A COMPREHENSIVE ANALYSIS ON SECURITY AND MOBILITY AWARE ROUTE PATH SELECTION IN MANET ENVIRONMENT

N. Naveen[1,*] and J. Nirmaladevi[2]
[1]Department of Information Technology, Excel Engineering College, Komarapalayam, Namakkal- 637 303, Tamil Nadu, India.
[2]Department of Computer Science and Engineering,Bannari Amman Institute of Technology,Sathyamangalam– 638 401, Tamil Nadu, India.
[*]Corresponding Author. Email: nanaveen@gmail.com

Abstract

Due to a lack of infrastructure support in an environment of scalable mobile ad hoc networks (MANETs), secure data dissemination is complex. Most prior routing methods for MANETs have either ignored security or addressed a particular security aspect without improving routing performance. By studying the packet forwarding characteristics of surrounding nodes, due to the lack for various type of attacks in MANET like Blackhole, wormhole, sinkhole and rushing attacks. In this survey, we collected 36 papers to analyze the secure routing in MANETs.The causes of high mobility in terms of high traffic and malicious nodes for attacking area. MANETs require detecting misbehaving links and narcissistic nodes to prevent packet-dropping attacks. The quality of service (QoS), routing efficiency, dependability, delay per packet, packet delivery ratio, and control overheads are all examined. Here, we outline the most cutting-edge QoS-based, fault-tolerant, scalable, and reliable hybrid routing algorithms and techniques.

Keywords: Quality of Service, MANETs, Attacks, Secure Routing, Path Selection

DOI Number: 10.48047/nq.2022.20.22.NQ10116 **NeuroQuantology 2022; 20(22):1383-1392**

1. INTRODUCTION

In general, mobile ad hoc networks consist of a large number of wirelessly communicating nodes [1-5]. The MANET network lacks centralized management and specific infrastructure, and its nodes can move freely in the environment [6-8]. Wireless nodes that serve as routers send information from one site to the destination. In addition, MANET governs paths that might facilitate improved communication between nodes [9-13]. Due to the development of intelligent gadgets, transmission advancements, and MANET's adaptability, it is employed for various purposes [14-22]. The MANET is then organized into clusters that serve as clusterheads, while the other communication nodes are called clustermembers. In addition, the clustering approach is used to divide the whole network into clusters, which are interconnected substructures [23-28]

Quality of service support is undoubtedly one of the most complex concerns associated with MANETs. Network lifespan and average end-to-end latency are the crucial quality of service factors for a MANET. Regarding network longevity, keep in mind that the majority of MANET nodes are battery-

powered. Regarding end-to-delay, several applications (such as real-time) include time-sensitive data. A routing technique that computes routing tables based on energy or delay measurements may enhance the abovementioned two metrics[29-31]

MANET stands out because of its malleability, low cost, and ease of setup. The highly dynamic routing algorithms are defenceless because they lack a clear front line. That leaves the MANET vulnerable to disruption from malicious actors. Although several MANET security protocols have been created in recent years to address specific risks, no such system has yet been shown to be completely bulletproof[32]

Mobile ad hoc networks with fault tolerance may continue to deliver data even if links and nodes fail due to interference or internal difficulties [33. The most typical reasons for downtime in MANETs are problems with the battery, the transceiver, or the process. Ad hoc network performance would suffer due to these weaknesses, resulting in increased packet loss, slow data transfer rates, and perhaps network disconnections [34]. Because these defects disturb typical network activity, network performance suffers [35]. Mobile ad hoc networks must be built to detect defective nodes, try to fix them, and then broadcast the data packet to its final destination or collection of destinations [36]. While a network is flawed, its capacity to tolerate failure increases and the network becomes fault-free. MANET research dedicated to studying and implementing robust routing protocols has increased.

2 DIFFERENT ATTACKS IN MANETS

2.1 Blackhole Attack

DoS attack and a blackhole attack are both separate attack styles. The intruder discovers the fastest route to hit the destination. The intruder attacks the larger part of the road, because of his awareness of the best direction. Whenever the source node gets the RREQ response, it sends a wrong RREP message automatically. The source code is the first to obtain RREP in front of other RREPs from the malicious node. The malicious node would not transmit data packets to the target. It often loses one of the packets you sent to accomplish this notorious act. Node 1 is the source node, node 4 is the destination node; node 3 is the operation node-negative. If a source (a machine that wants to transfer data from it to a pair) wants to establish a path to its target, it sends an RREQ message to the neighbouring nodes. So, node 2, 5, and 6 are sent with the tie-breaker message: Because three are a malicious unit, it sends an RREP reaction back to the first node with a large sequence number suggesting a negative reaction. You will place packets on the best route if you believe that RREPs are the best route and intend not to use any other route. However, node 3 loses all data packets rather than sending them to the expected destination.

2.2 Rushing Attack

Suppose the weakened node receives a demand bundle from the source node during hurricane assaults. In that case, the parcel can rapidly flow over the network until separate nodes, which also obtain a similar demand set. For, e.g., the "F" node to the rushed attack node, where "An" and "D" allude to the source and destination nodes. The onset attack on the agreed node "4" easily moves on the course demand messages to ensure that the RREQ response itself emerges earlier than those from different nodes. This outcome happens while the "D" node is nearby. They dispose of inquiries. "S" thereby struggles to pursue a good path or secure course in the face of such attacks without the assistance of the attacker.

2.3 Wormhole Attack

In a wormhole attack, the malicious node gets the knowledge packet and at some stage in the network tunnels it to another malicious node. The tunnel occurs between two malicious nodes, and this is referred to as a wormhole. For example, The 'X' and 'Y' nodes are malicious network tunnel nodes. As the

originating node "S9" starts to locate the path to the destination node "S2" with the RREQ code, "S4" and "S5" are the closest to the neighbour node to obtain the message from the originating node to their respective neighbours "S6" and "S8." When the "S8" node gets the RREQ, it automatically shares the node with "S9" and then begins to send the RREQ to the neighbouring node through the RREQ to the goal node "S9"

2.4 Gray hole Attack

The malicious node argues that its packets are ideal for the node in this kind of attack. It is comparable to a black hole attack but lowers the data packet for a specific node.

2.5 Sinkhole Attack

A compromised node or node advertises inaccurate routing details to generate itself as a particular node and collect the total network traffic in Sinkhole Attack. After the total network traffic, such as improvements to a data packet, it modifies the hidden knowledge or making the network more complex. A malicious node tries to secure all adjacent nodes.

3. SURVEY ON DIFFERENT ROUTING METHODS IN MANET

Ahmed et al., 2017[2] To single out malicious nodes, the authors of A Flooding Factor-based Framework for Trust Management (F3TM) use an estimated trust value. Conclusions drawn from the framework's design, development, and evaluation are as follows: It was found that F3TM's scalability and security made it an ideal solution for distributing data.

Dhananjayan, G., & Subbiah, J. (2016)[4]. The method enhances the standard Ad hoc On-Demand Distance Vector (AODV) routing protocol by imposing limits on connection establishment stability, energy management, and mobility-based prediction of dangerous behaviour. In reputation-based routing systems, trust assurance was derived from peers, resulting indecreased PDR and throughput as the percentage of malicious nodes rose. To address this issue, these authors developed the T2AR, which uses direct and indirect observation strategies to collect log data from neighbouring nodes.

F. Wu et al. (2021)[6]The authors created the T2AR protocol to improve secure data transmission speed and node trust in mobile ad hoc networks (MANETs). The approach adds connection setup stability and energy and mobility-based hazardous behaviour prediction constraints to the current Ad-hoc On-Demand Distance Vector (AODV) routing protocol. In reputation-based routing systems, the assurance of trust was gained from peers, causing a drop in PDR and throughput as the fraction of malicious nodes increased. The T2AR was created to improve on this by collecting log data from neighbouring nodes using direct and indirect observation tactics.

Gulati, M. K., & Kumar, K. (2012).[8]An analysis of the fundamental ideas and challenges of quality of service routing in MANETs. Multipath, cross-layer, stable, load-balancing, and power-efficient were categories used to categorize the protocols. These protocols were chosen to show the range of approaches to QoS routing in MANETs and include the bulk of the field's most important recent developments. Every protocol's functionality and essential parts are briefly outlined.

Kukreja, D. et al. (2015)[10] Energy Efficient Secure Dynamic Source Routing (EESDSR) ensures the most reliable, secure, and quickest trustworthy method possible by selecting a route in which the trust value of each node is such that all nodes are benign. The route has a greater average trust than any other cached source route. Simulations demonstrate that even with malicious nodes present, EESDSR achieves better PDR, lower packet loss rate, and lower average end-to-end latency than DSR.

M. F. Rangkuty et al. (2020)[13] These writers focus on the data plane network LB, which employs the Least Loaded Channel (LLP) approach, which has trouble with flow

distribution on a single busy channel with no other route. As previously observed, the load balancer generates several pathways for the best method and equitably reroutes the detected channels. Mininet's goal was to imitate network topologies.

N. Nosrati and H. S. Shahhoseini (2020)[15]Traffic-balanced selection strategies equally divide network traffic in mesh-based NoCs to reduce congestion. A stair-shaped zone collects congestion data for routing choices. The step-like area delivers accurate and timely congestion statistics by considering local and distant router traffic. The suggested selection function determines the average congestion over the shortest pathways that might carry the packet using the packet's origin and destination locations. These authors examine linear, diagonal, L, and accessible models.

Pathan M et al. (2018)[16] To improve overall system performance and reduce route failures in the highly dynamic environment of MANETs, the trust-based secure quality of service routing scheme (TSQRS) takes into account channel quality, residual link life, and residual energy during the identification of on-demand routes. Using CFR, DFR, and intimacy level in conjunction with trust updates is crucial for keeping malicious nodes out of the routing process.

Rakesh Kumar, S., & Gayathri, N. (2016). [19]Security of network packet transit is discussed. As a method of removing the rogue node from the network, a secure OLSR was suggested (sOLSR). The node's dependability was utilized to choose a safe route. The suggested technique's packet delivery ratio, latency, and routing overhead were compared to the Optimized Link State Routing Protocol (OLSR). sOLSR outperforms OLSR in situations with varied numbers of malicious nodes and mobile speeds, according to experimental data.

S. Mohapatra and M. Siddappa(2017)[21] As route selection may be made unilaterally and any node can join a network for energy efficiency, These authors'security method was best suited for open networks and required the use of secret personal keys. These authors' security method does not employ distributed CA or TA services to avoid the vast volume of communications and computing activities necessary for these administrations.

Sarkar, D.e t al(2017)[23] For MANET, the Enhanced-Ant-AODV routing protocol has been proposed. The performance of the suggested system has been evaluated in addition to Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Enhanced-Ant-DSR. Simulation results show Enhanced-Ant-AODV has a higher packet delivery ratio, throughput, average end-to-end latency, and node percentage.

T. A. Alghamdi and M. E. Woodward (2016)[25] To solve this difficulty, these authors presented Energy Efficient Secured Routing Protocol in which Secure Optimized Link State Routing Protocol is used to choose to route (SOLSR). On-demand for a new route, the route database was inspected for nodes' power states. Then, to decrease energy usage, These authors used a modest amount of messages in the group essential distribution procedure. The group key will be updated frequently to prevent non-authorized nodes and the reuse of the same group key for more than a certain quantity of data.

Thakrar P et al. (2020)[27] Networks have become an integral aspect of wireless networking because oftheir many advantages, such as simplicity of deployment, decentralization, and self-configuration. With a thorough understanding of these networks, the workings, the kinds of protocols, the advantages and uses, and their limits are recognized. There are primarily two types of protocols: reactive and proactive. Based on a comprehensive analysis of the literature review and research gaps of different protocols, the TORA protocol was selected, and its complete study and functionality were observed.

Vatambeti, R et al. (2021)[29],to manage and cluster MANET routes, these experts came up with the innovative Eagle Based Density Clustering (EBDC) method. The Star design, utilized in these authors' MANET nodes, reduces packet loss by centralizing communications in the cluster's hub and is, therefore, the primary emphasis of their method. The proposed method begins with identifying the cluster's epicentre and its associated communication channels. Accordingly, it evaluates the energy consumption of each node and uses that information to identify the route's (link's) failure.

Walker, G. A., &Biradar, R. C. (2017)[30] The researchers began by categorizing hybrid routing methods and introducing the paper's purpose and methodology before evaluating the approach and performance of numerous standard protocols in this arena. Hybrid routing strategies based on topology and services were the primary focus of the study. Network topologies may be broken down into several classes, such as mesh, tree, zone, and multipath protocol.

3.1 SURVEY ON BLACKHOLEMITIGATIONROUTINGINMANET

Siddiquaetal.(2015)Suggested a packet loss algorithm to detect and avoid by creating a discovery of information to classify black hole nodes. This work strengthens the current AODV routing protocol to protect the link between nodes while avoiding black hole attacks.

Poojaetal.(2015)The emergence of Blackhole Network Efficiency Attacks was detected. This paper introduces a modern technique named the Hint-based Probabilistic routing protocol. It is used to track black hole attacks by considering local utility functions. This paper analyzes network behaviour using a three-movement model and chooses the preferred simulation parameters.

EiKhinet al.(2014)Security risks against black hole attacks are studied, which drop all obtained data packets planned for transmission. A simulation-based performance review and an analysis of the black hole attack effect on AODV protocol were investigated.

Mahamuni etal.(2013)Proposed DSR-based routing with a black hole attack detection update. It is split into two phases: pre-path identification and protection of malicious nodes in data transmission. The proposed scheme's core advantage is its flexibility and reliability in complex situations for identifying malicious nodes. This maliciousness knowledge is processed in the nodes.

ShekharTandanetal.(2011)Fix the black hole attack problems. This black hole attack draws packets incorrectly by constructing the wrong direction by providing incorrect details about itself. This paper is intended for the public with prior awareness of network routing protocols and their quantitative measurements.

MangeshGhongeetal.(2012)The problems of black hole intrusion in ad hoc networks were studied. In a black hole attack, the malicious node attempts to say that it is the target node by submitting a bogus route response to the source node that initiated the inquiry. The malicious node will redirect packets and generate network traffic. Simulation findings demonstrate the consequences of the AODV protocol blackhole invasion.

Table 1 survey of Route Path Selection Mechanism for secured MANET Environment

Paper No	Author	Methodology	Advantage	Disadvantage
2	Ahmed et al. (2017)	Factor-based Framework for Trust Management (F3TM)	effective data distribution	The use of energy was extensive.
4	Dhananjayan, G., & Subbiah, J.	a trust-aware ad-hoc routing (T2AR) protocol	reduction in the number of unfounded positive	It used more energy.

	(2016)		results	
6	F. Wu et al. (2021)	a multipath congestion control mechanism, named MPCC	enhance throughput while decreasing transmission time performance	The cache hit ratio was poor
8	Gulati, M. K., & Kumar, K. (2012)	Quality of Service quality of service routing metrics	MRNLM balances the energy in all channels, extending the network lifespan.	The end-to-end latency was somewhat longer.
10	Kukreja, D., et al (2015)	Energy Efficient Secure Dynamic Source Routing (EESDSR)	fewer packet losses	Limitation of preferred neighbours
13	M. F. Rangkuty et al (2020)	Least Loaded Path (LLP) mechanism	helps the load balancer function more quickly	Appropriate for low-density networks
15	N. Nosrati and H. S. Shahhoseini (2020)	traffic-balanced selection mechanism Adaptive Routing Algorithm	increased average delay	a restricted view of the network's condition
16	Pathan, M et al. (2018)	KPIs for Measuring the Quality of Service in Routing	TSQRS can enhance packet delivery consistency and route overhead.	Malicious nodes may connect to the network.
19	Rakesh Kumar, S., & Gayathri, N. (2016).	Optimized Link State Routing Protocol (OLSR)secure-OLSR	Overhead is kept to a minimum.	Few data packets are sent and received
21	S. Mohapatra and M. Siddappa(2017)	Load Balanced Energy Enhanced Clustered Bee Ad Hoc Routing (LBEE)	The speed of the system may be improved by using shorter keys.	A decrease in efficiency
23	Sarkar, D.e t al(2017)	Ad-hoc On-Demand Distance Vector (AODV) protocol with Ant Colony Optimization (ACO)	There will be fewer interruptions in the route and more packets sent per second.	a small number of nodes
25	T. A. Alghamdi and M. E. Woodward (2016)[	Secure Optimized Link State Routing Protocol.	Efficient and delivers messages quickly.	Used a few group key messages
27	Thakrar, P et al. (2020)	Temporarily Ordered Routing Algorithm (TORA)	In the group key, a modest number of messages were utilized.	Since DSR and AODV exceed TORA, they are seldom used.
29	Vatambeti, R et al (2021)	the novel Eagle Based on Density	It made many nodes.	Many nodes require a lot of

		Clustering (EBDC)		energy.
30	Walikar, G. A., &Biradar, R. C. (2017)	hybrid routing mechanisms	more adaptable	Limits on the number of nodes

4 DISCUSSION

The list of candidate routes includes several options for getting from A to B. Our dynamic technique computes the relative congestion on any route between any two specified nodes. Alterations are made to the set of possible routes by exchanging the most heavily overcrowded ones with a new group of less crowded ones. The dynamic solution proposed here differs from the static one in that it dynamically modifies the set regularly based on the value of the Recalculate Path system variable, which was not the case in the original work. Recalculation makes a single change to the set, but it gives you the time or number of connections you need to kick off the dynamic method.

The concepts and issues of quality of service routing in MANETs are thoroughly examined. These protocols were chosen to show off various approaches to QoS routing in MANETs while also touching on recent developments in the field. Each protocol's functioning and significant characteristics are described in detail. Within this subject are several subfields, each with its own set of issues and promise for improving the growth and distribution of MANETs and their particular applications. Some topics include stability, robustness, security, support for heterogeneous MANETs, power consumption, resource availability, location management, inter-layer integration of quality-of-service services, and support for location-aware services. New QoS routing protocols must be created and deployed in MANETs to properly and efficiently address these concerns.

5 CONCLUSION

In this Survey, By analyzing the packet forwarding behaviour of neighbouring nodes and different secure routing with black hole attack detection, and in this investigation classifies the sources of high mobility according to two broad categories: high traffic and malicious nodes. MANETs must identify bad connections and disconnect nodes to stop packet-dropping assaults. Quality of service (QoS), control overheads, packet latency, and packet delivery ratio are also discussed in routing systems QoS. Recent developments in hybrid routing that prioritize user experience, network efficiency, and fault tolerance are highlighted. For further we develop a framework for avoiding the attacks.

6 REFERENCES

1. A.Abada, L. Cui, C. Huang and H. -H. Chen, "A Novel Path Selection and Recovery Mechanism for MANETs P2P File Sharing Applications," 2007 IEEE Wireless Communications and Networking Conference, 2007, pp. 3472-3477, doi: 10.1109/WCNC.2007.637.
2. Ahmed, M. N., Abdullah, A. H., Chizari, H., &Kaiwartya, O. (2017). F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs. Journal of King Saud University - Computer and Information Sciences, 29(3), 269–280. doi:10.1016/j.jksuci.2016.03.004
3. Costagliola, N., López, P. G., Oliviero, F., & Romano, S. P. (2011). Energy- and Delay-Efficient Routing in Mobile Ad Hoc Networks. Mobile Networks and Applications, 17(2), 281–297. doi:10.1007/s11036-011-0335-1
4. Dhananjayan, G., & Subbiah, J. (2016). *T2AR:* trust-aware ad-hoc routing protocol for MANET. *SpringerPlus, 5(1).* doi:10.1186/s40064-016-2667-6
5. Eissa, T., Abdul Razak, S., Khokhar, R. H., & Samian, N. (2011). Trust-Based Routing Mechanism in MANET: Design and

Implementation. Mobile Networks and Applications, 18(5), 666–677. doi:10.1007/s11036-011-0328-0

6. F. Wu, W. Yang, M. Sun, J. Ren and F. Lyu, "Multi-Path Selection and Congestion Control for NDN: An Online Learning Approach," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1977-1989, June 2021, doi: 10.1109/TNSM.2020.3044037.
7. G. Thanigaivel, N. A. Kumar and P. Yogesh, "TRUNCMAN: Trust based routing mechanism using non-cooperative movement in mobile ad-hoc network," 2012 Second International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), 2012, pp. 261-266, doi: 10.1109/DICTAP.2012.6215430.
8. Gulati, M. K., & Kumar, K. (2012). QoS routing protocols for mobile ad hoc networks: a survey. International Journal of Wireless and Mobile Computing, 5(2), 107. doi:10.1504/ijwmc.2012.046783
9. H. -S. Chuang, L. -T. Lee and C. -F. Wu, "A Channel-Aware Path Selection Scheme for Mobile WiMAX Networks," 2013 International Conference on Information Science and Applications (ICISA), 2013, pp. 1-4, doi: 10.1109/ICISA.2013.6579330.
10. Kukreja, D., Dhurandher, S. K., & Reddy, B. V. R. (2015). Enhancing the Security of Dynamic Source Routing Protocol Using Energy Aware and Distributed Trust Mechanism in MANETs. Advances in Intelligent Systems and Computing, 83–94. doi:10.1007/978-3-319-11227-5_8
11. Kukreja, D., Dhurandher, S. K., & Reddy, B. V. R. (2017). Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack. Journal of Ambient Intelligence and Humanized Computing, 9(4), 941–956. doi:10.1007/s12652-017-0496-2
12. M. -E. -A. Brahmia, A. Syarif, A. Abouaissa and P. Lorenz, "A combined path selection and admission control scheme for IPTV in IEEE 802.16j MMR networks," 2015 IEEE International Conference on Communications (ICC), 2015, pp. 6803-6808, doi: 10.1109/ICC.2015.7249410.
13. M. F. Rangkuty, R. Muslim, T. Ahmad and M. H. A. Al-Hooti, "Path Selection in Software Defined Network Data Plane using Least Loaded Path," 2020 International Conference on Advanced Computer Science and Information Systems (ICACSIS), 2020, pp. 135-140, doi: 10.1109/ICACSIS51025.2020.9263120.
14. M. Kalyani and S. -H. Park, "Ontology based routing path selection mechanism for underwater Internet of Things," 2021 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia), 2021, pp. 1-5, doi: 10.1109/ICCE-Asia53811.2021.9642009.
15. N. Nosrati and H. S. Shahhoseini, "Regional Selection Mechanism for Traffic-balanced Adaptive Routing Algorithms in Mesh-based NoC Architectures," 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), 2020, pp. 513-518, doi: 10.1109/ICCKE50421.2020.9303650.
16. Pathan, M., Zhu, N., He, J., Zardari, Z., Memon, M., & Hussain, M. (2018). An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. Future Internet, 10(2), 16. doi:10.3390/fi10020016
17. R. Jmal and L. C. Fourati, "An overview of shortest path mechanisms for Metro-Ethernet networks," 2015 2nd World Symposium on Web Applications and Networking (WSWAN), 2015, pp. 1-6, doi: 10.1109/WSWAN.2015.7210325.
18. R. S. Mangrulkar and M. Atique, "Trust based secured adhoc On demand Distance Vector Routing protocol for mobile adhoc network," 2010 Sixth International conference on Wireless Communication

and Sensor Networks, 2010, pp. 1-4, doi: 10.1109/WCSN.2010.5712310.

19. Rakesh Kumar, S., & Gayathri, N. (2016). Trust Based Data Transmission Mechanism in MANET Using sOLSR. Communications in Computer and Information Science, 169–180. doi:10.1007/978-981-10-3274-5_14
20. S. Chakraborty and S. Nandi, "QoS associated path selection in wireless mesh networks," 2014 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS), 2014, pp. 1-6, doi: 10.1109/ANTS.2014.7057283.
21. S. Mohapatra and M. Siddappa, "Enhancing security for load balanced energy enhanced clustered bee ad hoc network using secret public keys," 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2017, pp. 343-348, doi: 10.1109/ICIMIA.2017.7975632.
22. Sarfaraz Ahmed, A., Senthil Kumaran, T., Syed Abdul Syed, S., &Subburam, S. (2015). Cross-Layer Design Approach for Power Control in Mobile Ad Hoc Networks. Egyptian Informatics Journal, 16(1), 1–7. doi:10.1016/j.eij.2014.11.001
23. Sarkar, D., Choudhury, S., & Majumder, A. (2018). Enhanced-Ant-AODV for Optimal Route Selection in Mobile Ad-Hoc Network. Journal of King Saud University - Computer and Information Sciences. doi:10.1016/j.jksuci.2018.08.013
24. Simpson, S. V., & Nagarajan, G. (2021). A fuzzy based Co-Operative Blackmailing Attack detection scheme for Edge Computing nodes in MANET-IOT environment. Future Generation Computer Systems, 125, 544–563. doi:10.1016/j.future.2021.06.052
25. Singh, T., Singh, J., & Sharma, S. (2016). Energy efficient secured routing protocol for MANETs. Wireless Networks, 23(4), 1001–1009. doi:10.1007/s11276-015-1176-9
26. T. A. Alghamdi and M. E. Woodward, "QoS Algorithm for Localised Routing Based on Bandwidth as the Dominant Metric for Candidate Path Selection," 2010 10th IEEE International Conference on Computer and Information Technology, 2010, pp. 321-328, doi: 10.1109/CIT.2010.85.
27. Thakrar, P. M., Singh, V., & Kotecha, K. (2020). Improved route selection algorithm based on TORA over mobile adhoc network. Journal of Discrete Mathematical Sciences and Cryptography, 23(2), 617–629. doi:10.1080/09720529.2020.1729508
28. Ubarhande, S. D., Doye, D. D., &Nalwade, P. S. (2017). A Secure Path Selection Scheme for Mobile Ad Hoc Network. Wireless Personal Communications, 97(2), 2087–2096. doi:10.1007/s11277-017-4597-1
29. Vatambeti, R., Sanshi, S., & Krishna, D. P. (2021). An efficient clustering approach for optimized path selection and route maintenance in mobile ad hoc networks. Journal of Ambient Intelligence and Humanized Computing. doi:10.1007/s12652-021-03298-3
30. Walikar, G. A., &Biradar, R. C. (2017). A survey on hybrid routing mechanisms in mobile ad hoc networks. Journal of Network and Computer Applications, 77, 48–63. doi:10.1016/j.jnca.2016.10.014
31. Siddiqua,A,Sridevi,K&Mohammed2015,'PreventingBlackhole Attacks in MANETs using Secure Knowledge Algorithm', ProceedingsoftheInternational ConferenceonSignalProcessingand CommunicationEngineeringSystems,vol.1,pp.421-425.
32. Pooja&Chauhan,R.K2015,'Anassessmentbasedapproachto detect blackholeattackinMANET',Proceedings oftheInternational ConferenceonComputing,Communication& Automation, vol.1, pp.552-557.

33. EiKhin&ThandarPhyu2014, 'MitigatingScheme for BlackHole AttackinAODVRoutingProtocol',Proceedings oftheInternational Conference on Advances in Engineering and Technology, vol. 1, pp.29-30.
34. Mahamuni&Chandrasekar2013, 'Mitigate BlackHole Attackin DynamicSourceRouting (DSR)ProtocolbyTrapping,International JournalofComputerScienceIssues,vol.10, no. 2,pp. 49-54.
35. Shekhar Tandan Prane&EtSaurabh2011,'APDRRBasedDetection Technique forBlackhole',InternationalJournalofComputerScience andInformationTechnologies,vol.2,no.4.pp. 1513-1516.
36. MangeshGhonge&Nimbhorkar,S.U2012,'SimulationofAODV under Blackhole Attack in MANET', International Journal of Advanced Researchin ComputerScienceandSoftwareEngineering, vol.2,no.2.