Journal of Information Technology and Computing
https://jitc.sabapub.com
ISSN: 2709-5916

2023 Volume 4, Issue 2 : 20 – 30
DOI : 10.48185/jitc.v4i2.930

APPROACHES FOR SOLVING ROUTING AND SECURITY ISSUES IN MOBILE AD-HOC NETWORKS (MANETs): A REVIEW

RAJI R. O [1], OYELAKIN A. M. [2,*]

[1]Department of Computer Science, Faculty of Natural and Applied Sciences, Al-Hikmah University, Ilorin, Nigeria
[2]Department of Computer Science, College of Information and Communication Technology, Crescent University, Abeokuta, Nigeria

Received: 14.11.2023 • Accepted: 25.12.2023 • Published: 30.12.2023 • Final Version: 30.12.2023

Abstract: Mobile Ad hoc Networks (MANETs) have been very popular for some years now owing to their ability to allow communication in dynamic and infrastructure-less environments. However, the unique characteristics of MANETs, such as node mobility, limited power resources, and absence of centralized infrastructure, pose challenges in ensuring efficient routing and robust security. This paper presents a review of the existing techniques aimed at improving routing protocols and security in MANETs. Scholarly articles, conference papers, and technical reports published in notable research outlets were sourced. Then, the papers were categorized into two main areas: routing techniques and security mechanisms based on the target of this work. Regarding routing techniques, this review discusses the evolution of traditional routing protocols, including proactive, reactive, and hybrid approaches, and highlights their strengths and limitations. Moreover, the review presents some recent advancement such as location-based, Quality of Service (QoS)-aware, and energy-efficient routing protocols, which address specific challenges in MANETs. In terms of security mechanisms, this review provides an overview of the various threats and attacks that MANETs are susceptible to, including black hole, wormhole, and Sybil attacks. The review then examines the countermeasures proposed in the literature to tackle the security challenges. This article further highlights the emerging trends and research directions in the field of MANETs which include blockchain-based security, machine learning-assisted routing, and Internet of Things (IoT) integration. It is believed that this review can provide further insights to researchers in this domain.

Keywords: MANET, Routing Protocols, Security Vulnerabilities, Infrastructure-less Networks

1. Introduction

Computer Networks have become a very important aspect in the technology development because it promotes communication between people and businesses (Raheem, 2011). A good example of computer network is Mobile Ad-hoc Network. A MANET is a self-configuring, infrastructure-less networks that consist of mobile nodes without a centralized administration, (Praveen et al., 2022; Khudayer, Alzabin,Anbar,Tawafak, Wan, Alsideiri,Almeidy,2023). MANETs have emerged as a promising technology for various applications. These networks are particularly useful in situations where there is no pre-existing infrastructure or in rapidly deployable scenarios, such as disaster response or military operations to smart cities and vehicular networks. They also provide a flexible

* Corresponding Author: moruff.oyelakin@cuab.edu.ng

and dynamic communication environment, enabling nodes to communicate directly with each other, forming a temporary network on-the-fly, (Conti & Giordano, 2014).

MANET is autonomous system of nodes connected by wireless links that usually has a routable networking environment on top of a Link Layer ad hoc network (Oyelakin, Agboola, Abdullahi and Yusuf, 2020). Generally, this kind of network consists of a set of mobile nodes connected wirelessly in a self-configured, self-healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behaves as a router as they forward traffic to other specified nodes in the network. However, the decentralized and dynamic nature of MANETs presents numerous challenges, especially in terms of routing and security (Bhatnagar, Gobi, Aqeel & Solanki, 2023).

Routing is a fundamental aspect of MANETs, as it determines the path for data transmission between nodes. Since there is no fixed infrastructure in MANETs, routing protocols play a critical role in establishing efficient and reliable communication paths. Traditional routing protocols designed for wired networks, such as the popular Internet Protocol (IP) routing protocols, are not suitable for MANETs due to the unique characteristics of these networks, including node mobility, limited resources, and frequent topology changes. Consequently, several routing protocols have been proposed specifically for MANETs, aiming to optimize routing performance, minimize overhead, and adapt to dynamic network conditions (Nithya, Amudha, Musthafa, Ramirez-Asis, Velayutham & Sengan, 2022).

Korir and Cheruiyot (2022) mentioned that in a MANET, nodes do not know the topology of their network. Rather, they have to discover it by their own as the topology in the ad-hoc network is dynamic topology. The basic rules is that a new node whenever enters into an ad-hoc network, must announce its arrival and presence and should also listen to similar announcement broadcasts made by other mobile nodes. Generally, a mobile ad-hoc network (MANET) is characterized by the following criteria: dynamic topology (Karthik et al.2010), limited Bandwidth- (Kumar & Kumar, 2012), limited physical security (Kumar et al., 2012) and decentralized network control, (Kumar et al., 2012).This study focuses on reviewing of different approaches proposed in literature for solving routing and security issues in MANET.

2. Methodology

The approach used for conducting this study titled “approaches for solving routing and security issues in mobile ad hoc networks (MANETs)” utilizes a structured and comprehensive method to identify, select, analyse, and synthesize relevant literature. A set of search strings was used. Some of them include: “Mobile Ad-hoc Network (MANET)” or “Routing Protocols and techniques in Mobile Ad-hoc Networks”. Also, others are: “Security Challenges, mechanisms and protocols in Mobile Ad hoc Networks (MANETs)” or “Attacks in Mobile Ad hoc Networks (MANETs)”, or “Detection and Prevention of Attacks in Mobile Ad hoc Networks (MANETs)”. The search focused on getting some of the literature from notable repositories and databases such as researchgate, IEEE, ACM, Springer Link, Google Scholar, and Google search engine. Subsequently, the most precise, accurate and applicable articles were selected. Thereafter, a variety of methods reported in literature are presented in this paper.

3. Literature Review

Thiagarajan,Ganesan, Anbarasu, Baskar, Arthi and Ramkumar (2021) carried out a study that involved achieving optimised secure approach for the detection and isolation of malicious nodes in MANET. The authors argued that the technique is efficient for the purpose it was designed for. Oyelakin et al. (2020) investigated the performances of selected MANET routing algorithms using a nomadic scenario.. Also, Alslaim, Alaqel and Zaghloul (2014) reported that a Mobile Ad-hoc Network (MANET) consists of wireless mobile hosts forming a temporary network without the need for standalone infrastructure or centralized administration. The study also emphasized that the nodes in the network, due to their mobility, possess the ability to self-organize and self-configure. Notably, these nodes serve not only as hosts but also perform the functions of routers.

Dynamic Source Routing (DSR) is a pure reactive routing protocol which is based on the concept of source routing. DSR protocol is composed of two important phases: route discovery and route maintenance. DSR does not employ any periodic routing advertisement packets, link status sensing or neighbor detection packets (Sultana et al.., 2017). Therefore, the routing packet overhead is less because of its on-demand nature. Due to dynamic nature of the MANET operating environment, any route can fail anytime. Therefore, the route maintenance process will constantly monitors the network and notify the other nodes with the help of route error packets as well as route cache would be updated (Minhas, Mahmood & Malik, 2012). Raza, Umar, Qasim, Ashraf and Irfan (2016) defined Mobile Ad-Hoc Network (MANET) as a wireless network without any fixed infrastructure, comprising autonomous mobile nodes such as smartphones, laptops, iPads, PDAs, and more. The network has a self-configuring ability to dynamically reconstruct its topology and routing table information, allowing the exchange of data packets when nodes join or leave on an ad-hoc basis.

Ad-hoc On-demand Distance Vector (AODV) algorithm is pure reactive in nature and it contains the properties of both DSR and DSDV protocols. AODV algorithm is an improvement on DSDV in the sense that it minimizes the number of broadcasts. AODV borrows the concept of hop by hop routing, sequence numbers, periodic beacon messages from DSDV protocol (Sultana et al., 2017). When a node wants to send a message to destination node, first it will check whether it has a valid route to the destination or not. If not, then it broadcast a route request packet (RREQ) to its neighbors which then forwards the request to their neighbors and so-on, until either it reaches to the intermediate node which has a valid route for the destination or the destination node. In AODV, once the route request has reached the destination or an intermediate node with a valid route, the destination/intermediate node responds by unicasting a route reply (RREP) message back to the neighbor node from which it first received the RREQ (Minhas et al., 2012).

Sunil and Ashwani (2010) provided an overview of various on demand/reactive routing protocols Dynamic Source Routing, Ad-hoc On-demand Distance Vector and Temporary Ordered Routing Protocol (DSR, AODV and TORA) by presenting their characteristics, functionality, benefits and limitations and then makes their comparative analysis so to analyze their performance. It was observed that the performance of all protocols studied was almost stable in sparse medium with low traffic. The claim was that TORA performs much better in packet delivery owing to selection of better routes using acyclic graph.

Applications of Mobile Ad-hoc Networks (MANETs)

Several studies have established the fact that a MANET is a wireless network that enables mobile devices to connect without relying on any pre-established infrastructure or access point (Karthik et al., 2010; Oyelakin et al., 2020). There are several scenarios in which MANET technology can be

deployed to solve a problem. For examples, some of the applications of MANET include: Sensor Networks for environmental monitoring; rescue operations in remote areas; remote construction sites; emergency operations; military battlefield; civilian environments; law enforcement operations; and commercial projects as well as in nomadic education as argued by Oyelakin and Jimoh (2017).

Challenges in MANETs

Challenges in MANETs are of different categories. They include routing, power consumption, internetworking, Quality of Service and Security. Brief explanations are as outlined below:

(i) Routing: since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Furthermore, multicast routing even imposes a bigger challenge because the multicast tree is no longer static. This is due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops. Therefore, the design of the protocol becomes even more complicated (Umesh, Mewada, Iaddhani & Bunkar, 2011).

(ii) Power Consumption: the routing protocol should take into consideration the limited power resource of the mobile wireless nodes. In other words, the routing protocol should be efficient and energy-aware (Kumar et al., 2012).

(iii) Internetworking: a MANET may be interconnected with a fixed network. Therefore, the routing protocol should take into consideration the coexistence of other routing protocols designed for fixed networks (Karthik et al., 2010).

(iv) Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment imposes a further challenge (Karthik et al., 2010).

(v) Security is another critical concern in MANETs, as these networks are vulnerable to various attacks due to their open nature, lack of centralized control, and limited resources. The absence of a fixed infrastructure and the presence of malicious nodes pose significant challenges in maintaining the confidentiality, integrity, and availability of data transmitted over MANETs.

Routing Protocols in Mobile Ad-hoc Networks

Mamood and Zengin (2021) established that routing is the method of selecting a traffic path in a network or over multiple networks, which to send and receive data. It directs the passing of logically addressed packets from their source toward their ultimate destination through intermediary nodes. Routing protocol is the routing of packets based on the defined rules and regulations. Every routing protocol has its own algorithm on the basis of which it discovers and maintains the route. Each routing protocol has a data structure which stores the information of route and modifies the table as route maintenance is requires.

Types of Routing Protocols

Figure 1 show the prominent way of classifying MANETs routing protocols. The protocols may be categorized into two types, Proactive and Reactive. Other category of MANET routing protocols which is a combination of both proactive and reactive is referred as Hybrid.

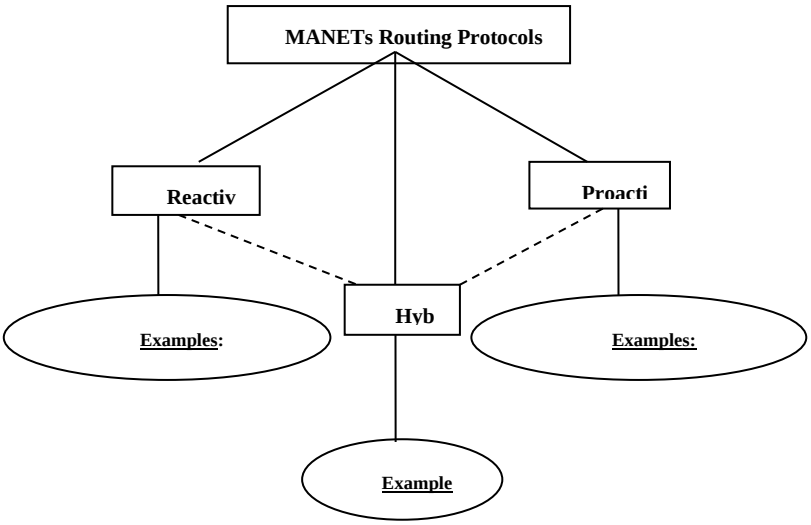

Figure 1. Classification of MANET routing protocols, (Pandey & Swaroop, 2011).

Reviewed Works on MANET Routing Protocols

Praveen et al. (2022) proposed a secure and energy-efficient routing protocol is proposed by using group key management. Asymmetric key cryptography is used, which involves two specialized nodes, labeled the Calculator Key (CK) and the Distribution Key (DK). The authors argued that these two nodes are responsible for the generation, verification, and distribution of secret keys. Kumar and Singla (2022) carried out a performance analysis of Optimized ACO-AOMDV Routing Protocol with AODV and AOMDV in MANET scenarios. The work focused on measuring the performances of the optimized ACO-AOMDV routing algorithms and the existing AODV and AOMDV ones. It reported that the optimized one out-performed the other two ones.

Revath, Karpagavall and Jullet (2020) proposed a Hybrid Approach for Cost-Effective Routing and Security in MANETs using BSSO-DSR and AES-ECC Algorithms. In their study, they highlighted the use of the DSR-BSSO-MANETs algorithm, which effectively detects malicious attacks in MANETs by isolating an improved path through the BSSO clustering algorithm to optimize energy consumption and maintain load balancing. The research identified the successful recognition of blackhole attacks using the MND-TX/RX Mechanism. The results obtained from the study led to the conclusion that the DSR-BSSO-MANETs method outperforms other existing systems in terms of routing efficiency, including better Routing Overhead, PDR (Packet Delivery Ratio), Throughput, energy consumption, and packet delay.

David, Cordova, Alexandre, Nguyen i, Mai and Guy (2020) proposed a system named Block graph. It is a platform that promotes blockchain technology for mobile ad hoc networks. The technique established argument for the deployment of ad-hoc network that can be used to support transactions in blockchain platform..

Oyelakin et al. (2020) equally conducted a study comparing MANET routing protocols in a Nomadic Community Scenario. The study further emphasized the importance of the protocols in promoting the performances of the networks in the scenario being used for. The researchers simulated a Mobile Ad-hoc Network (MANET) to explore its potential for network connectivity in

a large nomadic environment. The study focused on scenarios where nomads require wireless connectivity without relying on central network facilities due to their operating environments. Comparative analysis was performed on the DSDV and AODV algorithms in this specific scenario. The used Network Throughput and End-to-End Delay as performance metrics to determine which protocol performs better under the experiment's circumstances.

Kwan-Wu, John, Aidan, and Rogar (2019) outlined their implementation and deployment experiences with MAD-HOC's AODV and DSDV protocols for MANETs. Some of the key issues they identified are: handling unreliable/unstable links, minimizing dependence on topology-specific parameters, mechanisms for handoff and reducing packet loss as well as incorporating neighbor discovery and filtering. The authors observed that neighbor selection is very important in MANET routing protocols. Thus, they advocated for adaptive parameter adjustment and exploring pre-emptive route construction based on signal strength. They propose developing a neighbor selection sub-layer with various metrics, filters, and heuristics for enhanced MANET routing.

Thiagarajan and Moorthi (2017) addressed various routing techniques in their paper. Subsequently, they introduced a dynamic and secure routing method called OLSE (optimized link state routing) to optimize routing performance. OLSE is a proactive routing protocol that employs periodic metrics, offering efficient results in managing network traffic overload and improving throughput. The proposed mechanism was evaluated through simulation software, demonstrating its effectiveness in achieving optimal routing outcomes.

Reviewed Works on Security Challenges and Detection of Attacks in MANETs

Murugeshwari, Amirthavalli, Sri and Pari (2023) conducted research on a hybrid key authentication scheme to ensure privacy in Ad-hoc communication. Their study introduces a team-centered rekey control framework with a grouping component that divides the network into smaller groups using group clusters. This approach effectively addresses the privacy issue by utilizing rekeying to update shareable keys, enabling both forward and reverse privacy. The periodic beacon signals sent by team members help detect and prevent node replication attacks in the sensor field. Experimental results demonstrate that the proposed system outperforms the current model in terms of power utilization, privacy level, key accuracy, memory utilization, and time consumption.

Ghodichor et al. (2023) conducted research on securing MANET against attacks using a blockchain-based Secure Routing Algorithm (SRA). MANET, being an infrastructure-less network with a dynamic topology, is highly vulnerable to attacks. The proposed SRA with blockchain technology authenticates nodes and safeguards data and control flow. The study shows that this approach enhances MANET security, reduces delay, and improves parameters such as packet delivery ratio, throughput, and end-to-end delay. The authors mentioned that their future work will explore further applications of blockchain in MANET. Korir et al. (2022) carried out a survey on security challenges in the current MANET routing protocols. The work provided deep insights on security related issues in MANET protocols.

Nishi and Pooja (2022) argued that generally that MANETs are faced with a lot of security vulnerabilities because of their usual decentralized nature. This nature makes the mobile nodes/devices to be susceptible to different attacks. Network layer attacks in MANET include Black hole, Gray Hole, Wormhole, flooding, and sinkhole attacks, which disrupt packet routing and degrade network performance. Several routing protocols are used in MANET, including AODV, DSR, DSDV, and ZRP. It has equally been reported that some of the limitations of MANET include energy constraints, security attacks, scalability issues, and security vulnerabilities.

Srilakshmi, Alghamdi, Vuyyuru, Veeraiah and Alotaibi (2022) proposed a Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks. The algorithm uses optimization algorithms for the improvement of routing and ensure trust-based secure and energy-efficient navigation in MANETs. The fuzzy clustering approach is employed to select Cluster Heads (CHs) based on indirect, direct, and recent trust values. Value nodes are identified based on their trust ratings. The CHs then engage in multi-hop routing using the projected protocol, selecting the best routes considering factors like latency, performance, and connectivity within the network.

Sivapriya and Mohandas (2022) presented an overview of various topics that have been discussed on MANET security. This effort led to the identification of elements contributing to threat scenarios, a summary of network security requirements, and the categorization of attacks based on the communication protocol stack. The article also presents potential research directions for developing promising future security systems for MANETs and related application paradigms. Thiagarajan, Ganesanb, Baskar and Ramkumar (2021) proposed a system for detecting and isolating malicious nodes in MANET. Once detected, the malicious node is isolated and discarded, and an alternative path is established using different techniques. The system uses an algorithm to enable multipath reliable routing, finding paths for a group of nodes. These paths are then reorganized based on the reliability index.

Khan, Chawhan, Mushrif, and Neole, (2021) built a mechanism to analysed the performance of Adhoc on-demand Distance Vector Protocol (AODV), a reactive routing protocol under the influence of Black hole, Gray hole and Worm hole attacks in MANET. They proposed a security mechanism that is based on two techniques, namely: cryptography-based, and trust-based. They further argued that cryptography technique is more accurate but consumes more energy and takes more time for detection and prevention of attacks as compared to trust based. Trust based technique consumes less energy and time but sometimes doesn't provide accurate detection. The researchers opined that the technique is not efficient for multiple attacks and can be used for particular type of attacks.

Khalifa, Nuri and Ali (2021) proposed an Intrusion Detection System (IDS) using three Machine Learning (ML) techniques. The algorithms include Random Forest (RF), Support Vector Machines (SVM), and Naive Bayes (NB). These techniques were applied to classify nodes in MANET using the Dynamic Source Routing (DSR) protocol. The Random Forest algorithm demonstrated the highest accuracy in experimental research. SVM is a supervised learning technique that identifies patterns for classification and regression, reducing data and enhancing predictive performance. NB is a probability classifier model that can handle multiple classes simultaneously, requiring minimal data for training compared to other models.

Regassa and Yeom (2021) implemented an IDS mechanism along with the OLSR protocol to accurately detect misbehaving nodes in a MANET. The mechanism validates the path and detects attackers, isolating them through an alternative path for End-to-End communication. Although this approach adds some network overhead, it significantly improves network security. Future research directions include evaluating the routing protocol and developing mechanisms to minimize the introduced overhead in network traffic. Aside this, Ibrahim, Ahmed, Sundaram and Karthika, (2021) introduced the rushing attack in the AOMDV multicast routing protocol, revealing its detrimental impact on MANET performance. Then, the researchers implemented a prevention mechanism based on time threshold and random route selection techniques. They claimed that the rushing attack involves nodes transmitting excessive route requests with higher transmission power, disrupting data transmission. The prevention mechanism successfully protected the network, improving throughput,

packet delivery ratio, and reducing end-to-end delay compared to the attacked AOMDV routing protocol. Authors claimed that this method does not require additional external resources, making it suitable for resource-constrained Mobile Ad hoc Networks.

Pooja, Kavita, and Gia (2020) proposed a protective mechanism against dual attacks in MANET with specific focus on Black Hole Attack and Gray Hole attacks. The approach involved leveraging the concept of Artificial Neural Network (ANN) as a deep learning algorithm in conjunction with the swarm-based Artificial Bee Colony (ABC) optimization technique. The ABC optimization technique emulates the intelligent behavior of honeybees and is used to categorize the network nodes into two lists: healthy nodes and affected nodes. The affected nodes are further subdivided into BHA nodes and GHA nodes. ANN is then employed to train the network using these categorized properties. The network's performance was evaluated based on parameters such as Packet Delivery Ratio (PDR), throughput, and delay. The results demonstrated significant improvement in PDR, throughput, and delay when employing the swarm-based Artificial Bee Colony (ABC) optimization technique for protection against BHA and GHA attacks.

Deepak, Nisha, Sunil and Sudesh (2020) analysed and compared ant colony optimization algorithm with DSDV, AODV, and AOMDV based on shortest path in MANET (2020) discussed an ant colony optimization algorithm based on the shortest path in MANET. Swarm Intelligence (SI) techniques, such as Ant-Colony Optimization (ACO) and Particle Swarm Optimization (PSO), are utilized to find optimal communication paths among nodes. The protocol is optimized to select the best path, thereby extending communication availability. These SI-based techniques resolve various routing challenges and offer improved packet delivery speed, throughput, power efficiency, and packet delay.

Prasath and Sreemathy (2019) examined the performance of the optimized Dynamic Source Routing protocol (DSR) for MANETs. They utilized the Firefly algorithm to modify the conventional DSR algorithm and find the best routes between communication nodes. The suggested technique improved DSR routing performance by using the Firefly algorithm to facilitate well-organized packet transfers from source to destination nodes. The best path was determined based on link quality, node mobility, and end-to-end delay. Bhagyalakshmi (2018) proposed Q-AODV, a Flood Control Ad-Hoc on Demand Distance Vector Routing Protocol, to minimize control packet volume by reducing intermediary nodes in the route discovery process. It uses queue length to control route request (RREQ) broadcast, leading to enhanced QoS metrics and network lifespan compared to AODV. Ravilla and Reddy (2016) discussed the use of the Secured Hash Algorithm (SHA3-256) for secured routing in MANETs with the Hybrid Routing Technique. The Hashed Message Authentication Code (HMAC) was employed to ensure data integrity and authenticity. The Zone Routing Protocol (ZRP) served as the hybrid routing method.

4. Findings and discussions

The review in this paper involves an analysis of scholarly articles, conference papers, and technical reports published in notable research outlets. The selected papers were categorized into two main areas: routing techniques and security mechanisms. Regarding routing techniques, this article discussed the evolution of traditional routing protocols, including proactive, reactive, and hybrid approaches, and highlights their strengths and limitations. Then, some of the countermeasures proposed in the literature were mentioned. The review equally discussed some of the performance metrics used in evaluating the proposed techniques and identify the gaps and challenges in the existing literature. It was equally observed that there are emerging trends and research directions in

the field of MANETs. These new trends blockchain-based security, machine learning-assisted routing, and Internet of Things (IoT) integration. This paper pointed out that some of the works of researchers have proposed various innovative mechanisms for the detection and prevention of common attacks in MANET. The innovative methods include cryptography-based, trust-based, machine learning-based, and blockchain-based solutions. It is believed that the review in the study can create a comprehensive understanding of MANETs, including their routing protocols, security challenges, attacks, and potential solutions for the security in various scenarios.

Conclusion

This study reviewed and analyzed various techniques for improving routing and security in the network. Routing techniques, such as energy-aware routing, Quality of Service (QoS) routing, and cross-layer routing, were discussed, highlighting their advantages and challenges. Security techniques, including authentication and key management, intrusion detection and prevention systems (IDPS), trust-based routing, and secure data forwarding, were also explored to address the security concerns in this kind of network. A comparative analysis of the reviewed techniques provided a comprehensive understanding of their performance characteristics. The insights gained from this review can assist researchers and network practitioners in selecting appropriate techniques for enhancing the routing efficiency and security resilience of MANETs. This study summarizes the findings of existing research papers on this subject and it is believed that the insights obtained will further drive researches in the area of routing and security issues in MANET.

References

[1] Alslaim, M. N., Alaqel, H. A., & Zaghloul, S. S. (2014). A comparative study of MANET routing protocols. In *The Third International Conference on e-Technologies and Networks for Development (ICeND2014)* (pp. 178-182) , IEEE.

[2] Bhatnagar, G., Gobi, N., Aqeel, H., & Solanki, B. S. (2023). Sparrow-based Differential Evolutionary Search Algorithm for Mobility Aware Energy Efficient Clustering in MANET Network. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(8s), 135-142.

[3] Conti Marco & Giordano Silvia (2007).Multihop Ad Hoc Networking: The Reality,IEEE Communications Magazine 45(4):88 – 95, Follow journal, DOI: 10.1109/MCOM.2007.343617,IEEE Xplore

[4] David Alexis, Cordova Morales, Alexandre Laube, Nguyen Thi, Mai Trang, Guy Pujolle (2020). Blockgraph: A blockchain for mobile ad hoc networks. In *2020 4th cyber security in networking conference (CSNet)* (pp. 1-8). IEEE.

[5] Deepak Sinwar, Nisha Sharma, Sunil Maakar & Sudesh Kumar (2020). Analysis and comparison of ant colony optimization algorithm with DSDV, AODV, and AOMDV based on shortest path in MANET, Journal of Information and Optimization Sciences 41(2):621-632, DOI: 10.1080/02522667.2020.1733193

[6] Dilli, R., & Reddy, P. C. S. (2016, October). Implementation of security features in MANETs using SHA-3 standard algorithm. In *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 455-458). IEEE.

[7] Ghodichor, N., Sahu, D., Borkar, G., & Sawarkar, A. (2023). Secure Routing Protocol To Mitigate Attacks By Using Blockchain Technology In Manet. *arXiv preprint arXiv:2304.04254*.

[8] Goswami M. M., (2017) "AODV based adaptive distributed hybrid multipath routing for mobile AdHoc network," in Proc. International Conference on Inventive Communication and Computational Technologies, pp. 410-414.

[9] Ibrahim H. A., Ahmed A. S., Sundaram B. B., Karthika P., (2021), Prevention of Rushing Attack in AOMDV using Random Route Selection Technique in Mobile Adhoc Network, Proceedings of Fifth Int. Conf. on Electronics, Communication and Aerospace Tech. (ICECA2021) IEEE.

[10] Karthik S, Kannan S., Arunachalam V. P., Ravichandran T., and Valarmathi M. L..(2010).An investigation about performance comparison of multihop wireless ad-hoc network routing protocols in MANET, *International Journal of Computer Science Issues (IJCSI)*, 7(3), pp. 35— 41.

[11] Khalifa M. M., Nuri O., Ali Alheeti K. M., (2021).New Intrusion Detection System to Protect MANET Networks Employing Machine Learning Techniques, *International Conference of Modern Trends in Information and Communication Tech. Industry (MTICTI) IEEE*.

[12] Khan A. U., Chawhan M. D., Mushrif M. M., Neole B., (2021).Performance Analysis of Adhoc On-demand Distance Vector Protocol under the influence of Black-Hole, Gray-Hole and Worm-Hole Attacks in Mobile Adhoc Network, *Proceedings of the Fifth Int. Conf. on Intelligent Computing and Control Systems (ICICCS 2021)*, IEEE Xplore Part Number: CFP21K74-ART; ISBN: 978-0-7381-1327-2.

[13] Khudayer, B. H., Alzabin, L. R., Anbar, M., Tawafak, R. M., Wan, T. C., AlSideiri, A., ... & Al-Amiedy, T. A. (2023). A Comparative Performance Evaluation of Routing Protocols for Mobile Ad-hoc Networks. *International Journal of Advanced Computer Science and Applications*, *14*(4).

[14] Korir, F., & Cheruiyot, W. (2022). A survey on security challenges in the current MANET routing protocols. *Global Journal of Engineering and Technology Advances*, *12*(01), 078-091.

[15] Kumar S., and Kumar J. (2012).Comparative analysis of proactive and reactive routing protocols in mobile ad-hoc networks (MANET), Journal of Information and Operations Management, 3(1), pp. 92—95.

[16] Kumar V. and Singla S., (2022). Performance Analysis of Optimized ACO-AOMDV Routing Protocol with AODV and AOMDV in MANET, *in Advances in Computing and Data Sciences: 6th International Conference, ICACDS 2022*, Kurnool, India, April 22–23, 2022, Revised

[17] Kwan-Wu Chin, John Judge, Aidan Williams & Roger Kermode Sydney (2019). Networks and Communications Lab Motorola Australia Research Centre 12 Lord St, Botany, NSW, Australia {kwchin, johnj, aidan, rkermode}@arc.corp.mot.com

[18] Mamood, A., & Zengin, A. (2021). Performance Evaluation of MANET Routing Protocols AODV and DSDV Using NS2 Simulator. *Sakarya University Journal of Computer and Information Sciences*, *4*(1), 1-10.

[19] Murugeshwari B., Saral Jeeva Jothi D., Hemalatha B.,Neelavathy Pari S. (2023).Trust Aware Privacy Preserving Routing Protocol for Wireless Adhoc Network, International Journal of Engineering Trends and Technology Volume 70 Issue 9, 362-370, September 2022, ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I9P236 © 2022 Seventh Sense Research Group®

[20] Minhas, H. Mahmood, & H. Malik,(2012). Incentive driven cooperation to avoid packet loss in multihop ad hoc networks, in 2012 *International Conference on Emerging Technologies*, 2012, 1–6.

[21] Nithya, R., Amudha, K., Musthafa, A. S., Sharma, D. K., Ramirez-Asis, E. H., Velayutham, P., ... & Sengan, S. (2022). An optimized fuzzy-based ant colony algorithm for 5G-MANET. *Computers, Materials & Continua*, *70*(1), 1069-1087.

[22] Oyelakin, A. M., Yusuf, S. A., Agboola, R. O., & Abdullahi, F. (2020). A Study on The Comparative Analysis Of MANET Routing Protocols In Nomadic Community Scenario. *Amity Journal of Computational Sciences (AJCS) Volume 4 Issue 1 ISSN: 2456-6616.*

[23] Oyelakin A.M. & Jimoh R.G. (2018). Simulation of Mobile Ad-hoc Network and its Applicability in Academic Scenario, *in proceedings of 10th iSTEAM Multi-Disciplinary Conference, February,2018 Conference*, Delta State Polytechnic, Ogwuashi-uku, Delta State, Nigeria,679-687

[24] Pandey, K., & Swaroop, A. (2011). A comprehensive performance analysis of proactive, reactive and hybrid manets routing protocols. *arXiv preprint arXiv:1112.5703*.

[25] Pooja Rani, Kavita, Sahil Verma and Gia Nhu Nguyen, (2020), Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm with Artificial Neural Network, IEEE.

[26] Prasath, N., & Sreemathy, J. (2019). Optimized dynamic source routing protocol for MANETs. *Cluster Computing*, *22*(Suppl 5), 12397-12409.

[27] Praveen Bondada, Debabrata Samanta Manjit , Kaur Kaur & Heung-No Lee (2022).Data Security-Based Routing in MANETs Using Key Management Mechanism, January 2022, *Applied Sciences*, 12(3):1041,DOI: 10.3390/app12031041

[28] Raheem Ali H. (2011). Security Issues in Mobile Ad-Hoc Network and Solutions,*Telecommunication Systems*, 1-6

[29] Raza, N., Umar Aftab, M., Qasim Akbar, M., Ashraf, O., & Irfan, M. (2016). Mobile ad-hoc networks applications and its challenges. *Communications and Network*, *8*(03), 131-136.

[30] Regassa D., Yeom H. Y., Son Y., (2022), Efficient Attacker Node(s) Detection and Isolation Schemes in MANETs OLSR Protocol, Int. Conf. on Information Networking (ICOIN) IEEE.

[31] Revathi, P., Karpagavalli, N., & Angel, K. J. C. A Hybrid Approach For Cost-Effective Routing And Security For Manets Using BSSO-DSR And AES-ECC Algorithms.

[32] Sivapriya, N., & Mohandas, R. (2022). Analysis on Essential Challenges and Attacks on MANET Security Appraisal. *Journal of Algebraic Statistics*, *13*(3), 2578-2589.

[33] Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. *IEEE Access*, *10*, 14260-14269.

[34] Sun .Z, Wei M., Zhang .Z., and Qu .G (2019).Secure Routing Protocol based on Multi-Objective Ant-colony-optimization for wireless sensor networks, Appl. Soft Comput. J., vol. 77, pp. 366–375.

[35] Sultana Jeenat & Ahmed Tasnuva (2017).Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography, 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), February 2017, DOI: 10.1109/ECACE.2017.7912964

[36] Thakker, V. M., Reddy, G. M., Kumar, K. V., & Moses, D. (2018). Choosing optimal routing protocol by comparing different multipath routing protocols in mobile Adhoc networks. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 1284-1290). IEEE.

[37] Thiagarajan R. and M. Moorthi,(2017). Efficient routing protocols for mobile ad hoc network," in Proc. Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bioinformatics,. 427-43

[38] Thiagarajan, R., Ganesan, R., Anbarasu, V., Baskar, M., Arthi, K., & Ramkumar, J. (2021). Optimised with secure approach in detecting and isolation of malicious nodes in MANET. *Wireless Personal Communications*, *119*, 21-35.

[39] Umesh K. S., Mewada S., Iaddhani L., & Bunkar K. (2011).An overview and study of security issues & challenges in mobile ad-hoc networks (MANET), International Journal of Computer Science and Information Security, 9(4), pp. 106—111.