Decision Making: Applications in Management and Engineering

ISSN: 2560-6018, eISSN: 2620-0104

PERFORMANCE COMPARISON OF RELAY NODE RANDOM SELECTION METHOD USING DIFFERENT SET OF PARAMETER FOR MANET

K.Thamizhmaran[1], Dr.A.Charles[2]

[1]Department of ECE, Annamalai University, Chidambaram, Tamilnadu, INDIA

[2]Department of ECE, Annamalai University, Chidambaram, Tamilnadu, INDIA

[1]*tamil10_happy@rediff.com*, [2]*charlesgceb@gmail.com*

[1&2]*www.annamalaiuniversity.ac.in (+91-9566642737)*

[1]Corresponding Author

Abstract

Treads of today research uncertainty environment and natural situation if focussed in Mobile Ad hoc Networks, a big challenge to develop routing protocol that can meet different application needs and optimize routing paths according to the topology change in mobile ad hoc networks [1], [2]. 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 connection [3]. This research aims to propose CH-RNSR with hybrid cryptography (ECC) using RNSR algorithm. The main aim of the proposed research CH-RNSR with ECC algorithm is to increase the remaining energy with the number of malicious nodes detected during the communication via acknowledgement base than RNSR with help of one of leading simulation model called Network Simulator 2.34 work with different set of nodes, malicious nodes in same topology size using various parameters such as packet delivery ratio, throughput, routing overhead, packet loss, delay and remaining energy via Network Simulator 2 (NS2).

Keywords: MANET, attack, Energy Models, cryptography, NS2.

I. INTRODUCTION

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 **[4]**, **[5]**. 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. In this manuscript performance comparison between RNSR, CH-RNSR and CHRNSR-ECC algorithms with various types of scenarios, multipath importance techniques using alternative multiple paths in network which can elide provide such as tolerance increase bandwidth and improving security, communication based on some criteria like minimum cost, minimum weight, maximum forwarding capability, maximum receiving capability, minimum link breakage path etc **[6], [7] [8]**.

II. PROBLEM IDENTIFICATION

The dynamic nature of MANET requires the routing protocol to refresh the routing tables frequently and suffers from transmission time delay and congestion. The CH-RNSR improves the network performance in the presence of consecutive collaborative misbehaving nodes in a route of active and passive path for both low speed and high-speed networks, even though in CH-RNSR the network security is more robust, the utilized energy and network routing overhead increase **[9], [10], [11], [12]**. To overcome this, CH-RNSR along with elliptical cryptography is proposed to increase the remaining energy, throughput and reduce memory allocation, time taken and overhead of the routing network. IT should be noted that in ECC, reduced energy utilization time the period of key exchange.

Algorithm:

Encryption Process (Suppose X sends a message M to Y)

- Look up B's Public Key: Q.
- Represent the transmitting message 'M' as pair of the field elements (M_1, M_2), M_1 GF, M_2 Z_p-1.
- Select a random integer, such that Z_p-1
- Compute the point (A_1, B_1) = P
- Compute the point (A_2, B_2) = Q.
- Combine both the field elements M_1, M_2 with A_2, and B_2 with an algorithm to give two field elements C_1 and C_2.
- Transmit the data M = (A_1, B_1, C_1, C_2) to Bob.

Decryption Process (B gets the text M = (A_1, B_1, C_1, C_2) from A)

- Compute the point (A_2, B_2) = k (A_1, B_1), using its private key k.
- Decrypt M_1 and M_2 from M. The prime p used in the ECC hybrid system is smaller than the numbers required in all the other types of cryptograms. So another advantage of the ECC is that the modified calculations required are carried out over a smaller modified operation. This leads to a significant improvement in efficiency in the operation of the ECC over both integral factorization and discrete algorithm cryptograms [13].

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	1000m*1000m,
Number of nodes	100, 200
Protocols	CHRNSR-ECC
Constant bit rate	4 (packets/second)
Packet size	512 bytes
Initial energy/node	100 joules
Simulation time	500 sec
Malicious node	10, 20

IV. RESULT AND DISCUSSION

In this section we discussed results and discussion of existing and proposed methods with four different parameters via NS2.

Table 2 Results of Parameter Values (SA=1000m, NN=100 & MN=10) (*Source*: from Ref. [9 &10])

Packet Delivery Ratio					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	0.24	0.29	0.34	0.39	0.44
RNSR (K.Thamizhmaran, 2022 [9])	0.51	0.55	0.59	0.63	0.68
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.56	0.60	0.64	0.68	0.73
CHRNSR-ECC	0.61	0.65	0.69	0.73	0.78
Throughput					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	210	260	310	360	410
RNSR (K.Thamizhmaran, 2022 [9])	280	330	380	430	480
CH-RNSR (K.Thamizhmaran, 2022 [10])	320	370	420	470	520
CHRNSR-ECC	340	390	440	490	540
Packet Loss					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	0.53	0.49	0.44	0.40	0.35
RNSR (K.Thamizhmaran, 2022 [9])	0.43	0.39	0.34	0.30	0.25
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.36	0.32	0.27	0.23	0.18
CHRNSR-ECC	0.32	0.28	0.23	0.19	0.14
Remaining Energy					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	820	740	690	650	610
RNSR (K.Thamizhmaran, 2022 [9])	840	760	710	670	630
CH-RNSR (K.Thamizhmaran, 2022 [10])	810	710	660	620	580
CHRNSR-ECC	920	840	790	750	710
Routing Overhead					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	0.10	0.16	0.20	0.28	0.36
RNSR (K.Thamizhmaran, 2022 [9])	0.12	0.18	0.22	0.30	0.38
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.10	0.13	0.16	0.24	0.32
CHRNSR-ECC	0.06	0.10	0.12	0.20	0.28

PDR=Packet Delivery ratio, PL=Packet Loss, RE=Remaining Energy, RO=Routing Overhead

Simulation results are obtained by varying the number of nodes from 10 to 100. The performances of the proposed CHRNSR-ECC and the existing CH-RNSR, RNSR & DSR compared. Fig. 1(a) and Table 2 show the proposed model with improved packet delivery ratio in number of malicious nodes is varied from 1 to10 when compared to the existing method. It is clear that proposed scheme surpasses 35.17% than DSR, 10% than RNSR and 5% than CH-RNSR, is able to detect malicious in the presence of receiver collision, 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 CHRNSR-ECC has increase average throughput by

2% than CH-RNSR, 6% than RNSR and 13% then DSR 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 packet loss with varying number of malicious nodes using ECC 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 packet loss by 4% than CH-RNSR, 11% than RNSR and 21% than DSR protocol with the increase in the number of malicious nodes from 1 to 10 out of 100 nodes. If the malicious node is detected, the RNSR algorithm finds alternate shortest route between the sender and receiver, because of RNSR algorithm to allow strongest node transmit without traffic route in the network. The impact of packet loss on reaming energy is analysed using the four 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 average utilization energy by 12.67% than CH-RNSR, 8% than RNSR and 10% than DSR 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 routing traffic when the number of malicious nodes varied and compared to the existing system. It is clear that the proposed design reduced the average overhead by 3.84% than CH-RNSR, 9% than RNSR and 7.34% than DSR with the increasing nodes 10 to 100, due to increases duration of time period of acknowledgments than other acknowledgments it is possible to increases remaining energy and reduced traffic, although CHRNSR-ECC requires public and private key at all acknowledgement process with number of malicious nodes 10 out of 100 using 1000m*1000m topology size.

Table 3 Results of Parameter Values (SA=1000m, NN=100 & MN=20) (*Source*: from Ref. [9 &10])

Packet Delivery Ratio					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	0.25	0.30	0.35	0.40	0.45
RNSR (K.Thamizhmaran, 2022 [9])	0.52	0.56	0.60	0.64	0.69
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.57	0.61	0.65	0.69	0.74
CHRNSR-ECC	0.62	0.66	0.70	0.74	0.79
Throughput					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	230	280	330	380	430
RNSR (K.Thamizhmaran, 2022 [9])	300	350	400	450	500
CH-RNSR (K.Thamizhmaran, 2022 [10])	340	390	440	490	540
CHRNSR-ECC	360	410	460	510	560
Packet Loss					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	0.52	0.48	0.43	0.39	0.34
RNSR (K.Thamizhmaran, 2022 [9])	0.42	0.38	0.33	0.29	0.24
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.35	0.31	0.26	0.22	0.17
CHRNSR-ECC	0.31	0.27	0.22	0.18	0.13
Remaining Energy					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	800	720	670	630	590

RNSR (K.Thamizhmaran, 2022 [9])	820	740	690	650	610
CH-RNSR (K.Thamizhmaran, 2022 [10])	790	690	640	600	560
CHRNSR-ECC	900	820	770	730	690
Routing Overhead					
Protocol / Number of Nodes	20	40	60	80	100
DSR (K.Thamizhmaran, 2022 [9])	0.08	0.14	0.18	0.26	0.38
RNSR (K.Thamizhmaran, 2022 [9])	0.10	0.16	0.20	0.28	0.36
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.08	0.11	0.14	0.22	0.30
CHRNSR-ECC	0.04	0.08	0.10	0.18	0.26

The result obtained is given in Table 3 and Fig. 2(a), Fig. 2(b), 2(c), 2(d), 2(e) and 2(f) the malicious node is varied from 1 to 20 out of 100 and simulation is carried out to calculate the packet delivery ratio using all the three methods. It is clear from the simulation results of Fig. 2(a) that the CHRNSR-ECC has the maximized average packet delivery ratio 5% than CH-RNSR, 10% than RNSR and 35.17% than DSR with topology size 1000m*1000m. Result of Fig. 2(b) shows that CHRNSR-ECC has increase average throughput by 2% than CH-RNSR, 6% than RNSR and 13% than DSR. 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 packet loss by 4% than CH-RNSR, 11% than RNSR and 21% than DSR protocol with the increase in the number of malicious nodes from 1 to 20 out of 100 nodes. Simulation results are shown in Fig. 2(d) and Table 3. From the simulation results it is understood that the proposed algorithm reduced average energy utilization 12.67% than CH-RNSR, by 8% than RNSR and 10% than DSR design. Fig. 2(e) it is clear that the proposed design decreases the overhead by 3.84% than CH-RNSR, 9% than RNSR and 8.34% than DSR with the increasing nodes with number of malicious nodes 20 out of 1000 using 1000m*1000m.

Table 4 Results of Parameter Values (SA=1000m, NN=200 & MN=10) (*Source*: from Ref. [9 & 10])

Packet Delivery Ratio					
Protocol / Number of Nodes	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	0.22	0.27	0.32	0.37	0.42
RNSR (K.Thamizhmaran, 2022 [9])	0.47	0.51	0.54	0.59	0.64
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.53	0.57	0.61	0.65	0.70
CHRNSR-ECC	0.58	0.62	0.66	0.70	0.75
Throughput					
Protocol / Number of Nodes	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	180	230	280	330	380
RNSR (K.Thamizhmaran, 2022 [9])	250	300	350	400	450
CH-RNSR (K.Thamizhmaran, 2022 [10])	290	340	390	440	490
CHRNSR-ECC	310	360	410	460	510
Packet loss					
Protocol / Number of Nodes	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	0.56	0.52	0.47	0.43	0.38
RNSR (K.Thamizhmaran, 2022 [9])	0.46	0.42	0.37	0.33	0.28
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.39	0.35	0.30	0.26	0.21
CHRNSR-ECC	0.35	0.31	0.26	0.22	0.17

Remaining Energy					
Protocol / Number of Nodes RE/NN	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	750	670	620	580	540
RNSR (K.Thamizhmaran, 2022 [9])	770	690	650	600	560
CH-RNSR (K.Thamizhmaran, 2022 [10])	740	650	600	550	510
CHRNSR-ECC	850	770	720	680	640
Routing Overhead					
Protocol / Number of Nodes	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	0.14	0.20	0.24	0.32	0.40
RNSR (K.Thamizhmaran, 2022 [9])	0.16	0.22	0.26	0.34	0.42
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.10	0.13	0.16	0.24	0.32
CHRNSR-ECC	0.06	0.10	0.12	0.20	0.28

Above simulation outcomes performances of the proposed CHRNSR-ECC and the existing CH-RNSR and RNSR compared with 1000m*1000m using 10 malicious nodes out of 200 nodes, Fig. 3(a) and Table 3 it is clear that proposed scheme surpasses CHRNSR-ECC has the maximized average packet delivery ratio 5% than CH-RNSR, 11.17 than RNSR and 34.16% than DSR, Result of Fig. 3(b) shows that CHRNSR-ECC has increase average throughput by 2% than CH-RNSR, 6% than RNSR and 13% than DSR. 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 packet drop by 4% than CH-RNSR, 11% than RNSR and 21% than DSR with the increase in the number of malicious nodes from 1 to 12 out of 60 nodes. Fig. 3(d) and Table 4 from the simulation results it is understood that the proposed algorithm reduced average utilization energy by 12.34% than CH-RNSR, 7.88% than RNSR and 10% than DSR 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 traffic rate when the number of malicious nodes varied compared to the existing system. It is clear that the proposed design reduced traffic rate 3.84% than CH-RNSR, 13% than RNSR and 11% than DSR with the increasing nodes 40 to 200, due to minimize duration of time period of acknowledgments than other acknowledgments it is possible to increases remaining energ.

Table 5 Results of Parameter Values (SA=1000m, NN=200 & MN=20) (*Source*: from Ref. [9 &10])

Packet Delivery Ratio					
Protocol / Number of Nodes	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	0.22	0.27	0.32	0.37	0.42
RNSR (K.Thamizhmaran, 2022 [9])	0.47	0.51	0.54	0.59	0.64
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.53	0.57	0.61	0.65	0.70
CHRNSR-ECC	0.58	0.62	0.66	0.70	0.75
Throughput					
Protocol / Number of Nodes	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	180	230	280	330	380
RNSR (K.Thamizhmaran, 2022 [9])	250	300	350	400	450
CH-RNSR (K.Thamizhmaran, 2022 [10])	290	340	390	440	490
CHRNSR-ECC	310	360	410	460	510
Packet loss					
Protocol / Number of Nodes	40	80	120	160	200

DSR (K.Thamizhmaran, 2022 [9])	0.56	0.52	0.47	0.43	0.38
RNSR (K.Thamizhmaran, 2022 [9])	0.46	0.42	0.37	0.33	0.28
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.39	0.35	0.30	0.26	0.21
CHRNSR-ECC	0.35	0.31	0.26	0.22	0.17
Remaining Energy					
Protocol / Number of Nodes	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	750	670	620	580	540
RNSR (K.Thamizhmaran, 2022 [9])	770	690	650	600	560
CH-RNSR (K.Thamizhmaran, 2022 [10])	740	650	600	550	510
CHRNSR-ECC	850	770	720	680	640
Routing Overhead					
Protocol / Number of Nodes	40	80	120	160	200
DSR (K.Thamizhmaran, 2022 [9])	0.14	0.20	0.24	0.32	0.40
RNSR (K.Thamizhmaran, 2022 [9])	0.16	0.22	0.26	0.34	0.42
CH-RNSR (K.Thamizhmaran, 2022 [10])	0.10	0.13	0.16	0.24	0.32
CHRNSR-ECC	0.06	0.10	0.12	0.20	0.28

Table 5 and Fig. 4(a) packet delivery ratio, Fig. 4(b) throughput, Fig.4(c) packet loss, Fig. 4(d) remaining energy, Fig. 4(e) routing overhead carried out the malicious node is varied from 1 to 20 out of 90 using topology area is 1000m*1000m and simulation is to calculate the all the parameters using all the three modes. Fig. 4(a), 4(b) & 4 (c) shows that CHRNSR-ECC has the maximized average packet delivery ratio by 16.78%, average throughput by 7% and average remaining energy by 10.06% compared to the CH-RNSR, RNSR and DSR. 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 packet loss by 12% than existing design. Fig. 4(e) it is clear that the proposed design reduces the average routing overhead by 9.28% with the increasing nodes 40 to 200 than CH-RNSR, RNSR and DSR.

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

V. CONCLUSIONS

In this research, simulation result of all the proposed algorithms as compared with the existing three algorithms with four different scenarios through the network simulation 2.34. This developed model ability to detect misbehaviour nodes with improves average packet delivery ratio for all the four scenarios with three different existing models by 16.89%, improved average throughput by 7%, clearly shows propose system increased average remaining energy by 10.14%, reduced average packet loss for all the four scenarios by 12% and reduce average routing overhead by 8.09% than other methods with number of malicious node 10 & 20 out of 100 & 200 nodes using 1000m*1000m network topology, Fig 5 and Table 6 results of all parameters with average values of all scenarios also solve weakness of existing method.

Table 6 Results of Parameter Average Values of All Scenarios

Scenarios	Parameters	DSR	RNSR	CH-RNSR

Average Value of scenarios 1, 2, 3 & 4	Packet Delivery Ratio	35.08%	10.59%	5%
	Throughput	13%	6%	2%
	Packet Loss	21%	11%	4%
	Remaining Energy	10%	7.93%	12.50%
	Routing Overhead	9.42%	11%	3.84%

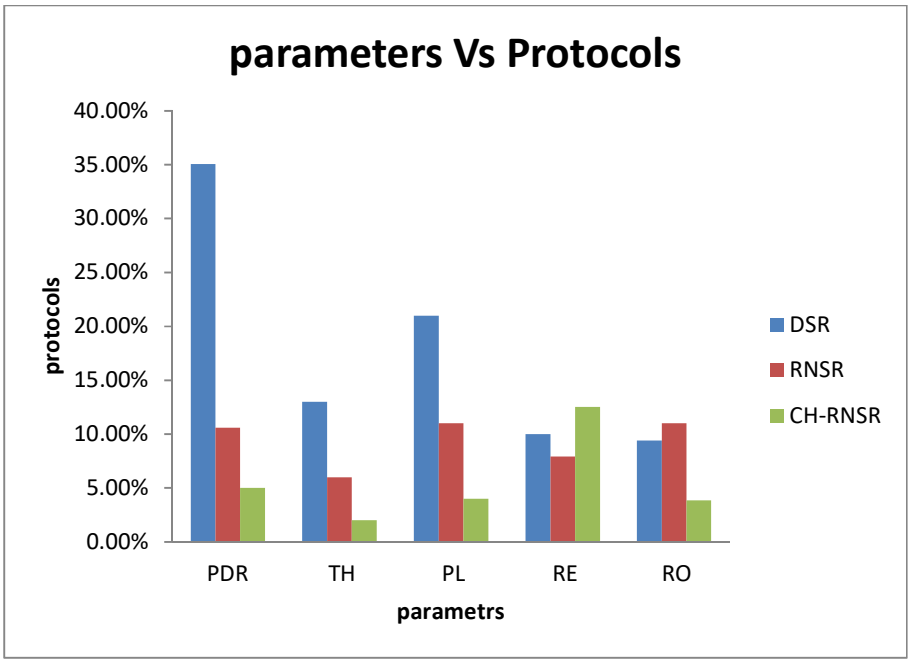

Fig 5 results of all parameters with average values of all scenarios

We plan to investigate the following issues in our future research. 1) The possibilities of adopting the shortest path algorithm to eliminate the requirement of redistributed; can be examined. 2) The performance of CHRNSR-ECC can be tested in real time network environment Instead of software simulation.

There is no funding source for my research article

Deceleration

Prof. Dr. A. Charles who provides ideas to build the manuscript and also share review comments, corresponding author of this paper Prof. K. Thamizhmaran who has collecting data with implementation using software with manuscript preparation.

Conflict of Interest

I confirm that neither I nor any of my relatives nor any business with which I am associated has any personal or business interest in or potential for personal gain from any of the organizations or projects

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 intuitions Annamalai University,

VI. REFERENCE

1. Li. Chun-Ta, "A New Password Authentication and User Anonymity Scheme Based on Elliptic Curve Cryptography and Smart Card", *IET Information Security,* Vol. 7, No. 1, pp. 3–10, March. 2013.
2. Chien-Lung Hsu, and Yu-Li Lin, "Improved Migration for Mobile Computing in Distributed Networks", *Computer Standards & Interfaces,* Vol. 36, No. 3, pp. 577–584, 2014.
3. Baojun Huang., Muhammad Khurram Khan., Libing Wu., T. Faha, Bin Muhaya., and Debiao He., "An Efficient Remote User Authentication with Key Agreement Scheme Using Elliptic Curve Cryptography", *Wireless Personal Communications,* Vol. 85, No. 1, pp. 225-240, May. 2015.
4. K. Prabu and K. Thamizhmaran, "Forward Direction to Future Research for Big Data", *International Journal of Modern Computer Science,* Vol. 4, No. 1, pp. 74-77, 2016.
5. K.Thamizhmaran, M.Anitha and Alamelunachippan "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.
6. Akram Kout., Said Labed., Salim Chikhi., and El Bay Bourennane., "AODVCS, a new bio-inspired routing protocol based on cuckoo search algorithm for mobile ad hoc networks", *Wireless Network,* Vol. 24, No. 7, pp. 2509-2519, Oct. 2018.
7. Danish Sattar and Ashraf Matrawy "Optimal Slice Allocation in 5G Core Networks," *IEEE Networking Letters,* Vol. 1, No. 2, pp. 48-51, March. 2019.
8. N.S. Saba Farheen, and Anuj Jain, "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, June. 2020.
9. Nobuyoshi Komuroa, and Hiromasa Habuchi, "Nonorthogonal CSK/SS ALOHA system under MANET environment", *The Korean Institute of Communications and Information Sciences,* Vol. 7, No. 3, pp. 78-84, Dec. 2021.
10. Nivedita Yutao Liu, Yue Li, Yimeng Zhao, and Chunhui Zhang, "Research on MAC Protocols in Cluster-Based Ad Hoc Networks" *Wireless Communications and Mobile Computing,* Vol. 23, 1-12, March. 2021.
11. K.Thamizhmaran & A.Charles "Energy Efficient Data Transmission for Mobile Ad hoc Network", *Grenze International Journal of Engineering and Technology,* Jan Issue, pp. 326-331, 2022.
12. K. Thamizhmaran & Dr. A. Charles "Cluster Head Selection based Energy Aware Routing Protocol for MANET", *International Journal of Communication,* Vol. 7, pp. 6-11, 2022.
13. Jafar Ramadhan Mohammed, and Rasha Bashar Mohammed, "Simplified Adaptive Interference Suppression Methods Based on Subarray Configurations for 5G Applications," *International Journal of Microwave and Optical Technology,* Vol.17, No.4, pp. 331-338, July. 2022.

BIOGRAPHICAL NOTE

Prof. K. Thamizhmaran received his B.E, M.E, degree from Faculty of Engineering and Technology. Post Graduate diploma in yoga, M.sc in yoga degree from Faculty of Education and Post Graduate in Guidance & Counseling degree from Faculty of Psychology, Annamalai University. He is currently pursing Doctor of Philosophy in Mobile Ad hoc Network (Network Security) from 2013 to till date. He is currently working as an Assistant Professor & NSS Programme Officer in the Dept. of ECE, Government College of Engineering, Bodinayakkanur, Theni and Tamilnadu. Teaching experience 15+ years, research experience 13 years and industrial experience 02 months (team leader in honey drops-Chennai). His research interest includes Wireless Communication, Mobile Ad hoc Networks, Networks Security, Mobile Communications and Supply Chain Management, E-Waste Management. He has published more than 560+ technical papers at various National / International Conferences and in reputed journals including SCI / Scopus / WoS with UGC approved journals. He has published 04 academic technical books for International Publication. He has published more than 07 book chapters at various International reputed publications from India and Germany and act as Editor of 10 international conference books from India & Turkey. He is a member life 26 professional bodies and he is editor, advisory board member and reviewer of 35+ international journals throughout world.

Prof. Dr. A. Charles received his B.E, M.E, Ph.D degree from Faculty of Engineering and Technology, Annamalai University and India. He is currently working as an Assistant Professor in the Dept. of ECE, Government College of Engineering, Bargur and Tamilnadu, teaching experience 16+ years. His research interest includes Mobile Ad hoc Networks, Networks Security. He has published more than 45 technical papers at various National / International Conferences and in reputed journals including SCI / Scopus / WoS with UGC approved journals.