Secure, Energy Efficient and Power Aware Routing Protocols in Ad Hoc Networks - A Survey

[1]B. Sandhya Rani, [2] Kattula Shyamala

[1]Research Scholar, [2] Professor
[1,2] Department of Computer Science, University College of Engineering,
[1,2] Osmania University, Hyderabad, Telangana, India.

***Abstract*—Mobile Ad-hoc Network (MANET) is a collection of nodes that organize themselves without any infrastructure. Nodes in such networks are battery operated. A network in MANETs is formed dynamically, where devices join and leave the network frequently changing network topology. Energy consumption, limited resources, signal fading, security, and routing are the issues in such networks. This paper provides a literature survey on energy-efficient, secure, and power-aware routing protocols in MANET.**

***Index Terms*— Ad hoc networks, Energy Efficient Protocols, Power aware protocols, secure routing protocols.**

I. INTRODUCTION

Nodes in MANET dynamically form a network, configure and maintain themselves without the need of an administrator. Due to their dynamic nature MANETs are used in military, mining operations, maritime communications, disaster recovery, and campus networks [1]. Nodes are free to move in a network and are capable of receiving and forwarding packets to their neighbors. Scalability, dynamic topology, battery operated devices with limited resources are some of the characteristics of MANETS. Nodes in the transmission range communicate directly. However, nodes take multiple hops to reach the destination, if they are not in the transmission range. The packets are transmitted in a store and forward manner from source to destination. As a result of their self-organized feature, these networks are highly feasible for insecure environments leading to vulnerable attacks. The primary focus of this paper is to present the literature survey of existing work on secure, power-aware, and energy-efficient protocols. Section II presents Literature Survey, and Section III presents Conclusion.

II. LITERATURE SURVEY

Secure Routing Protocols

A survey on network layer attacks and their countermeasures has been proposed in [2] -[3]. A defense mechanism for AODV is presented in [4] to overcome black hole attacks. Data Routing Information (DRI) table and cross-checking phase are added to the existing AODV protocol. DRI table maintains additional details about the packets that have been routed from and through the node as shown in Table I. If the "From" bit field of the DRI table is 1, it means packets are sent from the node and if it is 0, it means the node has not sent the packets. Similarly, if the "Through" field is 1, it means packets are sent through the node otherwise it means packets are not sent through the node. In cross-checking phase, the trustworthiness of a node is verified. If a node is trustworthy, packets are routed through the node otherwise it is identified as a misbehaving node and the routing tables are updated accordingly. NS2 is used for simulation. In the 1000 m X 1000 m area 30 nodes are randomly placed using a random waypoint mobility model and the simulation is run for 1000 sec. Constant Bit Rate (CBR) is used for traffic generation, packet size is considered as 512 bytes and the simulation is run in the presence of 2 malicious nodes. Results show that the Packet Delivery Ratio (PDR) of the proposed protocol is increased by 17% compared to the AODV protocol in the presence of a black hole attack.

TABLE I. DRI Table

Node No.	From	Through
3	0	1
2	1	0

SRD-AODV [5] is proposed to detect black hole attacks. Sender and receiver compare seq_num in RREQ and RREP messages against a predefined threshold value. Three different thresholds values have been defined for small, medium, and large environments. If the seq_num in RREQ or RREP is greater than the predefined threshold, nodes are identified as malicious nodes. Simulation is carried out in the NS2 simulator by increasing nodes from 50 to 200 in 1000 m * 1000 m area. CBR traffic is used to generate packets of 64 bytes each. PDR of SRD-AODV is improved up to 97% for a small environment, 97% for a medium environment, and 97% for large environments compared to standard AODV protocol.

Jain, Sakshi in [6] have proposed a mechanism to detect malicious nodes by deploying a special node called as Black Hole (BH) node, which periodically broadcasts RREQ packets with a randomly generated destination address. Only malicious nodes respond by sending a reply message, as they don't refer to their routing tables. BH node maintains a list of all such nodes and marks them as malicious nodes. Block message is generated and is broadcasted in the network. All other nodes after receiving block messages,

identify malicious nodes and stop communicating with them. The simulation environment is set up with 10-50 legitimate nodes and 1 malicious node scattered in 800 m * 800 m area with 250 m of transmission range and 5 m/s mobility using NS2. PDR is increased by 112% compared to the AODV protocol.

Trust-based mechanisms are proposed in [7, 8] to identify black hole attacks. Trust value for each node is computed as a ratio of the number_of_packets_dropped to the number_of_packets_forwarded. Each node secretly listens to its neighbors to check if they are forwarding the packets to their neighbors by buffering them. If a node is unable to receive the same packet from its neighbor, it is assumed to be dropped. A node with a trust value less than the threshold is marked as a malicious node.

To address tunneling attacks SDSR protocol is proposed in [9]. It is based on DSR protocol, which uses a broadcast authentication mechanism to provide security. In NS2, with 50 nodes in 1500 m * 300 m area, 2Mb/s channel capacity, and 512 bytes of packet size simulation is carried out. An improvement in PDR and average latency is achieved, compared to DSR and Ariadne. Due to the efficient broadcast authentication mechanism lock synchronization in SDSR is not required.

In [10] authors proposed an algorithm that uses Digital Signature and One Way hashing technique to provide security. Clusters are formed with 4-5 nodes and Cluster Head is elected among them. Cluster nodes before communicating with each other have to authenticate themselves with the CH. If a malicious node tries to communicate with other nodes, access is denied because the malicious node is not authenticated by the CH. The digital signature is used for authentication, one- way hashing is used for communication between cluster nodes.

Fuzzy-based secured routing protocol FBeeAdhoc protocol is proposed in [11]. Source generates a route request message and appends source id, destination id, and list of trusted nodes. After forwarding the packet, the node enters into promiscuous mode and computes the Trust Value (TV) of the neighboring node. The intermediate node upon receiving the route request verifies that the message it has received is not modified by comparing the route with the list of trusted nodes. Destination node upon receiving the route request message computes the Route-Trust value and selects a node with the best Route-Trust value if multiple routes are available. Destination node unicasts an RREP message along the path from which it has received RREQ messages. The source node uses a digital signature to authenticate the message and the intermediate node verifies the integrity of the received message. Simulation is carried out in MATLAB with 10-20 nodes and packet size is considered as 512 bytes. Results show that the PDR, End to End Delay (EED), and transmission efficiency of FBeeAdhoc are improved compared to the AODV protocol. But, the PDR of FBeeAdhoc is the same, EED is more and the transmission efficiency is high compared to BeeAdhoc protocol.

Grade Trust (GT) routing protocol is proposed in [12]. The protocol computes GT as a ratio of numbers_of_packets_received to the number_of_packets_transmitted. Based on the trust value the nodes are classified into three categories; Trusted Friends (tf) grade 3, Friends (f) grade 2, and Possible Friends (pf) grade 3. During a route discovery process, the source node selects a node from the tf group. If there is no neighbor from the tf group then a node from f group is selected to forward packets. Trust compromised metric is calculated to push a malicious node to the lower level quickly so that the node becomes unreliable. If a node is identified as malicious, then its trust compromise value is computed as total nodes in the f list plus four times the number of nodes in the pf list. Simulation is carried out in NS2 and the results show that the protocol outperforms AODV and Fish Eye Routing protocol in terms of PDR, EED, and Trust Compromise.

A fuzzy rule-based secure routing algorithm is proposed in [13], which uses the TV of a node as a metric to evaluate IF Then-based Rules. Eleven rules are formulated to decide the level of encryption required to provide security. If the TV lies between 0-1 the node is considered as unreliable, 2-4 marginally reliable, 5-8 reliable and 9-10 extremely reliable. A node labeled as unreliable drops the packets. Marginally reliable, reliable, and extremely reliable nodes require high, medium, and low encryption. The protocol has achieved a high level of security compared to classic MANET routing protocols.

BP-AODV protocol proposed in [14] to secure against cooperative black hole attack during route discovery and forwarding phase in SAODV protocol. The protocol uses a challenge response-confirm pattern to identify trusted routes. Source and Destination nodes exchange challenges and responses as part of route discovery. Genuine nodes send the same response value while the malicious nodes send a different response value. Malicious nodes start their confirmation phase quickly while the genuine nodes wait for the confirmation phase to start. In the confirmation phase, the destination reveals the secret value used for computing response value to all the nodes, and the nodes that received wrong response values from malicious nodes identify them and inform the same to the destination node. Later, destination node removes malicious nodes entries from the routing table. The results are compared with AODV, SAODV, and PCBHA protocols and results show that the BP-AODV protocol perform best in identifying black hole attack.

Robinson and Y. Harold in [15] have proposed a multipart trust-based public key management technique to reduce security vulnerabilities; where a forwarding node has to prove its trustworthiness to its predecessor and vice versa and uses public-key cryptography to send data.

Energy Efficient Routing Protocols

Shreyas S Vidyarthi and Vijayalakshmi in [16] proposed the EAODV protocol for Multi-Rover Systems. In addition to the Routing table, Distance Vector Table (DVT) and Path Memory Tables (PMT) are maintained to record the direction (sector number) of the neighboring nodes along with the distance of nodes from the source. PMT stores information about the number of nodes per sector. The Ping messages are broadcasted by nodes periodically to track their respective neighbors, distance, and their direction in the DVT. Due to the symmetry of the antenna model, table updation is not required for each but will occur in pairs. The RREQ messages are sent from segment to segment using the directional information from the DVT. Once the route is established, data is transmitted in a direction that leads to the destination, making the system energy efficient. In E-AODV protocol when a node is about to fail, the source starts buffering the packets and finds an alternate node (next node to the failed node), and continues its transmission. Results were tested by varying the number of nodes depending upon the density parameter with a packet size of 5

KB and ensuring the communication density was 50% of the total number of nodes. Up to 28% and 36% of improvement is achieved in PDR and EED compared to the AODV protocol.

To enhance average throughput and PDR, the E-DYMO protocol is proposed in [17]. Network traffic and residual energy of path are used to compute routing metrics and a path with the highest ratio is selected to route the packets. Average throughput and PDR are increased by 154% and 153% compared to DYMO protocols [18] with 3 Mbps of data rate, 1000 bytes of packet for 30 nodes randomly distributed in 1000 m X 1000 m area in NS2.

Kaur and Kanwaljeet have proposed a protocol in [19] to construct a secure and energy efficient cluster in MANETs. Mobility, energy and signal strength of neighboring node is used to calculate weightage of a node. A node with high weightage is considered as a Cluster Head(CH) to process the requests. Performance of the protocol is evaluated against Weighted Clustering Algorithm (WCA) using NS2 simulator with 32 nodes in an area of 1200 m X 700 m for 100 sec. Network lifetime, delay, throughput and less energy consumption is observed compared to WCA.

Wei Liu and Chi Zhang in [20] classified nodes as P-nodes (Energy reservoirs) and B-nodes (normal nodes). Residual energy and traffic at the nodes are used as metrics to route the packets. P-nodes are used for packet transmission to conserve energy. To evaluate the performance of DELAR, in an area of 1500 m X 300 m 50 nodes are randomly placed with a transmission rate of 2 Mbps. Packets size is taken as 512 bytes in OPNET modeler. Initial energy of B-nodes is 3kJ, TX power and RX power are 1560mW and 930 mW are considered. Simulation is carried out for 900 secs. Results show that 50% of average energy consumption is reduced in presence of 6 p-nodes.

Jing Zuo and Chen Dong in [21] has presented a literature review on cross layer aided energy-efficient routing protocols. Cross layer design deals with designing operations across physical layer, data link layer and network layer and work with them to reduce energy consumption of routing packets.

Saloua Chettibi and Salim Chikhi in [22] have proposed a protocol in which each node uses dynamic residual battery level value and drain rate as input to Fuzzy Logic System (FLS) to decide the probability of forwarding the RREQ packets. An improvement in PDR and energy efficiency is observed in dynamic version compared to the dynamic FLS.

Authors in [23] have proposed Linear Automata based energy efficient routing protocol. Initially stability measurement model is constructed and later effective energy ratio function is defined. Each node is assigned a value based on the ratio and this value is used as an iteration parameter for the linear automata. Simulation is carried out in NS3 and the results are compared with ACSRA, ANNQARA, LASEERA and AODV protocols. The results show an improvement in terms of PDR, EED, survival time, energy consumption, and energy balance compared to other protocols.

IE2R protocol is proposed [24]. The protocol is based on entropy and Preference Ranking organization method and also uses Intuitionistic Fuzzy Soft Set (IFSS), an intelligent method to identify an efficient route. Results are show that the protocol out performs EASRP, RECI and EN-AODV protocols in terms of residual energy, QOS support, network life time, delay, PDR, throughput, packet loss, scalability, communication overhead etc.

Authors in [25] have proposed an analysis of energy efficient routing protocols. Christy and Kowsigan have proposed an ant colony optimization protocol in [26]. The protocol considers residual energy, number of packets and dynamic topology and uses ant colony optimization technique for selecting the next hop to forward packets. The results are tested using the ns2 simulator and are compared against EER-LEM and EELAM protocols. The results show an improvement in terms of PDR, EED, Network lifetime, and energy depletion time.

Energy Efficient and Secure Routing Protocols

In [27] network is divided into groups based on energy levels and encryption is performed on group signature with a secret key. Simulation is carried out in NS2 with 20 to 100 legitimate nodes, 2 malicious nodes and 250 m of transmission range, and 512 bytes of packet size. In PPSEER delay is 83% less, PDR is 29% higher, packet drop ratio is 94% less and the energy consumption is 5% less compared to PRISM protocol [28].

To provide security against route hijacking and jamming a Markov chain model is proposed in [29]. The energy consumption value of the forwarding packet is used to determine the optimal routing path. Sender then selects a path stochastically among multiple paths to route packets. Simulation results show that the throughput is increased and the delay is reduced compared to AODV.

To combat against RREQ flooding attack EESM-AODV protocol proposed in [30] identifies multiple paths. The destination node sends RREP packets along the paths, from which it has received RREQ packets. Sender upon receiving all RREPs sorts them using hop count and uses the best three paths among them. In case of a route failure, the source node selects the next best path for transmission. The average residual energy of participating node is increased by 5% with 20 nodes spread in 1100 m X 1100 m area with 250 m of transmission range using NS2 simulator.

Energy-Efficient Secure Routing Protocol (EESPR) is proposed in [31] to provide the link and message security. EESPR uses SOLSR protocol and uses a public key, private key, and certificate to obtain group key. In this protocol, it is assumed that the nodes form a group and run the SOLSR protocol to identify a secure link. Power status information of each is maintained in the routing tables. Nodes with high residual energy are selected as MultiPoint Relays (MPR) and are allowed to forward packets. A group key is generated by an authorized node and is distributed in the group. If a node tries to share the group key with other non-group members, a trigger is generated and the node is identified as a malicious node and is removed from the group. The process is repeated until the message is forwarded to the destination. Simulation results are compared with Source Anonymous Message Authentication (SAMAS) protocol. Results show that the PDR, EED, packet drop ratio, and residual energy of the EESPR protocol are improved compared to the SAMAS protocol.

To address the Denial of Service attack a Cluster-Based Energy Efficient Secure Routing Algorithm (CBEESR) is proposed in [32]. The Trust score (TS1) of the nodes is computed twice. In the first round, TS1 is computed as the ratio of the number_of_

acknowledgments_sent to the number_of_packets_received from the neighbors. TS2 is computed as the ratio of the number of packets dropped to the total number of packets and finally, the average of TS1 and TS2 is taken and the scores are compared with the threshold. If the average is greater than the threshold, the node is considered genuine; else it is considered as a malicious node and is intimated to the rest of the nodes in the cluster. The results are compared with AdHoc On-demand Trusted-path Distance Vector (AOTDV) protocols. The results show that CBSEER outperforms AOTDV in terms of average Trust Score, PDR, throughput, and energy consumption.

Multi-Objective Ant Lion Optimized Based Energy Efficient and Secure Routing OLSR Protocol is proposed in [33]. Source node after identifying the possible routes uses delay and degree of interest as a parameter to choose a node as a multi-point relay to transmit packets. The protocol also uses vulnerability, suspicious factor, and reputation factor, contingency of threat parameters to compute fitness function to identify a secure route. Results are compared with standard OLSR and EMOLSR protocols. Results show that the packet loss is improved by 15.25% and 20.63% and the throughput is improved by 26.54% and 20.59% compared to OLSR and EMOLSR protocols.

Power Aware Routing Protocols

A survey on stability-based and power-aware routing protocols is proposed in [34]. Chen and Ching-wen in [35] have proposed a protocol in which desired amount of data to be transmitted, intermediate sender's remaining power, and current minimal predicted remaining power of intermediate nodes are added to the RREQ packet. Upon receiving RREQ packet, the intermediate node computes the power consumption of source node and maintains the details of the precedent node that has maximal power remaining after data transmission and forwards the packet. The destination node upon receiving all RREQs sends RREP to the source along the optimal path. Simulation is carried out for 400s within 500X500m area with 110 nodes and 2.25 m/sec speed. The average lifetime of the route is increased by 25% and 65%; throughput is increased by 25% and 30%. Compared to MTPR and MMBCR protocols. The ratio of dead nodes is decreased by 80% and 50% compared to MTPR and MMBCR.

The efficient Power-Aware Routing protocol in [36] computes power consumption for each path and a path with the lowest power consumption is chosen to route the packets. In a 2000 m x 2000 m area 120 nodes moving at a speed ranging from 0 to 10 m/s are set up in the NS2 simulator, the performance of network lifetime is increased by 85% compared to MTPR and DSR protocols.

Residual power and number of hops are used to compute cost function (C) in [37]. The sender computes C for each available path and chooses a path with the highest value of C to transmit packets as the best path and the next highest C value as the next best path and so on. In an area of 1000 m X 1000 m with 30 nodes and a packet size of 512 bytes the simulation are run for 100s using NS2. Throughput is increased by 16% and 75%, EED is improved from 54% to 23% over Stable Path Routing Protocol and Modified-AODV protocols respectively.

Deepika and Sanjay Kumar in [38] have proposed a power-aware routing protocol that runs Intrusion Detection System (IDS) on a node with high residual energy. IDS is carried out near an accused node by promiscuously listening to the forwarding nature of a node. If PDR is more than the predefined ratio, the node is marked as a malicious node and all the entries in the routing table through the malicious node are dropped and a new route discovery is initiated. Results are tested in NS2 and the results show an improvement in PDR and energy consumption of the nodes.

III. Conclusion

Dynamic topology and open medium in MANETs lead to security attacks and energy depletion of nodes. This paper categorizes and summarizes the technical work published by various authors in providing security, energy-efficient, and power-aware routing protocols in MANETs.

IV. Acknowledgment

This research work is carried out in the Department of Computer Science and Engineering, University College of Engineering, Osmania University, Hyderabad, Telangana State, India and is funded by DST SERB.

References

[1] Hongmei Deng, Wei Li, and Dharma P Agrawal, "Routing security in wireless ad hoc networks", In IEEE Communications Magazine, vol. 40, pp. 70-75, 2002.

[2] Bing Wu, Jianmin Chen, Jie Wu, and Mihaela Cardei "A Survey of Attacks and Countermeasures in Mobile Ad hoc Networks", In Wireless Network Security, Springer, pp. 130-135, 2007.

[3] GS Mamatha and Dr SC Sharma,"Network Layer Attacks and Defense Mechanisms in MANETs -A Survey", In International Journal of Computer Applications, vol. 9, 2010.

[4] Sen, Jaydip, Sripad Koilakonda, and Arijit Ukil. "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", In Second International Conference on Intelligent Systems, Modeling and Simulation (ISMS), pp. 338-343, 2011.

[5] Tan, Seryvuth, and Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs.", In 10th IEEE International Conference on High Performance on Embedded and Ubiquitous Computing, p. 1159-1164, 2013.

[6] Jain, Sakshi, and Ajay Khuteta, "Detecting and Overcoming Black Hole Attack in Mobile Adhoc Network", In International Conference on Green Computing and Internet of Things, pp. 225-229, 2015.

[7] Fidel Thachil and KC Shet, ”A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET”, In IEEE International Conference on Computing Sciences, pp. 281-285, 2012.

[8] M Anugraha and SH Krishnaveni, “Recent Survey on Efficient Trust Management in Mobile Ad Hoc Networks”, In IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), pp. 1–4, 2016.

[9] L.Vijayanand, R.K Negesh, ”SDSR: A Secure On-Demand Routing Protocols for MANETs”, In IET International Conference on Sustainable Energy and Intelligent Systems, pp. 1-5, 2012.

[10] Md Monzur Morshed and Md Rafiqul Islam, ”CBSRP: Cluster Based Secure Routing Protocol”, In IEEE International Advance Computing Conference (IACC), pp. 571-576, 2013.

[11] Rafsanjani, Marjan Kuchaki, and Hamideh Fatemidokht. ”FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs.” In AEU-International Journal of Electronics and Communications, vol. 69(11), pp. 1613-1621, 2015.

[12] Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. ”GradeTrust: A secure trust based routing protocol forMANETs.”, In IEEE International Conference on International Telecommunication Networks and Applications Conference (ITNAC), 2015.

[13] Garg, Mukesh Kumar, Neeta Singh, and Poonam Verma. ”Fuzzy rule based approach for design and analysis of a Trust-based Secure Routing Protocol for MANETs.” In Procedia computer science, Elsevier, pp.653- 658, 2018.

[14] El-Semary, Aly M., and Hossam Diab. ”BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map”, In IEEE Access, pp. 95197-95211, 2019.

[15] Robinson, Y. Harold, and E. Golden Julie. ”MTPKM: Multipart Trust Based Public Key Management Technique to Reduce Security Vulnerability in Mobile Ad-hoc Networks.” In Wireless Personal Communications International Journal, vol. 109, issue 2, pp.739-760, 2019.

[16] Vidyarthi, Shreyas S., et al. ”Energy Efficient Enhanced-AODV Protocol for Multi-Rover Systems”,In 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, 2011.

[17] Aravind, Maya C, C. P. Sangeetha, and C. D. Suriyakala, ”Enhanced Dynamic MANET On-demand (En-DYMO) Routing Protocol for Mobile Ad Hoc Networks”, In IEEE Conference on Global Conference on Communication Technologies, pp. 544-549, 2015.

[18] Manchikalapudi, Varun, and Perla Ravi Theja. ”Routing in dynamic mobile adhoc networks.”, In International Journal of Advance Research in Computer Science and Management Studies, vol. 1.7, pp. 274-280, 2013.

[19] Kaur, Kanwaljeet, and Jaspinder Singh, “Weightage based Secure Energy Efficient Clustering algorithm in MANET”, In IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1006-1012, 2015.

[20] Wei Liu, Chi Zhang, Guoliang Yao, and Yuguang Fang, ”DELAR: A Device-Energy-Load Aware Relaying Framework for Heterogeneous Mobile Ad Hoc Networks”, In IEEE journal on selected areas in communications, vol. 29, 2011.

[21] Zuo, Jing, et al. ”Cross-Layer Aided Energy-Efficient Routing Design for Ad hoc Networks.”, In IEEE Communications Surveys & Tutorials, vol. 17, issue 3, pp. 1214-1238, 2015.

[22] Chettibi, Saloua, and Salim Chikhi. ”Dynamic Fuzzy Logic and Reinforcement Learning for Adaptive Energy Efficient Routing in Mobile Ad-hoc Networks”, Applied Soft Computing- Elsevier, vol.38, pp. 321- 328, 2016.

[23] Hao, Sheng, Huyin Zhang, and Mengkai Song. ”A stable and energy efficient routing algorithm based on learning automata theory for MANET.”, Journal of Communications and Information Networks, vol. 3.2, pp.43-57, 2018.

[24] Das, Santosh Kumar, and Sachin Tripathi. ”Intelligent energy-aware efficient routing for MANET.”, In Journal of Mobile Communication, Computation and Information, Springer ,Vol 24.4, pp. 1139-1159, 2018.

[25] Das, Sumanta, and Sarit Pal. ”Analysis of Energy-Efficient Routing Protocols in Mobile Ad Hoc Network.”, In Advances in Computer, Communication and Control. Springer, Singapore, pp.285-295, 2019.

[26] Malar, A. Christy Jeba, et al. ”Multi constraints applied energy efficient routing technique based on ant colony optimization used for disaster resilient location detection in mobile ad-hoc network.”, In Journal of Ambient Intelligence and Humanized Computing, pp. 1-11, 2020.

[27] E Ahila Devi and K Chitra. “Security Based Energy Efficient Routing Protocol for Ad Hoc Network”, In IEEE International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), pp. 1522–1526, 2014.

[28] Karim El Defrawy and Gene Tsudik. “Privacy Preserving Location Based On-Demand Routing in MANETs”, In IEEE Journal on Selected Areas In Communications, vol. 29. 10, pp. 1926-1934, 2011.

[29] Sajal Sarkar and Raja Datta “A Secure and Energy Efficient Stochastic Routing Protocol for Wireless Mobile Ad-Hoc Networks”, In IEEE Twentieth National Conference on Communications (NCC), pp. 1–6, 2014.

[30] Harishabha Raj Jain and Sanjay Kumar Sharma, ”Improved Energy Efficient Secure Multipath AODV Routing Protocol for MANET”, In IEEE International Conference on Advances in Engineering and Technology Research (ICAETR), pp. 1–9, 2014.

[31] Singh, Tejpreet, Jaswinder Singh, and Sandeep, ”Energy efficient secured routing protocol for MANETs”, In Journal of Mobile Communication, Computation and Information, Springer, pp. 1001- 1009, 2017.

[32] Muthurajkumar, Sannasy, et al. ”An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs.”, In Journal of Wireless Personal Communications, pp. 1753-1769, 2017.

[33] Kanagasundaram, Hamela, and Kathirvel Ayyaswamy. ”Multi objective ALO based energy efficient and secure routing OLSR protocol in MANET.”, In International Journal of Intelligent Engineering and Systems, vol 12.1, pp. 74-83, 2019.

[34] Natarajan Meghanathan and Leslie C Milton, “A Simulation Based Performance Comparison Study of Stability Based Routing, Power Aware Routing and Load Balancing On-Demand Routing Protocols for Mobile Ad Hoc Networks”, In IEEE Sixth International Conference on Wireless On-Demand Network Systems and Services, pp. 3–10, 2009.

[35] Ching-wen Chen, Keng-hao Lai, and Ching-lung Chan, “Power-Aware Routing Protocols with Link-Bandwidth and Path Remaining Power in Mobile Ad hoc Networks”, In 14th IEEE International Conference on Networks, vol. 6, pp. 1–6, 2006.

[36] KS Haseena, Sheena Anees, and Neela Madheswari, ”Power Optimization using EPAR Protocol in MANET”, In International Journal of Innovative Science, Engineering & Technology, vol. 1, 2014.

[37] Salwa Othmen, Aymen Belghith, Faouzi Zarai, Mohammad S Obaidat, and Lotfi Kamoun, “ Power and Delay-Aware Multi-Path Routing Protocol for Ad Hoc Networks”, In International Conference on Computer, Information and Telecommunication Systems (CITS), pp. 1–6, 2014.

[38] Kukreja, Deepika, Sanjay Kumar Dhurandher, and B V Ramana Reddy. ” Power Aware Malicious Nodes Detection for Securing MANETs Against Packet Forwarding Misbehavior Attack”, In Journal of Ambient Intelligence and Humanized Computing, vol. 9(4), pp. 941- 956, 2018.