using fuzzy controller in secured transmission. Hence, a new multipath routing algorithm named, hybrid FCH-AODV which is a combination of cluster head node & fuzzy controller is proposed. Part of in this manuscript, we discussed our proposed reactive routing protocol called cluster head node based ad hoc on-demand distance vector with fuzzy controller, the below design focused on increased delivery ratio with help of fuzzy logic (fuzzy logic reduced number of retransmission and reduced used energy). As show in fig 3 is FCH-AODV developed reactive routing protocol specially designed for mobile ad hoc networks. According to above figure 3 is cluster head based on-demand routing protocol with fuzzy controller clearly show very first from the source node simply broadcast the route request packet (RREQ) to destination through intermediate node, every intermediate node also done same work to other node till they reach destination node. If destination node once receive route request packet from source node, immediately they send route replay packet (RREP) through same intermediate node from destination node to source node this work done every reactive nodes but ADOV having some unique characteristics when start RREQ and RREP at a same time route discovery and route maintenance work simultaneously, the above set of rules designed traditional AODV routing protocol. After RREQ and RREP find cluster head node using maximum forwarding capacity, maximum receiving capacity with minimum link breakage. In this developed work is enhance on-demand routing protocol with help of fuzzy controller, set of rules slightly change also improved network performance due to fixed time period cannot able to receive RREP packet simply marked as malicious node because to detect and resolve the misbehaviours node and increased remaining energy due to reduces retransmitting rout request and route replay with help of fuzzy controller table 1 assumed packet type indicators.

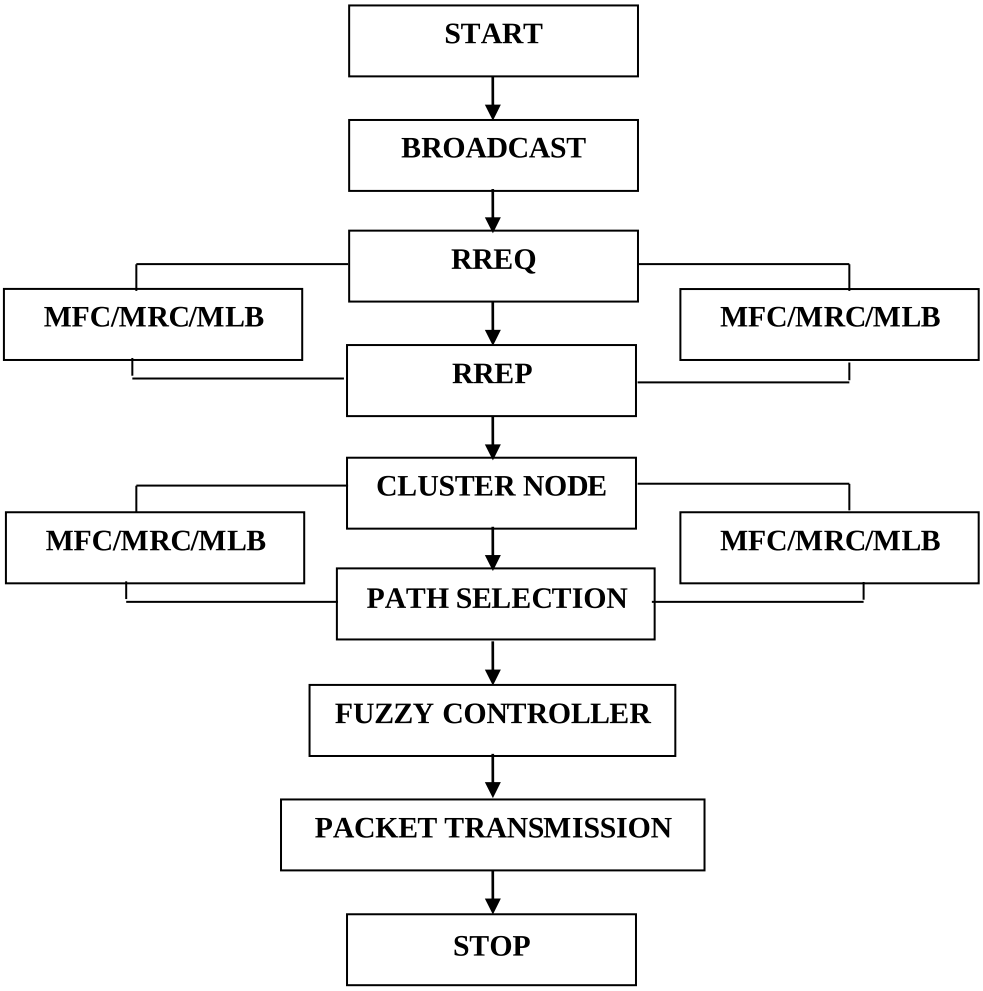

Figure 3 FCH-AODV

MFC=maximum forwarding capacity, MRC=maximum receiving capacity, MLB=minimum link brakeage

Table 1 Packet Type Indicators

Packet type	**General packet**	**RREQ**	**RREP**	**FC packet**
Packet flag	00	01	10	11

The proposed cluster head based on-demand fuzzy controller routing method is evaluated and compared with conventional AODV routing in terms of packet delivery ratio, throughput, routing overhead, packet loss and remaining energy consumption per node using network simulator 2, proposes a fuzzy path selection based on number of hops and remaining battery power along the path. In our previous papers, the routing decision is shared among the nodes along the path from the source to the destination during the route discovery process using fuzzy controllers which consider number of hops and delay factor. In this paper, we extended the FCH-AODV routing protocol to take the remaining battery power and packet queue occupancy in addition to number of intermediate hops as inputs to the fuzzy controller to produce the routes costs to be used in the route selection process.

Algorithm:

Procedural Steps of FCH-AODV Algorithm

- ✓ FCH-AODV processing starts with cluster head based 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.
- ✓ Find cluster head node using maximum forwarding capacity, maximum receiving capacity with minimum link breakage.
- ✓ Transmit the data in the alternate path to the destination, and go to step1.
- ✓ Transmit message packet through primary cluster head node, if fails primary cluster head node switch on secondary cluster head node.

We simulate using proposed protocol with below mentioned parameter values an open environment is evaluated, the simulations are carried out using network simulator 2. Initially nodes are placed at certain specific locations, the simulation parameters are specified below.

Table 2 Simulation parameters

Parameter	Values
Simulation area	600m*600m
Number of nodes	50
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

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 3 Results of packet delivery ratio

packet delivery ratio					
PDR / NN	10	20	30	40	50
AODV	0.40	0.49	0.58	0.67	0.76
FCH-AODV	0.55	0.64	0.73	0.82	0.91

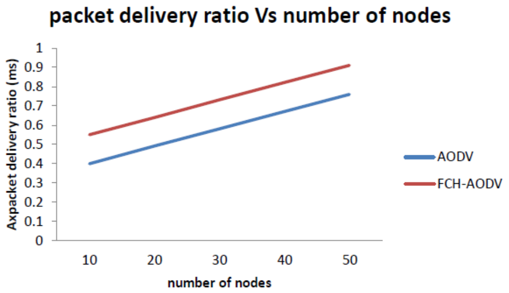

Figure 4 Packet Delivery Ratio Vs Number of Nodes

The performances of the proposed FCH-AODV and the existing AODV compared. Fig 3 and Table 4 show the proposed model with improved packet delivery ratio, when number of malicious nodes is 8 when compared to the existing method. It is clear that response of proposed scheme surpasses AODV performance by 15%, is able to detect malicious in the presence of receiver collision, limited transmission power, and false misbehaviour report and collusion attacks.

Table 4 Results of Throughput

Throughput					
Throughput / NN	10	20	30	40	50
AODV	0.36	0.44	0.52	0.60	0.67
FCH-AODV	0.51	0.59	0.67	0.75	0.83

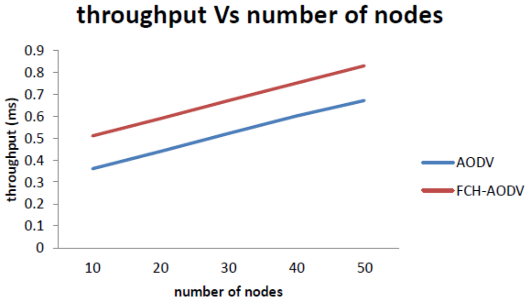

Figure 5 Throughput Vs Number of Nodes

Fig 5 and Table 4 compare the throughput performance using two algorithms. Simulation result of Fig 5 shows that FCH-AODV has increase average throughput by 15.2% compared to the existing method. Our suggested new design 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.

Table 5 Results of Remaining Energy

remaining energy					
Remaining Energy / NN	10	20	30	40	50
AODV	0.83	0.77	0.71	0.65	0.59
FCH-AODV	0.93	0.87	0.81	0.75	0.69

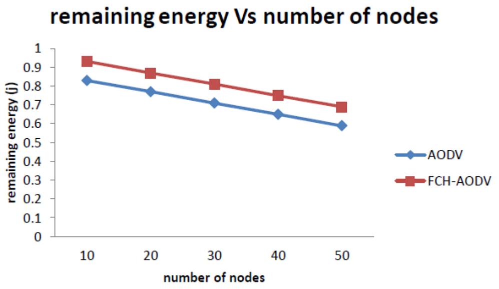

Figure 6 Remaining Energy Vs Number of Nodes

Fig 6 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 10% with the increasing nodes 10 to 50 than old routing protocol, due to increases duration of time period of acknowledgments than other acknowledgments it is possible to increases remaining energy.

Table 6 Results of Packet Loss

packet loss					
Packet loss / NN	10	20	30	40	50
AODV	0.09	0.11	0.13	0.15	0.17
FCH-AODV	0.04	0.06	0.08	0.10	0.12

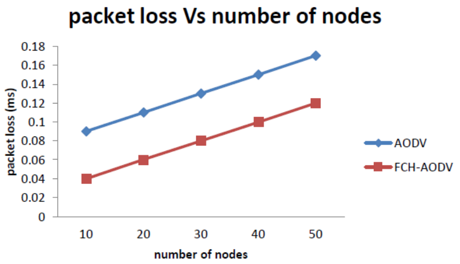

Figure 7 Packet Loss Vs Number of Nodes

The packet loss calculate with varying number of malicious node using FCH algorithm, performance comparison of the proposed and the existing methods is shown in Fig 7 and Table 6. It is observed from Fig 7, the proposed model decreases the average delay by 5% than AODV protocol with the increase in the number of malicious nodes 8 out of 50 nodes. If the malicious node is detected, the FCH algorithm finds alternate shortest route between the sender and receiver, because of new algorithm to allow strongest node transmit without traffic route in the network also new design is capable of finding unbreakable shortest path to reduce data loss while transmitting and receiving packets.

Table 7 Results of Routing Overhead

routing overhead					
Routing Overhead / NN	10	20	30	40	50
AODV	0.27	0.32	0.37	0.42	0.48

FCH-AODV	0.16	0.21	0.26	0.31	0.36

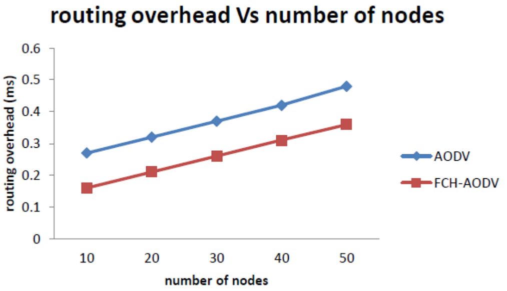

Figure 8 Routing Overhead Vs Number of Nodes

Fig 8 and Table 7 compare the routing overhead performance of the proposed FCH-AODV and existing acknowledgement based AODV schemes, developed method has reduced routing overhead with the number of malicious nodes from 1 to 8 when compared to the existing method as show in Fig 8. Suggested new method has the reduce average routing overhead by 10.2% than AODV, although proposed scheme requires public and private key at all acknowledgement process. Simulation results of the above all the tables and figures its clearly shows that, our proposed new suggested model better outcomes then our traditional on-demand routing protocol.

Conclusion

Cluster selection based mobile ad hoc networks is the important task to finding primary and secondary head selection nodes depends some of conditions such as maximum forward capacity, maximum receiving capacity with minimum path breakage (link breakage). Our developed new design based on the following conditions depends and RREQ, RREP with select best path in best nodes. Parameters of all the above outcomes better than traditional routing protocol, suggested FCH-AODV improved packet delivery ratio performance by 15%, increase average throughput by 15.2%, increases the average remaining energy by 10%, decreases the average delay by 5% and reduce average routing overhead by 10.2% when number of malicious nodes is 8, maximum number of nodes 50, topology area 600 m * 600 m with simulation time 500 s when compared to the existing method.

Declarations

I, certify that: I have read and approved the final version of the manuscript. I have made substantial contributions to the submitted work, which may include study design, data acquisition and/or analysis, and data interpretation.

Reference

[1] R. Santosh Kumar Mahto, et al, “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, 2012.

[2] Akshayadevi Arivazhagan, et al, “Performance Comparison of on Demand Routing Protocols under Back whole For MANET”, Advance Research in Computer science and software Engineering, Vol. 5, No. 3, pp. 407 – 411, 2015.

[3] Akshaya Devi Arivazhagan, et al, “Co-operative analysis of Proactive and Reactive Protocols Using Dijkstra's Algorithm” IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO-2015)”, Karpagam Engineering College, Coimbatore, India during 09-10 January 2015

[4] Akshaya Devi Arivazhagan. et al. “Energy Efficient Routing Protocol with Ad hoc On-Demand Distance Vector for MANET”, IEEE Explore, Vol. 2, pp.158-163, 2015.

[5] K. Thamizhmaran “Performance Evaluation of EA3ACK in different topology’s Using EAACK for MANET, I - Manager Journal of information technology , Vol. 5, No. 4, pp. 5-10, 2016.

[6] Alamelunachippan, et al. “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, 2017.

[7] Alamelunachippan, et al. “Performance Analysis of On-demand Routing Protocol for MANET Using EA3ACK Algorithm”, International Journal of Mobile Network Design and Innovation (Inderscience), Vol. 7, No. 2, pp. 88-100, 2017.

[8] K. Thamizhmaran “Modified ABR (M-ABR) Routing Protocol with Multi-cost Parameters for Effective Communication in MANETs, IJARCS, Vol. 8, No. 1, pp. 288-291, 2017.

[9] Alamelunachippan, et al. “Reduced End-To-End Delay for MANETS using SHSP-EA3ACK Algorithm”, Journal on Communication Engineering and System, Vol. 7, No. 3, pp. 8-15, 2018.

[10] R.Pushpavani, et al, (2017) “Fast Handover Algorithm for Mobility Management in VANETs”, IJARCS, Vol. 8, No. 3, pp. 860-863.

[11] K.Vennila and K.Thamizhmaran “Multilevel image segmentation based on firefly algorithm”, International Journal of Biometrics and Bioinformatics, CIIT, Vol.9, N0. 3, pp. 57-60, 2017.

[12] K.Thamizhmaran, Dr. K. Prabu “Trust Based Dynamic Source Routing Protocol by Exclusion of Black-Hole Attack for MANETs”, International Journals of Computer Science Trends and Technology, Vol. 5, No. 2, pp. 486-490, 2017.

[13] K.Thamizhmaran “Secure Three Acknowledgements Based Quality Routing Protocol for WSN”, Journal of Optoelectronics and Communication (HSBR), Vol. 2, No. 3, pp. 1-5, 2020. https://doi.org/10.5281/zenodo.4042916

[14] K.Thamizhmaran “EE-ATPSP – Evaluation Node Life Time for WSNs”, i-manager’s Journal on Wireless Communication Network Vol. 8, No. 4, pp. 27-35, 2020.

[15] A.Kayalvizhi, et al, “Implement PAPR Reduction in OFDM System Using SAS DCT with Commanding”, IJARCS, Vol. 8, No. 3, pp. 922-925, 2017.

[16] K. Thamizhmaran “EEQRP-Energy Efficient Quality Routing Protocol for Wireless Sensor Networks, Journal of Signal Processing, Vol. 3, No. 1, pp. 1-6, 2017.

[17] K.Thamizhmaran “Markovian Implementation Methods using Mobile Ad hoc Networks”, Journal of Wireless Communication, Network and Mobile, Vol. 4, No. 2, pp. 21-29, 2019.

[18] K.Thamizhmaran, “Performance Analysis of TS-AODV and MTS-AODV Routing Protocols in MANET”, Journal of Computer Science Engineering and Software Testing, Vol. 3, No. 1, pp. 1-8, 2017.

[19] A.Akshyadevi, et al, “Energy Efficient Routing Protocol with Ad hoc on-demand Distance Vector for MANET” WEAST, Vol. 2, No. 8, pp. 1-6.

[20] K.Thamizhmaran “Security Attacks in Wireless Sensor Networks – A Study”, i-manager’s Journal on Information Technology, Vol. 9, No. 1, pp. 35-43, 2020.

There is no funding source for my research article

ACKNOWLEDGMENT

I would like to thank the above researchers and respected expected reviewers who give their valuable review comments with suggestions for updating to improve quality of this research paper. We would like to thank authorities of the estimated Annamalai University, Tamilnadu, India.

Biography:
Prof. Dr. A. Charles received his Ph.D degree from Faculty of Engineering Annamalai University, Tamilnadu in the year 2018 respectively. He is currently working as an Assistant Professor in the Department of Electronics & Communication Engineering, Government College of Engineering, Bargur, and Tamilnadu, India, he is teaching experience 15.5. His research interest includes Wireless Communication, Ad-Hoc Networks. He has published more than 35 technical papers at various National / International reputed Conferences and in journals Scopus/h UGC approved publications.

Prof. V. Rajesh Kannan received his B.E and M.E degrees from Faculty of Engineering and Technology, Annamalai University, Tamilnadu in the year 2007 and 2012 respectively. He is currently pursing Doctor of Philosophy in Mobile Ad-hoc Network, Faculty of Engineering Annamalai University from 2018 to till date. He is currently working as an Assistant Professor in the Department of Electronics & Communication Engineering, Government College of Engineering, Bargur, Tamilnadu, India and teaching experience 14.6 years. His research interest includes Wireless Communication, Ad Hoc Networks, he has published more than 10 technical papers at various National / International reputed Conferences and in journals including Scopus/UGC approved publications.

List of Abbreviations

MANET – Mobile Ad hoc Network
NS2 – Network Simulator 2
FCH – Fuzzy Cluster Head
AODV - Ad hoc On-Demand Distance Vector
PRNET - Packet Radio Network
DARPA - Defence Advanced Research Projects Agency
WSN – Wireless Sensor Networks
WMN – Wireless Mesh Network
VANET – Vehicular Ad hoc Networks
PDA - Personal Digital Assistants
DoS - Denial of Service
WiMax - Worldwide Interoperability for Microwave Access
RREQ - Route Request

RREP – Route Replay
IEEE - Institute of Electrical and Electronics Engineers
MFC - Maximum Forwarding Capacity
MRC - Maximum Receiving Capacity
MLB - Minimum Link Brakeage
FC – Fuzzy Controller
ACK – Acknowledgement
PDR – Packet Delivery Ratio
NN – Number of Nodes