International Journal of Information Technology and Management
Vol. 19, Issue No. 1, February-2024, ISSN 2249-4510

DOI: https://doi.org/10.29070/7ddjde88

A Comprehensive Survey on MANET: Architecture, Protocols, and Challenges

Narendra Kumar Tiwari [1] *

1. Research Scholar, Department of Computer Science & Application, LNCT University, Bhopal, M.P., India
tiwari.narendra07@gmail.com

Abstract: Mobile Ad Hoc Networks, also known as MANETs, are a paradigm for wireless networks that are dynamic and self-configuring. They make it possible to communicate without any interruptions and do not rely on established infrastructure. This study offers a detailed review of MANET design, including the most important routing protocols and the issues that are related with them. The article addresses a variety of routing tactics, such as proactive, reactive, and hybrid protocols, and highlights the advantages and disadvantages of each of these approaches. Additionally, crucial difficulties like as security risks, energy efficiency, scalability, and quality of service (QoS) are investigated, along with potential solutions to these problems. The paper also investigates current developments and potential future research areas that might improve the performance of MANETs in applications that are used in the real world. The results of this survey provide scholars and practitioners who are working on MANET creation and optimisation with a valuable reference of information.

Keywords: MANET, Architecture, Protocols

X

INTRODUCTION

Mobile Ad Hoc Networks, also known as MANETs, are wireless networks that are decentralised and self-organising. They allow for smooth communication without relying on established infrastructure. Each node in a MANET performs the dual role of a host and a router, allowing it to dynamically create and maintain network communication. Because of its adaptability, MANETs are extensively used in a variety of applications, including military operations, disaster recovery, automobile networks, and other applications that require reliable communication that is not dependent on any particular infrastructure. MANETs are characterised by their dynamic topology, which presents a number of obstacles. These concerns include an efficient routing system, potential security risks, energy management, and scalability issues. Several different routing protocols have been created in order to overcome these issues. These methods can be generically categorised as proactive, reactive, or hybrid protocols. In order to achieve optimal performance, proactive protocols are responsible for the ongoing maintenance of network topology information, reactive protocols are responsible for the establishment of routes on demand, and hybrid protocols integrate portions of both techniques. In spite of the improvements that have been made in MANET research, there are still significant issues that need to be addressed, including network security, congestion control, and quality of service (QoS). The objective of this study is to give a complete examination of MANET design, investigate various routing protocols, and highlight important difficulties and potential solutions. Furthermore, in order to provide insights into the ever-changing landscape of MANET technology, we will highlight new trends as well as future research areas.

MANET

In the context of wireless ad hoc networks, the term "Mobile Ad Hoc Network" (MANET) is an abbreviation for a MANET that is composed of mobile devices that are capable of configuring themselves. When they are in a bind, Latin speakers frequently use the phrase "for this reason" in their conversation. Another aspect of what is commonly referred to as a "ad-hoc" network is the absence of centralised control and infrastructure that has been developed. It is possible for every particular node in an ad hoc mobile network to perform the functions of both a gateway and a terminal for other nodes in the immediate vicinity. It is possible for nodes to establish network topologies by self-organising and collaborating with one another. This would enable users and devices to interact without any prior preparation. In a general sense, the term "Wireless Ad Hoc Networks with Routable Networking Environments" is a more accurate way to describe MANETs than the term "Link Layer Ad Hoc Networks." When it comes to mobile ad hoc networks, there is no one controller present, in contrast to mesh networks. For any two mobile nodes that are within radio range of one another, it is possible to create a wireless link between them. Because of the fact that nodes located in different regions of the world are dependent on one another in order to transfer data, the architecture of the network is always changing. Because of its capacity for self-organization and self-configuration, mobile ad hoc networks are ideally suited for use in both the military and the civilian sectors.

When it comes to facilitating communication between nodes, these networks frequently make use of routing technology. There are two primary categories that can be applied to the protocols that are utilised by a MANET. Take, for instance, the router that uses the least amount of electricity as an illustration of a protocol. The path that it travels from beginning to end is the one that is the most energy-efficient conceivable. One of the problems with this category is that it always chooses the shortest routes, which means that they are the least costly, but they also "expire" very quickly. A general growing trend in network length is seen by the second set. An approach known as multi-path forwarding is utilised in order to divide the traffic strain. There are a few potential solutions, such as reducing the total number of nodes that are necessary for forwarding and allowing some forwarding nodes to sleep for variable amounts of time. As a result of the more even distribution of load, MANET networks have longer lifespans than other types of distributed networks. There are a variety of reactive routing strategies that may be utilised in order to enhance the performance of MANETs. About halfway through the decade of the 1990s, research on MANETs became increasingly important as a result of the growth of portable computers and wireless networking technologies such as Wi-Fi. When doing research in an academic setting, it is standard practice to examine methods and the degree to which they may be adapted to other settings. A number of metrics, including network performance, end-to-end latency, packet delivery ratio, and routing overhead, are typically utilised in the process of evaluating protocols.

Issues in Mobile Ad hoc Networks (MANETs)

Disaster relief&military combat communications were the primary early users of MANETs. However, concepts of ad hoc networks have lately expanded in several application fields, such as smart roads, remote environmental monitoring,&animal movement outposts. The quality of service criteria for these applications are distinct. Several Gb/s to a few Kb/s is the range of bandwidth needs. Some are sensitive to delays, while others are more concerned about losses. On the other hand, some are quite mobile while others could be somewhat immobile. Connecting MANETs to the internet is challenging for a number of

reasons. Some of these will be addressed later on.

Security

When it comes to MANETs, security is paramount. There is a higher chance of nose, mistake,&eavesdropping in wireless networks compared to cable ones. It is more difficult to provide security when there is mobility&wireless connections. Physical layer spread spectrum modulation (direct sequence or frequency hopping)&encryption are common security techniques employed because of this. Establishing a trustworthy connection is a challenging task.

Routing

When it comes to MANETs, routing is a major pain point. Data packets can be sent from one location to another in the most efficient way possible using a process known as routing. It is increasingly difficult to control the network when every device is acting as a router. For the simple reason that any node in the network is free to roam aimlessly. Since the best route at any given moment may not be viable a few seconds later, it is necessary to find&choose new pathways whenever a node relocates. Additionally, a path might fail if the environment is changed from an interior situation to an outside one.

Scalability

Both the network&packet sizes have a significant impact on how MANETs function. Finding suitable pathways&optimising routing get more challenging as the size increases. The forwarding process is also significantly affected by packet size. Network scalability refers to the ability of a network to keep providing a reasonable level of service even when its size&traffic volume rise. Routing protocols are another aspect that limits the scalability of MANETs.Providing the massive volume of broadcast messages in a dynamic environment becomes a significant difficulty due to the changing topology of a MANET.

Quality of Services

Programmers have a huge challenge when dealing with Quality of Services (QoS). It is more challenging to get excellent performance with MANET due to its very dynamic structure. It is important that the network can meet the level of service that users expect. Measurements of latency, jitter,&bandwidth provide insight into the performance. While on the go, it's not easy to keep these characteristics in top shape. Achieving quality of service in a MANET requires optimisation across several layers.

Types of MANET

Vehicular Ad hoc Networks (VANETs): Because of this, it's possible for cars&equipment placed along roadways to exchange data. To help cars respond intelligently to accidents&collisions, a sort of AI called intelligent vehicular ad hoc networks (In-VANETs) is utilised.

Smart Phone Ad hoc Networks (SPANs): Instead than relying on shared wireless infrastructure, cellular carrier networks, or access points, peer-to-peer networks make use of the built-in Bluetooth&Wi-Fi capabilities of regularly used smartphones. There is no requirement for a designated group leader in SPANs, unlike in Wi-Fi Direct, which uses hubs&spokes. In this way, no damage may come to the

network's architecture when peers join&go.

Internet based mobile ad hoc networks (MANETs): A kind of network that connects mobile nodes to gateways on the internet is called a "ad hoc" network. In a conventional Hub-Spoke VPN, for example, a geographically scattered MANET may be formed by merging several sub-MANETs. Traditional ad hoc routing methods cannot be used with these networks.

Characteristic of MANET

Wireless transmitters&receivers used by nodes in mobile ad hoc networks may be extremely directional, omnidirectional, or steerable. A random multi-hop graph network, sometimes called a "ad hoc" network, may form among nodes depending on their positions, the patterns of their coverage (transmitter&receiver), the strengths of their transmissions,&the degrees of co-channel interference. Over time, migration or other events may alter the communication between the nodes in an ad hoc network. One approach to describing these kinds of networks is as follows:"

Dynamic Network Topologies: As nodes travel at varying rates, the network's architecture changes. Nodes in a MANET may switch between hosting&routing data since they are all connected to the same network. I mean, it can run its own show.

Energy-constrained Operation: All modern electrical devices rely on batteries for electricity.Improving the network's design is necessary to reduce mobile devices' power consumption.

Limited Bandwidth: To make the most of the limited data transfer capacity of a Wi-Fi network, networks need to be fine-tuned.

Security Threats: When compared to cable connection, the security of wireless is far worse. Protecting the data in transit requires bolstering the MANET's security. Every part of the system, including routing, security,&host configuration, is interconnected. In this setup, the firewall is not located in one central location. Eavesdropping, spoofing,&denial-of-service assaults are more likely, therefore it's important to think about that. Beyond the faster, semi-static design of fixed Internet routing, there are additional assumptions&performance concerns with protocol design.

Multi-hop Radio Relaying: In MANETs, multi-hop routing is used to deliver messages to their ultimate destinations when the nodes at the source&destination aren't in radio range. Mobile nodes are characterised by their portability, lack of power,&memory.

Bandwidth-Constrained, Variable Capacity Links: Traditional methods of communication are often superior than their wireless counterparts in terms of reliability, efficiency, stability,&competence. When it comes to connection bandwidth, this graph shows how unpredictable wireless networks may be.

Other Features

- Because it is mobile & spontaneous, configuring the network is easier.
- All nodes have identical features & capabilities, creating a perfectly balanced ecosystem. A large user base with a high degree of user mobility.

- Intermittent communication between nodes.
- Regular upgrades to the routing scheme.

Applications of MANET

The fact that MANET permits the establishment of temporary connections without a predetermined infrastructure opens up several potential uses. Let me give you some instances.

Military Battlefield: Strong dependable communication is required in various ways in today's digital battlefield. Mobile vehicles, tanks, trucks, among other things, are equipped with a plethora of communication equipment. Also, soldiers could have handheld comms devices that can link up with a wireless base station or talk to each other directly if they're in radio range. Conversely, certain forms of expression are considered antiquated. If the enemy destroys the wireless base station the person being contacted is not in radio range, communication with other soldiers may be cut off. This is when mobile ad hoc networks come in handy. The ability of an ad hoc network to recover from the removal or relocation of nodes is what makes it self-organising. Multi-hop c communication enables armed forces to communicate data with other units by transmitting data from one radio equipment to another.

Sensor Networks: Sensor networks are one more MANET use case. A network of sensors of varying sizes is the basis of this technology. A wide range of qualities may be detected by using these. This comprises a wide range of environmental factors such as poisons, pollutions, other environmental factors. Applications include predicting earthquakes measuring the humidity of the ground for agriculture. There are only so many sensors that can transmit data to a central computer, therefore each one is dependent on the others to do so. Individual sensors are prone to failure loss because of their low computational power. It's possible that the future of homeland security will depend on mobile ad hoc sensor networks.

Automotive Applications: Currently, the topic of automotive networks is frequently explored. A variety of ad hoc networks of varying sizes should be created enabling cars to communicate with the road, traffic signals,&each other. With the help of the network, drivers will have access to up-to-the-minute information on traffic, road conditions,&accident warnings.

Commercial Sector: When responding to disasters like fires, floods, or earthquakes, ad hoc procedures may be necessary. When communication infrastructure is either destroyed or unavailable, a communication network has to be set up immediately, rescue activities must be launched in an emergency. A portable device is used to transmit data between members of the rescue crew. Additional business applications include ad hoc mobile communication between ships, police enforcement, others.

Personal Area Network: One frequent method of establishing a personal area network (PAN) is by use of ad hoc connections between various mobile (and stationary) devices. Although PANS may connect individual devices, like those in your house, they really shine when integrated into a larger network. This is one way in which PANs may be seen as a growth of the telecom network or the internet. The idea of "ubiquitous computing," sometimes known as "pervasive computing," is similar; it states that, no matter how subtle, individuals are constantly instantly interacting with technology.

Other Applications

- In the aftermath of a natural disaster.
- Mine cite operations mine.
- Meetings that must be attended as soon as possible.
- Messages exchanged privately
- Environments that foster cooperation
- Conferencing
- Networks at home
- Healthcare
- On the road, there's always something to keep you entertained (file sharing in cars, trains & planes)
- Computing that is both dispersed&collaborative.

Advantages of MANET

The benefits of MANET are as follows:

- They allow anybody, regardless of location, to access information & services.
- In addition, these networks may be established at any time&in any location.
- Networks can be built up quickly, easily,&affordably.
- Power may be decreased.
- Due to its structure, it is more resistant to single-component failures.

Disadvantages of MANET

- This is a list of some of the problems with MANETs:
- Physical security&limited resources.
- A weakness of mutual trust is that it may be exploited.
- There is a lack of access control.
- Volatile network architecture makes it difficult to discover harmful nodes.
- Wired network security procedures are not applicable to ad hoc networks.

MANET Challenges

The limitations&inefficiencies that plague a MANET must be addressed. Included are:

Spectrum Allocation: There are a number of issues that need to be resolved, including device mobility, interference, restricted range, limited data throughput, and radio frequency (RF) spectrum sharing. At this time, the Federal Communications Commission (FCC) is the entity that is accountable for monitoring and regulating the utilisation of radio transmission spectrum. The ISM band is the location where the majority of experimental installations of ad hoc networks are carried out. It is necessary for there to be a restricted or approved spectrum range within which ad hoc networks are permitted to operate in order for them to function without interfering with one another. Microwave ovens frequently make use of the 2.4 GHz frequency band, which has the potential to cause disruptions to wireless local area network deployments.

Energy Efficiency: It is necessary to find a solution to the problem of maintaining energy efficiency. Power consumption is not an issue for the majority of the protocols that are now in use since these protocols assume that all hosts and routes are powered by main power. However, batteries are the power source for the majority of today's portable electronic devices. Batteries are incredibly archaic and inefficient technological devices when compared to microprocessors. As of right now, the maximum amount of time that a Li-on battery may last is between two and three hours. Because of the limited number of hours that the gadget may be powered on, it is essential to make advantage of power conversion. Devices that are capable of functioning as routers are extremely important to mobile ad hoc networks. Because of this, the power consumption of mobile ad hoc network nodes for the transmission of packets is significantly higher than average.

The Wireless Link Characteristics are Time-Varying in Nature: Wireless channels sometimes experience transmission difficulties such as fading, route loss, obstructions, interference. There are a number of factors that reduce the reliability of the wireless transmission.

Limited Range of Wireless Transmission: Data rates are reduced due to the limited radio bandwidth compared to wireless networks. Therefore, it is essential to minimise administrative effort while maximising bandwidth efficiency.

Packet Losses Due to Errors in Transmission: Interference, high bit error rates (BERs) in wireless channels, rising collisions produced by "hidden terminals"&unidirectional connections, frequent route breakdowns caused by node mobility are among the many causes that may cause MANET packet loss.

Route Changes Due to Mobility: Frequent route interruptions are the outcome of network topology's dynamic nature.

Frequent Network Partitions: Because nodes may move around at random, the network might potentially become divided. The central nodes are particularly affected by this.

Secure Network: It is not an easy process to secure wireless ad hoc networks. Building effective security solutions begins with a comprehensive awareness of the many possible assaults. While many of the same dangers affect wired& wireless networks, ad hoc networks present their own set of problems. Limited to a circular shape by the field's complexity& diversity (different applications have different security procedures). You can't possibly cover all the angles with just one piece. Finding answers to questions about the security of ad hoc networking may be done by reading up on the subject. This list of ad hoc network

security considerations only includes the most crucial ones. Data that has already been modified may be replicated, altered, or deleted as part of an active assault. An ad hoc network may be compromised by certain active assaults. Disclosure, impersonation,& denial-of-service are three different kinds of denial-of-service attacks.

Secure Routing: It is possible for certain nodes to alter routing information, generate fake routing information, or masquerade as other nodes; secure routing systems deal with this threat so that hostile nodes cannot disrupt the normal functioning of a routing protocol.

Cooperation Enforcing: An essential component of any functional ad hoc network is the ability for ad hoc nodes to participate in fundamental network tasks like routing&packet forwarding. In contrast to conventional networks, in an ad hoc network every reachable node is accountable for basic network tasks including administration, packet forwarding,&routing. This discord may be the root cause of some of the ad hoc network-specific security problems. Ad hoc network nodes are unreliable for performing important operations. Since every node in an ad hoc network might double as a router, the routing in such a system is more open to assaults. Additionally, the forwarding mechanism works in tandem.

Intermediary relaying nodes allow communication with nodes that are further apart than one hop. We argue that nodes are misbehaving when they do things that aren't conducive to collaboration. A node's selfish or malicious intentions might cause it to engage in routing forwarding misbehaviours. A malicious node wilfully hinders network operation by refusing to cooperate in order to reject packets. A selfish node won't do anything to hurt other nodes; in fact, it won't even bother asking other nodes to forward packets for it if it doesn't have the resources to do so itself. Although it is not a participant in the network, this node does use it.

Security & Privacy: Among the many issues related to security&privacy in ad hoc networks are:

Ad hoc networks are susceptible to link attacks such active impersonation, message replay,& distortion due to their wireless nature. Passive eavesdropping is another kind of connection attack. An attacker may impersonate a node, introduce fake or altered messages, or tamper with or delete communications to get unauthorised access to a network.

The second reason is that nodes in dangerous locations (like as a battlefield) with limited physical security are at an extremely high risk of being hacked. This is why it's important to consider both external assaults&attacks launched from compromised nodes inside the system.

Additionally, it is dynamic since the network's design&membership are constantly changing (i.e., nodes join&leave the network at a regular interval). Thus, the trust relationship between nodes alters upon discovery of a compromised node.

In an ad hoc network, the number of nodes might go into the thousands. The management of such a massive network necessitates scalable security solutions.

Security Issues in MANET

Mobile Ad-Hoc Networks (MANETs) prioritise security above everything else. There is a solution to fix

security problems that will ensure the availability, secrecy,&integrity of data. There are a number of potential security issues with MANETs, including cooperative algorithms, decentralised administration, an open medium,&a topology that may alter. The MANET's strategy for mitigating security threats has so evolved in response to this.

In recent years, there has been a lot of talk&new ideas about how to make sure that computer networks are secure. Most of the discussions focused on static&wired-based networking. However, mobile Ad-Hoc networking security is an open question. New challenges &issues arise when using routing concepts in light of current&future networking technology. In contrast to conventional wired networks, mobile ad hoc networks function independently. Despite their similarities, the internet &mobile ad hoc networks (MANET) use separate routing protocols. Hosts linked by a static backbone have traditionally used a traditional routing table. This is because, since network topologies are always changing, Ad-Hoc networks can't stay put.

Some of the several reasons routing systems are susceptible to assaults include an absence of infrastructure, unestablished trust connections between nodes, &changeable topology. As of late, researchers have focused on four categories of vulnerabilities: selfishness, dynamic nature, resource restriction, &open network medium. Multiple attack methods can be used to circumvent MANET defences, including passive &active attacks, as well as attacks at the network layer, packet forwarding, routing, &network-layer.

There is no governing body in a MANET; instead, nodes communicate with one another through a system of mutual trust. Consequently, internal attacks on the MANET network are more likely to succeed. Since wireless connections are ubiquitous, they increase the MANET's vulnerability to intrusions, allowing an attacker to see what is currently being sent inside the networkWhen mobile nodes are close enough to a wireless network, they may listen in on conversations&even join the network itself.

ROUTING PROTOCOLS

To transmit and receive data and determine the optimal pathways between any two nodes in a local area network (LAN), routers employ what are known as router communication protocols. Routing algorithms are responsible for determining the optimal route. There is a limit to how many physically connected networks any one router can foresee and connect to. Systems that use algorithms to distribute broadcast messages to neighbouring nodes in a network. Routers may potentially learn about the network's design in this way. Routing protocols were created with routers in mind. Routers using these protocols may find it easier to exchange routing tables, which provide a list of recognised networks. Networks of varying sizes may be managed using the current routing methods. The timely delivery of packets while minimising bandwidth utilisation and expenses is of the utmost importance for routing algorithms in an ad hoc network.

A smaller number of mobile nodes are required for MANETs since they share a single frequency channel. One of the most desirable characteristics of MANET routing systems is their ability to maximise bandwidth efficiency. The protocol intends to improve network performance in response to application needs while minimising network costs. Dense configurations with numerous nodes, frequent connections between them, and frequent topological changes are necessary for a network to serve your application.

Traits of a Routing Protocol

When comparing routing protocols, you may take use of the following features:

Speed of Convergence: In network architecture, the term "speed of convergence" describes the rate at which routers learn each other's routes. Because routing loops can form in inconsistent routing tables in a dynamic network, a quick convergence process is better than a sluggish one.

Scalability:A network's scalability is directly related to the routing protocol utilised during setup. For networks that are always growing, router protocols need to be more scalable.

Class full or Classless (use of VLSM): Since the subnet mask is not provided in the routing headers (VLSM) of class full routing protocols, they do not permit subnet masks of variable length. When making updates, classless routing protocols take the subnet mask into account. In addition to being compatible with VLSM, classless routing protocols also provide a more accurate description of the route.

Resource Usage: When resources are used, for example, random access memory (RAM), CPU,&network bandwidth are all used. The increasing demands for resources need more hardware to handle packet forwarding mechanisms&routing protocols.

Implementation &Maintenance: Administrators of computer networks must be well-versed in the routing protocol for proper installation &ongoing maintenance of their networks.

For nodes to figure out how to get from A to B, an ad hoc routing protocol is required. An individual node may join a network by first broadcasting its presence&then actively seeking out broadcasts from other nodes in the same network. Details on how this finding is put into action are dictated by the various algorithms utilised by the routing protocol of the network.

Routing Protocol Security Flaws

Multiple research initiatives are now active to discover possible security risks and solutions for mobile ad hoc networks, which have lately witnessed an increase in security measures. Using a wireless network leaves you vulnerable to impersonation, denial of service attacks, and eavesdropping. Ad hoc networks rely on the freedom of mobility of nodes. This is one method an adversarial node may acquire access to the network and start using other nodes' resources without their knowledge. It is easy to build inefficient routing, reroute flows, intercept packets that may have been deleted, delayed, or altered, and so on. More research could lead to routing algorithms that address these concerns. Resistance to denial of service attacks and node intrusion detection are two further options.

Finding selfish nodes in MANETs was made possible with the use of the Packet Conservation Monitoring Algorithm (PCMA). In order to manage and prevent data loss, protocols are constantly reorganising. Some examples are Secure Message Transmission (SMT), Secure Single Path (SSP), and others. A threshold-based intrusion detection system was utilised in a multi-hop ad hoc wireless network to avoid message rejection or delays induced by intermediary nodes.

The SAN design may incorporate the link level security protocol (LLSP) (SAHN). They made sure to test all of LLSP's safety measures. We evaluated the predicted timings of several authentication techniques to

demonstrate that LLSP is possible. ' We find that LLSP link-level security service is effective for SAHNs and other ad hoc network types in our preliminary testing.

A practical solution to the security challenges posed by wireless sensor networks has been proposed for the connection layer. A user authentication system that was both lightweight and capable of CBC-X mode encryption and decryption was created by them. Additionally, they have come up with an innovative padding method that prevents the system from sending encrypted and authenticated packets twice. The security steps accounted for zero additional bytes.

Mobile self-organising wireless sensor networks were able to thwart many assaults thanks to their clever security architecture. The effect on security from some unstoppable assaults was also mitigated by this. Lightweight and capable of self-organising mobile wireless sensor networks were the conclusions drawn from their examination of its security architecture.

Security protocols for authentication and packet secrecy in MANETs based on trust Using routing layer data, a mechanism was developed early on in the protocol for detecting and rejecting malicious nodes. Each node had its own trust counter, which made packing easier. By raising or lowering its trust number, a node might be rewarded or punished. Malicious behaviour was indicated if the intermediary node's trust counter value fell below a certain threshold. The CBC-X authentication and encryption technology will be a part of the link-layer security with this protocol version. The results of the simulations demonstrate that this multi-layer security protocol has an impressive packet delivery ratio, low overhead, and low latency.

CONCLUSION

Many security threats can exploit mobile ad hoc networks' (MANETs) inherent decentralization, instability, and self-configuration. Many dangers beset these networks, which are frequently employed in disaster recovery, remote sensing, and military communication, including eavesdropping, unauthorised access, data manipulation, and denial of service. Furthermore, MANETs prioritise energy efficiency because the majority of their linked devices are battery-operated, which significantly affects the network's total performance lifespan. Therefore, minimising energy usage while providing robust security in MANETs is a demanding and extensively studied subject. Finding the sweet spot between these two considerations is the major goal of MANET security energy usage optimisation. Due to the high computational and communication demands of security protocols, mobile devices' battery life may be negatively impacted. However, while reducing energy consumption was the major focus, inadequate security measures might have compromised the network's availability integrity. As a result, it is imperative that the solution be both safe and energy efficient.

References

1. Devi M, Gill NS. Mobile ad hoc networks and routing protocols in IoT enabled. Journal of Engineering and Applied Sciences. 2019; 14(3):802-11.

2. Veeraiah N, Khalaf OI, Prasad CV, Alotaibi Y, Alsufyani A, Alghamdi SA, Alsufyani N. Trust aware secure energy efficient hybrid protocol for manet. IEEE Access. 2021 Aug 30; 9:120996-1005.

3. Usha MS, Ravishankar KC. Implementation of trust-based novel approach for security enhancements in MANETs. SN Computer Science. 2021 Jul; 2(4):1-7.

4. Tripathy BK, Jena SK, Reddy V, Das S, Panda SK. A novel communication framework between MANET and WSN in IoT based smart environment. International Journal of Information Technology. 2021 Jun;13(3):921-31.

5. Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient Authentication Algorithm for Secure Remote Access in Wireless Sensor Networks. Journal of Computer Science Research. 2021 Oct; 3(4): 43-50.

6. Simpson SV, Nagarajan G. A fuzzy based co-operative blackmailing attack detection scheme for edge computing nodes in MANET-IOT environment. Future Generation Computer Systems. 2021 Dec 1;125:544-63.

7. Amutha S, Balasubramanian K. Secured energy optimized Ad hoc on-demand distance vector routing protocol. Computers & Electrical Engineering. 2018 Nov 1;72:766-73.

8. Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. In The Fifth International Conference on Safety and Security with IoT 2023 (pp. 81-99). Springer, Cham.

9. Kowsigan M, Rajeshkumar J, Baranidharan B, Prasath N, Nalini S, Venkatachalam K. A novel intrusion detection system to alleviate the black hole attacks to improve the security and performance of the MANET. Wireless Personal Communications. 2021 Apr 26:1-21.

10. Quy VK, Nam VH, Linh DM, Ban NT, Han ND. A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. Wireless Personal Communications. 2021 Sep;120(1):49-62.

11. Tu J, Tian D, Wang Y. An active-routing authentication scheme in MANET. IEEE Access. 2021 Jan 27; 9:34276-86.

12. Albeshri A. An image hashing-based authentication and secure group communication scheme for IoT-enabled MANETs. Future Internet. 2021 Jun 27; 13(7):166.

13. Nyangaresi VO, Ogundoyin SO. Certificate Based Authentication Scheme for Smart Homes. In 2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

14. Badii C, Bellini P, Difino A, Nesi P. Smart city IoT platform respecting GDPR privacy and security aspects. IEEE Access. 2020 Jan 22; 8:23601-23.

15. Wang D, Bai B, Lei K, Zhao W, Yang Y, Han Z. Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city. IEEE Access. 2019 May 1; 7:54508- 21.

16. Ramphull D, Mungur A, Armoogum S, Pudaruth S. A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. In 2021 5th international conference on intelligent computing and

control systems (ICICCS) 2021 May 6 (pp. 204-211). IEEE.