IJMRSETM

e-ISSN: 2395 - 7639

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 9, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.580

+91 99405 72462 +9163819 07438 ijmrsetm@gmail.com www.ijmrsetm.com

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 9, Issue 5, May 2022 |

| DOI: 10.15680/IJMRSETM.2022.0905022 |

Energy-AwareTransmission Scheme for Secure Conscious Routing in Mobile Adhoc Network

Amandeep Makkar[1] and Sunil Taneja[2]

[1]Department of Computer Science, Arya Girls College, Ambala Cantt, Haryana, India

[2]Department of Computer Science, Government College, Aharwala (Bilaspur), Haryana, India

ABSTRACT: Digital Revolution is marked with diverse utility of wireless technology for mobile communication. MANET comprises of moving nodes and these nodes communicate with other nodes until they remain in radio range of each other. MANET suffers from two main issues, security attacks and high energy consumption. These two issues cumulatively deteriorate the performance of MANET. Therefore, improvement in routing protocol is a challenge for researchers to overcome security lacunas and achieve energy efficiency to facilitate mobile devices with advance computing capabilities that are mostly energy starved. In this research paper, effort has been made to overcome these challenges. Energy Aware Secure routing algorithm based on AODV routing protocol (EAS-AODV) is proposed in this paper. Simulation results through NS2 simulator shows that proposed mechanism provides an energy efficient secure routing protocol that enhances the performance of MANET over various parameters.

KEYWORDS: Adhoc, AODV, EAS-AODV, Energy, MANET, Network, Security

I. INTRODUCTION

Main characteristic of MANET is the infrastructureless system where nodes are self arranging. In MANET, every node can interact with others without having any base station[1]. Various mobile devices in MANETs comprise of limited resources for data communication such as battery power, limited radio range etc [2]. A node can communicate with other active nodes present in the network for data communication as sender, destination and intermediary node. Figure 1 depicts the data transmission from one node to other node through intermediate nodes which exists in the radio range of each other. During data communication, there can be multiple routes for sending packets from one node to other. Hence efficientrouting is a one of the biggest challenges in the MANET [3, 4].

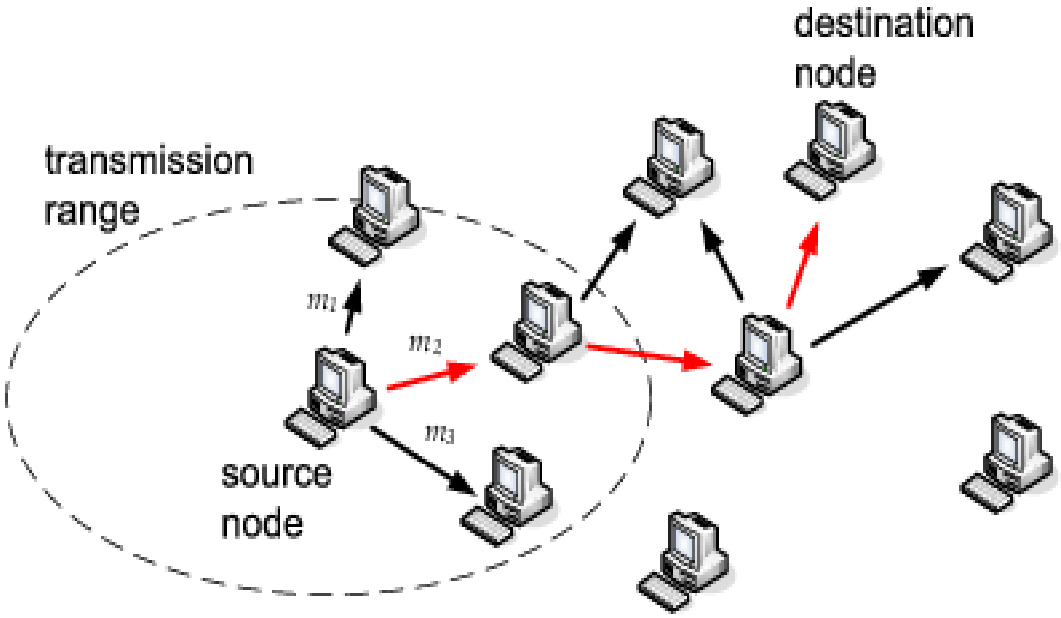


Figure1: Mobile Adhoc Network

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 9, Issue 5, May 2022 |

| DOI: 10.15680/IJMRSETM.2022.0905022 |

With expanding applications of MANET, energy conservation of mobile devices connected in MANET is the prime factor for performance of mobile communication in such networks [5]. For routing purposes, there are numerous routing protocols present in MANET and these protocols falls into three groups [6, 7] viz. "Proactive (table driven) routing protocol, reactive (on-demand) routing protocol and hybrid routing protocol (blend of these two routing schemes)".

On demand routing strategy establishes route only when required and it is most widely used routing because this is more efficient than table driven in mobile environments. A major reactive routing protocol is AODV routing that uses various packets during data communication such as RREQ, RREP and RERR [8]. Since nodes are in motion, recurrentlink break is integral characteristic of MANET leading to more routing overhead in the network. Re-routing process consumes extra energy of nodes leading to the decline of network lifetime [9]. This paper proposes an energy efficient mechanism for enhancing MANET performance through security conscious routing.

II. LITERATURE SURVEY

Ahila et al. proposed"Privacy Protecting Secure and Energy Efficient Routing Protocol (PPSEER)" [10]. This scheme is an effort towards addressing the key challenges of security and energy conservation in MANET. For security operation encryption technique based on group signature is used. Before executing encryption,organization of different nodes in network takes place based on their energy intensity. Encryption technique also includes other secure parameters like maximum transmission power and secret key and these parameters are only known to sender and receiver nodes. On comparison with existing algorithm, enhanced privacy of message and energy efficiency of nodes was found.

Arya et al. proposed modified algorithm with base protocol AODV that ensure more energy efficiency and security of the nodes[11]. Every node in the network set itself as an immoral node on the basis of various flag values and this is done to test out the nasty behavior of adjacent nodes. The route is formed locally with adjacent nodes which have the maximum energy intensity in order to achieve energy efficiency.

S. Kumar et al. projected a "Stability and Energy Aware Reverse Adhoc On demand Distance Vector (SEAR-AODV) Routing protocol" [12]. The work is basically enhancement of AODV protocol. Optimization in this algorithm is performed by calculating reliability factor of different nodes which includes two performance metrics viz. energy and route stability. Subsequently, thealgorithm chose the path with high reliability factor value for data communication.

Phu et al. proposed a secure AODV routing protocol for MANET [13]. In order to improve security in AODV, secure schema strategy is used in which every node in schema strategy holds a list of neighbouring nodes with secret that is mined by performing a key concord during unification of a network. The prime principle of this schema is that for ensuring the non repudiation and integrity of the network, each node performs message authentication process with the sender node before initiating route discovery process. This prevents the network from attacks from malicious nodes. When compared it with existing algorithm the scheme required less power in routing and provided more security.

N. Veeraiah et al. [14] proposed "Trust Aware Secure Energy Efficient Hybrid Protocol" for MANET to address the issues of security and energy management for MANET. A hybrid optimization algorithm was developed whereby fuzzy clustering algorithm, "cat slap single-player algorithm (C-SSA)" along with swarm optimization calculations have been used to achieve efficient and robust routing over MANET.

III. PROPOSED PLAN

As per study of literature, various gaps in MANET routing process are identified. The two major gaps explored in presentwork are security of network and energy conservation in mobile nodes. The proposed algorithm, Energy Aware Secure AODV (EAS-AODV) addresses these challenges.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 9, Issue 5, May 2022 |

| DOI: 10.15680/IJMRSETM.2022.0905022 |

EAS-AODV Algorithm:

Asymmetric cryptography technique is implemented for security of the network. For energy conservation, a mechanism has been devised in which, when route is discovered, upstream node initiates local route request (LRREQ) to its adjacent nodes as a substitute of generating RRER message and adjacent nodes respond with RREP with their respective energy values. Step by step methodis given below:-

1. Sender initiates RREQ with its certificate and

   IF (Energy left within a mobile node > Threshold energy)

   THEN
   Mobile node is chosen for route information

   OTHERWISE
   LRREQ is generated by upstream mobile node

2. RREQ is received by the neighboring node and

   IF(Neighboring node is destination node)

   THEN
   RREP is sent to source node

   OTHERWISE
   RRRQ is forwarded to the adjoining nodes and
   the process is repeated as long as destination node is not reached

3. Subsequently,

   IF(Destination node is able to carry out decryptionof certificate
   and extracts IP address, sender node's public key & time stamp)

   THEN
   Sender node is treated as *"legitimate node"*

   OTHERWISE
   RREQ has been originated by *"malicious node"*

4. Destination node initiates RREP with a range of routes accessible to destination. Each and every path is examined in order to compute total energy of each path which is divided by its equivalent hop count and is denoted as "E".

5. Finally, path with maximum value of "E" is chosen for transmission of packets.

IV. SIMULATION STUDY

Simulation through NS2 simulator is done to implement proposed protocol EAS-AODV over various parameters shown in Table 1. Performance is evaluated on various metrics and it is analyzed that proposed algorithm, EAS-AODV outperforms the existing algorithm.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

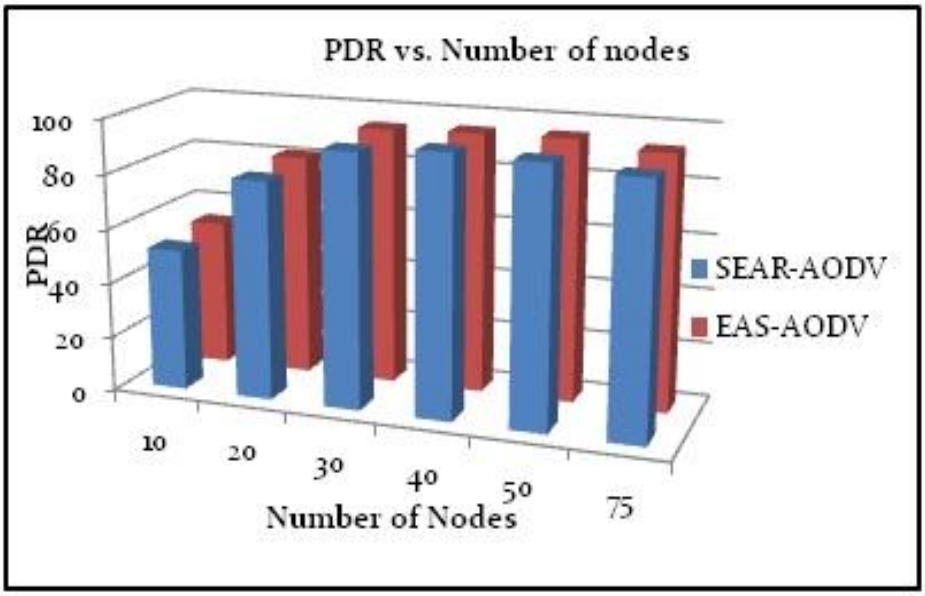
| Volume 9, Issue 5, May 2022 |

| DOI: 10.15680/IJMRSETM.2022.0905022 |

Table 1: Simulation Parameters

Parameter	Values
Routing Protocol	SEAR- AODV, EAS-AODV
No. of Nodes	10,20,30,40,50,75
Terrain Area	1000mX1000m
Simulation Time	100 sec
Packet Size	512 bytes
Maximum Speed of nodes	2,5,10,25,50,75 m/s
Transmission Range	250 m
No of Flows	10
Frequency Band	2.4 GHz
Propagation Type	Propagation/ TwoRayGround
Queue Type	Queue/Drop Trail/PriQueue
Mobility Model	Random Waypoint
Nodes' Initial Energy	100 J
S Thr2	1.5×R×Thr
S Thr1	1.5×R×Thr
Pause Time	2 sec
Queue Length	50
MAC Type	Mac/802_11b
Antenna	Antenna/Omni Antenna
Traffic Type	CBR
Bandwidth	2.0 Mbps
Transmission Rate	4 Packets/ Sec

It can be easily inferred from the graph 1 to graph 5 that the proposed algorithm is extra consistent than traditional routing protocol. Graph 1 provides comparison of "packet delivery ratio (PDR)" with varying number of nodes from 10 to 75. It is clear from the graph that EAS-AODV gives better PDR than SEAR-AODV routing protocol.



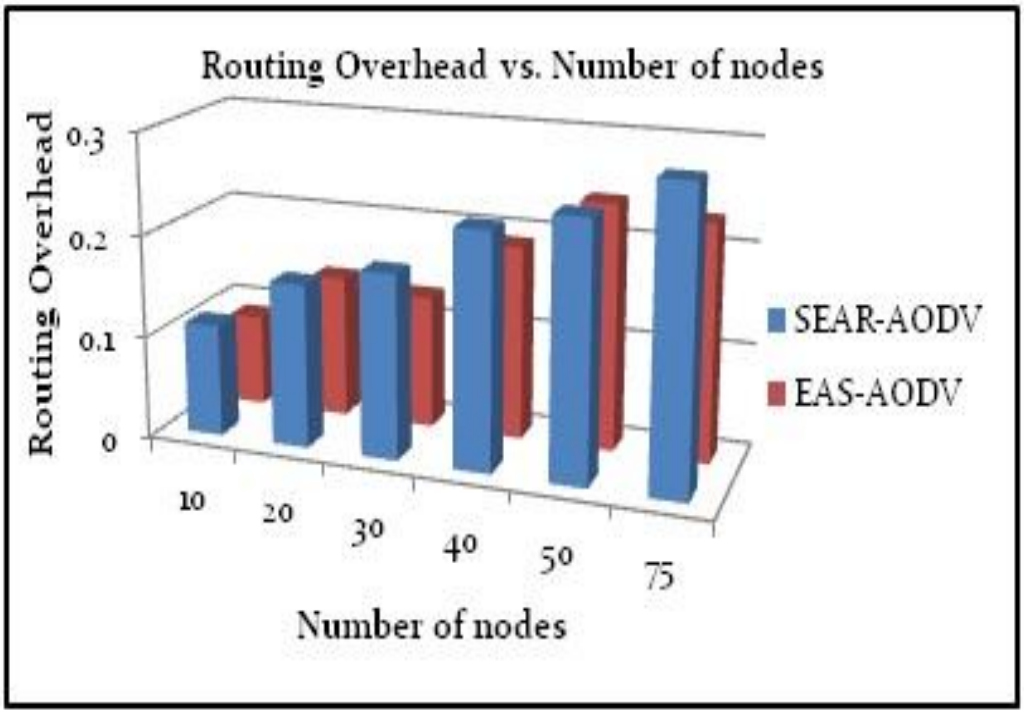
Graph 1: PDR

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

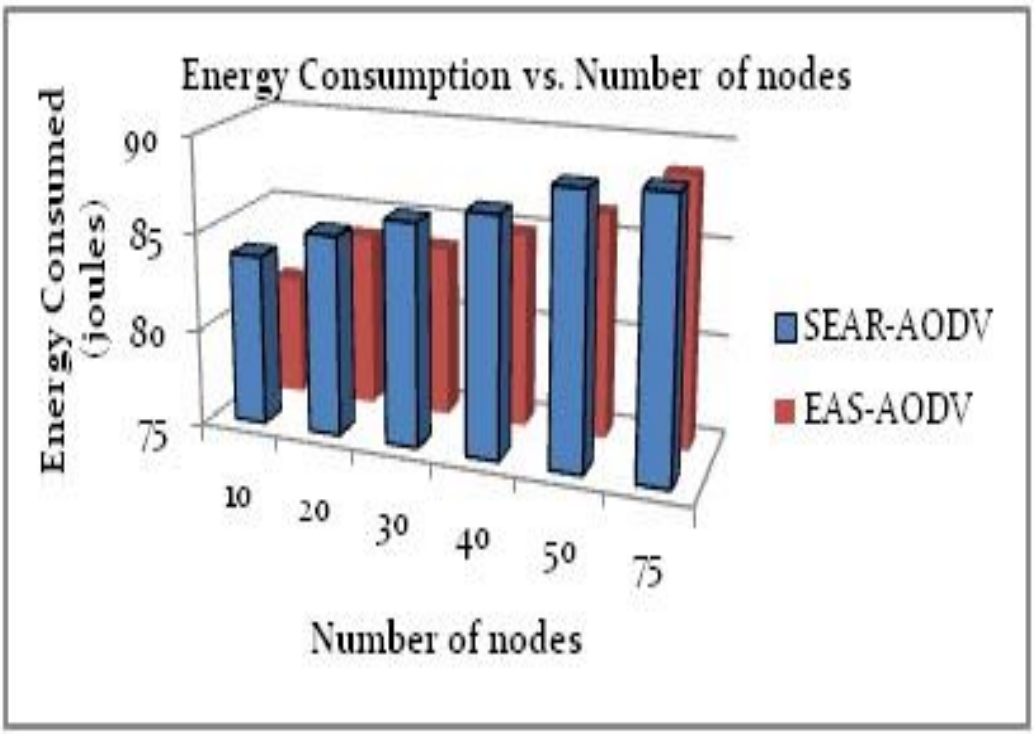
| Volume 9, Issue 5, May 2022 |

| DOI: 10.15680/IJMRSETM.2022.0905022 |

Graph 2 and Graph3 provides comparison of routing overhead and energy consumption during data communication respectively. As results are analyzed, it shows that EAS-AODV performs better in comparison to existing protocol.



Graph 2: Routing Overhead

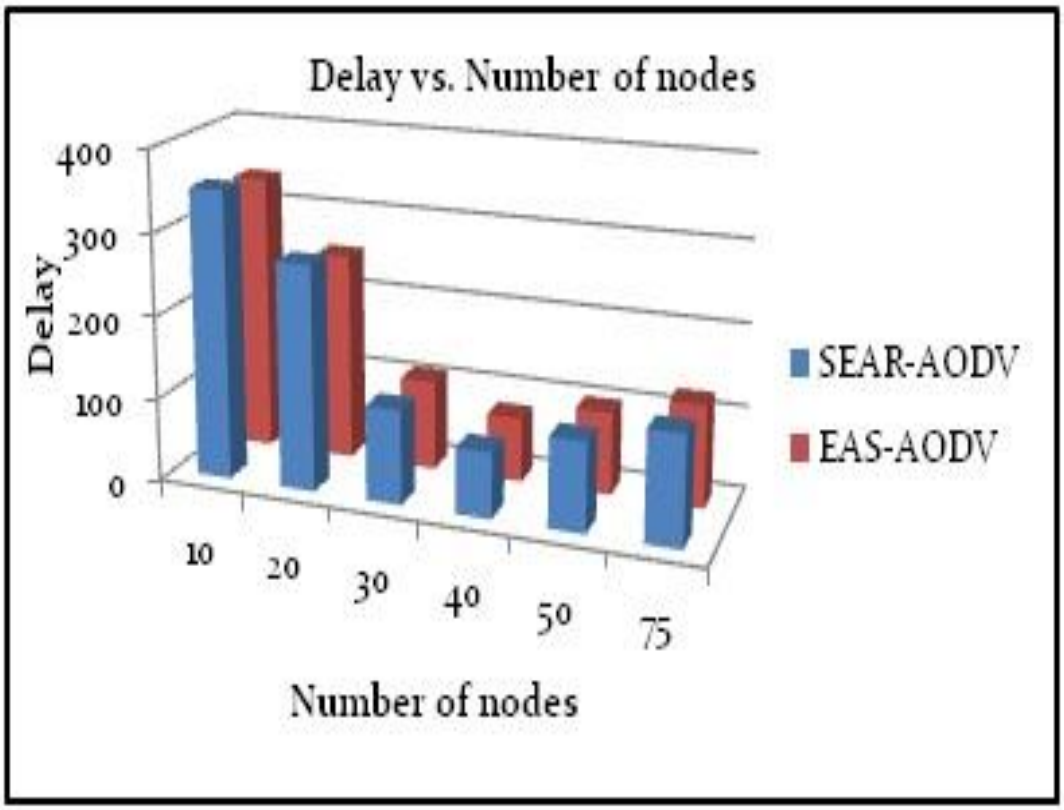


Graph 3: Energy Consumption

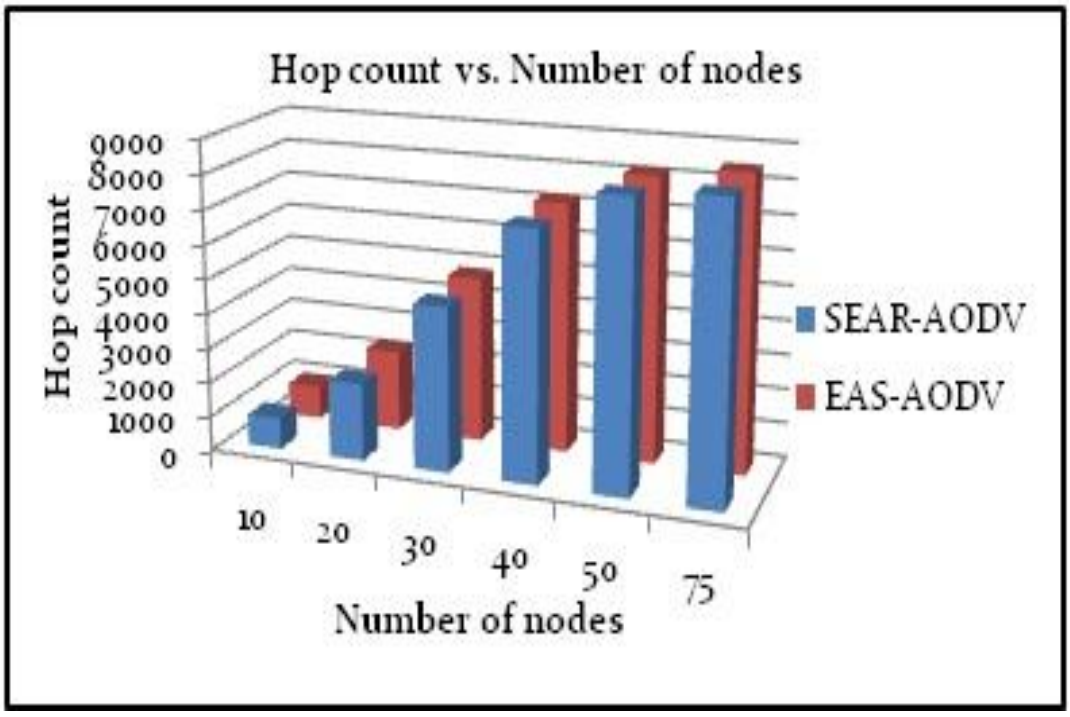
| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 9, Issue 5, May 2022 |

| DOI: 10.15680/IJMRSETM.2022.0905022 |



Graph 4: Delay



Graph 5: Hop Count

Graph 4 and Graph 5 provides comparison of end to end delay and hop count during data transmission.The results show that EAS-AODV performs better in comparison to existing protocol.

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 9, Issue 5, May 2022 |

| DOI: 10.15680/IJMRSETM.2022.0905022 |

V. CONCLUSION AND FUTURE SCOPE

An algorithm has been developed that addresses the challenges of security and energy conservation. Simulation studies clearly depicts that the proposed plan addresses these issues up to a large extent and performs better than traditional SEAR-AODV with the selected parameters. But due to increasing cyber threats in present scenario of MANET deployment, there is immense potential for further modification in reactive routing protocols. Multi-dimensional optimization of the routing protocols in term of energy efficiency,securityand other parameters is yet to be achieved.The future researchmay be done to make MANET routing more energy efficient and authenticated mobile communication mean for data transfer in emerging application areas of MANET.

REFERENCES

[1] A. Dorri et al., "Security Challenges in Mobile Ad Hoc Networks: A Survey", International Journal of Computer Science and Engineering Survey, (2015), 6(1), pp. 15-29.

[2] S. Yadav et al., "Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme", Proceedings of 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics, (2017), pp. 1–4.

[3] D. Kamboj et al., "Performance Evaluation of Secure Routing in Ad-hoc Network Environment", Proceedings of 1st International conference on Recent Advances in Information Technology, (2012), pp. 21-26 .

[4] N. Gupta et al., "Performance Evaluation of DSR, AODV and SAODV Routing Protocol in MANETs", International Journal on Future Revolution in Computer Science and Communication Engineering, (2018), 4(3), pp. 151-161.

[5] K. Taneja et al., "EEGRP: Grid Based and Caching Equipped Energy Efficient Routing Protocol for MANET with Restricted Movement", Far East Journal of Electronics and Communications, (2016), 3(1), pp- 185-199.

[6] U. Rashid et al., "Mobility and energy aware routing algorithm for mobile ad-hoc networks", Proceedings of International Conference on Electrical Engineering, (2017), pp. 1–5.

[7] E. Niewiadomska-Szynkiewicz et al., "Secure low energy AODV protocol for wireless sensor networks", Proceedings of 27th International Telecommunication Networks Application Conference ITNAC, (2017), pp. 1–6.

[8] P.S. Raval et al., "Energy Aware Routing Protocol for MANET", International Journal of Engineering Development and Research, (2014), 2(2), pp. 1673–1677.

[9] N. Kamboj et al., "An Enhanced Energy Efficient Secure Routing Protocol for MANET", International Journal of Advanced Science and Technology, (2020), 29(5), pp. 1135–1142.

[10] E. Ahila et al., "Security Based Energy Efficient Routing Protocol for Adhoc Network", Proceedings of International Conference on Control, Instrumentation, Communication and Computational Technologies, (2014), pp. 1522-1526.

[11] K.V. Arya et al., "Power Aware and Secure Routing in Mobile and Ad-Hoc Networks", Proceedings of IEEE 8th International Conference on Industrial and Information Systems, (2013), pp. 477–482.

[12] S.K.Mohapatra et al., "Stability and energy aware reverse AODV routing protocol in MANETS", Proceedings of IEEE 2nd International Conference on Recent Trends in Information Systems, (2015), pp. 526–531.

[13] Phu P.H. et al., "Securing AODV routing protocol in mobile ad-hoc networks", Proceedings of International Working Conference on Active Networks, (2005), pp. 182-187.

[14] N. Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET", IEEE Access, Volume 9, (2021), pp. 120996-121005.

Impact Factor: 7.580

INTERNATIONAL JOURNAL
OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

+91 99405 72462 +91 63819 07438 ijmrsetm@gmail.com

www.ijmrsetm.com