International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-12, Special Issue-1, March-2024
https://doi.org/10.55524/CSISTW.2024.12.1.58
Computing for Sustainable Innovation: Shaping Tomorrow's World (CSISTW-2024) on 16th-17th February, 2024
Organized by B.N. College of Engineering and Technology, Lucknow, India

Examining MANET routing Protocols for Future Research in Disaster Management

Anuja Priyam[1], and Anita Yadav[2]

[1] Research Scholar, Department of Computer Science & Engineering Harcourt Butler Technical University, Kanpur, India
[2] Professor, Department of Computer Science & Engineering Harcourt Butler Technical University, Kanpur, India

Correspondence should be addressed to Anuja Priyam: anujapriyam@gmail.com

ABSTRACT- A mobile ad hoc network (MANET) is a wireless ad hoc network that is utilized in a specific scenario and is self- managed, self-organized, and non-centralized. To enable effective source-to- destination communication, a routing protocol is required due to the dynamic nature of the network's nodes and architecture. Because of its irregular and inconsistent use, MANET manipulates several spheres of life, including interpersonal communication, real-time information, rescue and emergency operations, network portioning, and catastrophe management. In order to manage time effectively, routing and maintenance are essential components and are being researched for MANET communication. The routing and maintenance process of a MANET, which dynamically changes its structure and nodes to transport data quickly, is the major topic of this study. Route discovery is the MANET research's motivating factor, and a number of methods have been put out for it. Each is expecting more than the other. This comparison study highlights problems with MANET communication maintenance and route discovery, such as which performs better under certain network circumstances. This study examines the literature on MANET route finding and maintenance approaches. Consequently, a comparison of several routing protocol approaches is done. These techniques contain some recommendations for enhancing performance through the use of routing protocols, particularly in the context of disaster management.

Index Terms--Ad hoc networking, Routing Protocols, MANET, and Disaster Management

I. INTRODUCTION

Networks without any infrastructure are known as mobile ad hoc networks or MANETs for short. Every node on a network without a fixed access point has the ability to function as a router. Every node has the freedom to roam around and link to other nodes in any way they choose through dynamic connections.

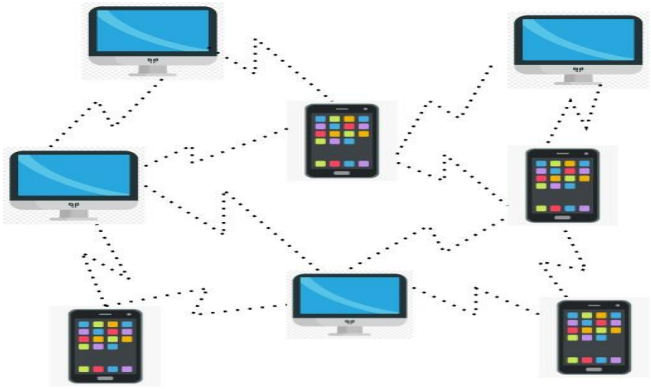

Figure 1: Wireless MANET

The network is organized, managed, and controlled by the terminals. Every terminal in the network has the freedom to roam around. A network like this is shown in Fig. 1.Catastrophes cause substantial disruptions to a community's capacity to manage with its limited resources. A multitude of factors, including technical, man-made, and natural hazards, can combine to cause disasters. Technology has developed at a dizzying rate in recent years. This validates the advancements made recently in fields like computer science, information processing systems, information security, and information technology. In recent years, information technology has advanced more quickly than other industries, especially in the areas of wireless and ad hoc technologies. The emergence of wireless technologies in the 1980s marked the beginning of the wireless network's survival, and since then, it has expanded into all areas of human endeavor [1]. Over the past fourteen years, ad-hoc network technology has made significant progress in the field of research, exhibiting numerous noteworthy achievements and acts that are worthy of praise. Many researchers have looked into this area in an effort to understand more and do more study. Numerous issues and obstacles need to be resolved in this field due to MANET's continuous topology changes. New areas of study for MANETs include energy efficiency, multicasting, clustering, routing and maintenance, and mobility management. Every node in a MANET configures itself and functions as a router [2]. This kind of network is designed for certain extraordinary circumstances, such wars and natural disasters [3].

II. ROUTING PROTOCOLS OF MANET'S

The routing protocols disseminate information on route selection among all nodes in a network and define the route direction across nodes [4]. Three categories of routing protocols exist: proactive routing protocols (PRP). The two types of routing protocols are hybrid (HRP) and reactive (RRP). In Figure 2, many MANET protocol types are shown in a hierarchical taxonomy of routing protocols. Proactive is typically regarded as a table-driven or link-state routing technique. Reactive in the sense of an on-demand routing system or distance vector. A hybrid that combines the two. The authors [4] contrast attempts to enhance certain road design processes and the availability of different road types with simulation studies. However, by looking at several quality of service (QoS) metrics and taking the routing process's quality into account, our analysis enhances the findings of the present study. Along with comparing several crucial elements, it also looks at how the ad hoc network functions and the working media.

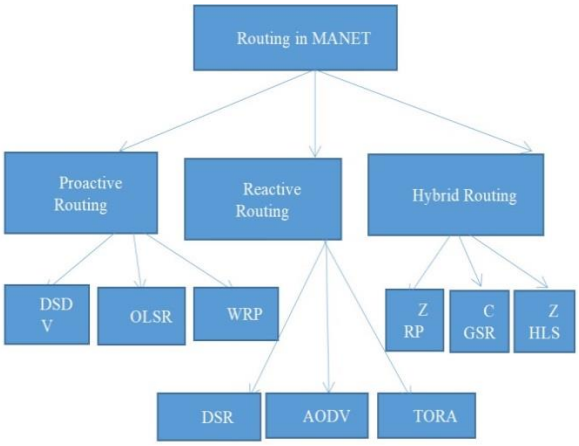

Figure 2: MANET routing protocol classification

To fulfill the program criteria, a number of characteristics or restrictions inside the MANETS QoS management system's operating system must be satisfied between the connection location and the source [5] [6]. Quantity and quality are needed to evaluate a conversion system's quality in order to gauge the routing protocol's overall effectiveness and quality [7].The authors [8] looked at magic in the context of a comparable transportation system in an effort to counteract some of the hoopla in the popular media. However, by examining several QoS measures and making decisions about the system optimization process based on them, our analysis adds to the body of knowledge currently available in this field. It also works with ad hoc networks, investigates how they operate, and compares the different approaches used.Four components of Quality of Service (QoS) are discussed together in the study in [8]: improved bandwidth, packet loss (package delivery rate), latency (path delay), and jitter (time difference). Based on RFC 2501, Table I display the features and attributes of the MANET routing system [7]. Furthermore, several standards make a size, scalability, and loop-free comparison between operating and work routes. Prophylactic and post protocol considerations should be made in light of these characteristics, with reference to the performance standards in this article. Numerous publications evaluate them in comparison.

Table 1. Comparisons between Proactive and Reactive Routing Protocol

Challenges	DSDV	OLSR	AODV	DSR
Issue with throughput	decreased in terms of mobility	superior outcome than that of DSDV	It is low for nodes more than 20.	Diminished rate of growth in mobility
Issue with Load Balance	Inverse	Inverse	Inverse	Inverse
Issues with validity and reliability	Good	Good	Good	Good
Issue of scale control	Inverse	Inverse	Inverse	Inverse
Issue with Control Management	Good	Inverse	Inverse	Inverse

Its primary function is the on-demand creation of routes from a source to a destination. It supports both multicast and unicast routing protocols. The AODV protocol creates routes between nodes upon request from the source node. It is referred to be an on-demand nature procedure as a result. It doesn't generate additional traffic for the purpose of communication along the link [7].Wireless mesh networks employ the DSR routing system. It works in a way similar to the AODV protocol, creating a route based on the request of a transmitting node.DSR operates entirely independently, without the need for administration or pre-existing network infrastructure. The two DSR processes, Route Discovery and Route Maintenance, cooperate to allow nodes to identify and control the primary source to random choice destination routes in the ad hoc network.Every node in TORA has a height parameter that calculates the distance between a source and a destination in terms of hops. The source node makes use of the height parameter to assist itself in choosing

the optimal path to reach the desired destination. To reduce communication overhead, multipath routing is used to destinations without iteration.The hybrid routing technique is dependent on a number of additional activated nodes, and its response to traffic demand is contingent upon traffic volume. By balancing the amount of proactive route information communication with the amount of reactive discovery required, SHARP's automatic method finds a balance point between both proactive and reactive routing.The Hybrid Base Routing Protocol (HRP) is known as Zone Routing Protocol (ZRP). It finds neighbor nodes by utilizing the advantages of proactive routing, and it routes between these neighbor nodes using reactive protocols. Every node in the Zone Routing Protocol (ZRP) has a designated zone, or region, of routing that specifies a range up to the hop at which each node must maintain network availability. Intra-zone routing protocols (IARP) are used for zone (region) inner side routing, and inter-zone routing protocols (IERP) are used for communication with other zones (regions).Pros and drawbacks of Reactive, Proactive and Hybrid protocol are listed in Table 2.

Table 2. Pros and Cons of Routing Protocol

Protocols	Advantages	Disadvantages
Reactive Routing	There is always a road available on demand. no iteration and minimal traffic volume	high incidence of tardiness
Proactive Routing	Reduction of tardiness and Availability of updated data	Overload in heavy traffic
Hybrid Routing	Ideal for a Big Network with Up- to-Date Information	More complicated

In a study published in [9], the routing protocols were reviewed over the course of ten years (2011–2020) in terms of performance parameters. Furthermore, the study grasps the main avenues for further investigation into MANET routing systems.

III. LITERATURE SURVEY

This assignment includes a synopsis of previous studies on wireless mobile ad hoc networks.In mobile Ad-hoc networks, Thakker and Kumar [10] employed an optimal routing technique by contrasting various multiple path routing methods. By contrasting several multiple routing of path security protocols in MANETs, they were able to choose the optimal multi secure routing protocol (MSR). Using routing protocol approaches (AODV, DSR, DSDV, MSR ZRP). Outcome of the exam as determined by NS-3 simulation software.Goswami [11], the author, proposed multiple routing with the AODV reactive base technique to reduce the overall number of routes discovered. There should be another route available. The packets were updated on a regular basis by the author using a Monte Carlo sampling of the whole path between the source and destination nodes. The network's quality is enhanced by the outcomes of simulations.The authors of Thiagarajan and Moorthi's [12] work provided a review of nearly all routing approaches. They then recommended OLSE (optimized link state routing), a dynamic secure routing technique, for the best possible routing performance. Using periodic metrics to route protocols is a proactive and efficient method. Through simulated software, the suggested schemer method yields more optimal results in terms of network throughput and traffic burden.Several patent and security-based techniques are used in this study by Kumar et al. [13] to verify node authentication in the MANET. They offer a protocol for validation and authentication based on the sending and receiving of certificates between nodes; to control the authority and validity of certificates, they employ a digital signature with a hash-style information function. The findings of simulation software demonstrate improved performance in terms of protocol managing throughput, end-to-end delay time, and packet drop ratio when mail function nodes are present in the MANET.In this paper, Sharma et al. [14] employed Hybrid Cryptography Technique (RSA and DES Algorithms) on SAODV. Solely talking about network layer attacks. Sharma et al, additionally, a comparison was made between SAODV (Secure-AODV) and AODV Routing protocol, both of which are based on a model of trust for the MANET and have distinct features including packet delivery and energy efficiency.In this paper, Kamal and Kumar [15] employed a suggested method that ensures data transitions in a highly secure manner using both symmetric and asymmetric cryptography. They used symmetric style cryptography with an encrypted data method. The authors employ asymmetric cryptography by using the information's hash. Make a data or information digital signature. The AES algorithm has been used to verify the suggested technique.Vidya and Shreyas [16] A system based on extremely secure information flow from one point to another was introduced in the study. For increased security, they call the system a hybrid cryptographic system. In an effort to reduce network overload and the high degree of secure packet delivery in the current system, they are utilizing digital signatures in addition to the Data Encryption Standard (DES) technique and the notion of Randomized Signature technique (RSA).In their study, Patil and Bharti [17] employed a dynamic protocol, and there was no high-altitude static design in their system. Every node functioned as the routing mechanism's transmitter. Nodes communicate with one another through a neighboring node. Via the open channel of its access, the MANET can be easily attacked. To improve the system, they employed hybrid approaches with the RSA and AES algorithms. Kushwaha et al.'s [18] suggested method for managing text using encryption is known as the Selective Significant Data Encryption Technique, or SSDE. Only the most important categories of data from the entire message have been processed by SSDE. This method improves standardization while reducing the amount of time spent on encryption. The symmetric key algorithm (SKA) in this

paper, together with BLOWFISH, is the primary aspect that is crucial to the success of encryption.Using the similar technique, Remiya and Lakshmi [19] created the Hierarchical Anonymous Routing Protocol (SHARP). The issue of anonymity between the source and the destination is lessened by the suggested approach. Comparing this policy to other regulatory measures, the security is stronger. An EAACK has been developed by Suvarna et al. [20] for secure data transfer via the MANET network. This paper's primary goals are to handle management concerns, transfer power, and lessen stress. It created a secure delivery manual algorithm technique.To counteract the mouth's failure features, Anand et al.[21] create a dynamic range of motion that offers a robust, resilient, and dependable system in MANET. Analyze performance according to size. Developer network contrasts packing and travel with numerous current technologies, like OCEAN, LARS, LMRSA, and older DSR systems. For the MANET network, Archana et al. [22] employ Secure and Reliable Routing Protocol (SRP) technology, which is an accurate, dependable, and dependable method of ensuring dependable data transfer.A monitoring system has been created by Patel et al. [23] to safeguard mountain anonymity. The SHA-1 algorithm is developed to guard against DOS MITM attacks. A common bath detection system (CBDS) was created by Nachammai and Radha [24] to safeguard data transmission from malicious code contamination. Use powder to detect a black hole attack. The MD5 and RC algorithms are used in the encryption process. physician. A more advanced version of AODV that employs codecs to thwart MANIT pollution attempts was published by Jane and Rajawat [25].A Connection System (ACK) was created by Rasika and Sudier [26] to identify corruption in the MANET network. The finest testing system is ACK. An encryption technique was presented by Al-Mahsoori and Behkar [27] for the transfer of data over networks. The suggested approach shortened the amount of time needed to conceal the data while comparing evidence for DES, AES, and RSA.Bhargavi and Raju [28] created a dependable MANET- based strategy to boost efficiency and package delivery. Doctors Kumar and Narasimha [29] have developed a dependable technique to produce a solution that is safer than MANET. This is accomplished by spreading the private key amongst the nodes and computing the trust value. In this procedure, remove any erroneous holes.Three strategies were developed by Gopalan and Krishnan [30] to determine the optimal and most trustworthy approach: the optimization of the ant coding (ACO) algorithm, the type of understanding, and both. Three different DDoS attack types— HELLO floods, large-scale floods, and harassment attacks were introduced into the OLSR social network by Moudgil and Rana [31]. This system's primary goals are to distinguish between phishing and spam and enhance network performance as a whole.Zafar [32] developed new biometric technologies to raise the MANIT network's security. To determine whether this procedure is effective, compare its results with those of the prior approach. In contrast to the present strategy, Satya et al.'s functional algorithm [33] lowers MANET performance. Performance was assessed in terms of network endurance, PDR, latency, and performance. Novel applications of genetic algorithms for mobile networks' low-power roaming have been demonstrated by Agarwal and Manjlani [34]. If the path fails, this algorithm offers the optimal means of transferring data. Both the guidelines based on budget reduction and locations are used by the writers.In order to address the block-related problem, he developed the BAT algorithm [35].

Table 3. Review At A Glance

Authors	Protocols/Methodology	Issues	Summary
Bairwa[2022]	Redesigned version of the AODV algorithm that is naïve	Immediate	Enhance the quality of service
Kachooei [2021]	The superiority of the CALAR-DD protocol lies in its latency and packet delivery ratio.	Resolving latency issues	Utilizing only AODV and OLSR
Alameri [2020]	DSDV and AODV	Evaluation by comparison of DSDV and AODV	Few metrics for measurement
Mahiddin [2019]	Effective Route Selection Scheme for GWRS	Congestion in the traffic	Adaptable loop determination
Quy et al. [2019]	QAODV	In order to facilitate the multi-media apps	The multimedia applications were handled by the protocol in a flexible and bandwidth-efficient manner.
Thakker et al. [2018]	(IMSRP) Ideal Multi Secure Routing Protocol	Best possible safe routing	Safe Routing
Quy et al. [2018]	An addition to AODV is AERP	In order to meet 5G's high data rates and QoS requirements	It was capable of handling the high data rate requirements of 5G

IV. CONCLUSION AND FUTURE SCOPE

In order to address security concerns in the literature review, we looked at and explored a variety of routing protocols in this study, as well as the challenges they provide with regard to energy, security, routing, and security attacks on the physical structure of layers and data. The different protocols mentioned above are quite effective and beneficial for new researcher that aims to highlight present challenges for further investigation. These days, a plethora of innovative techniques, guidelines, formulas, and protocols are available to achieve routing solutions. Even yet, there are still a lot of unanswered research questions, such what protocol, approach, method, algorithm, or procedure works best in a certain setting. Even

if a lot has been accomplished in this subject thus far, there are still a lot of problems and obstacles to be solved.

REFERENCES

[1] M. Z. Hasan, H. Al-Rizzo, and F. Al-Turjman, ―A survey on multipath routing protocols for QoS assurances in realtime wireless multimedia sensor networks,‖ IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1424-1456, 2017.

[2] H. Zhang and J. Guo, ―Application of manet routing protocol in vehicular ad hoc network based on NS3,‖ in Proc.

[3] 7th IEEE International Conference on Electronics Information and Emergency Communication, 2017, pp. 391-394.

[4] J. K. Er and G. S. Er, ―Review study on MANET routing protocols: Challenges and applications,‖ International Journal of Advanced Research in Computer Science, vol. 8, no. 4, 2017.

[5] M. Bheemalingaiah, M. M. Naidu, D. S. Rao, and P. S. Moorthy, ―Survey of routing protocols, simulation tools and mobility models in mobile ad hoc networks,‖ International Journal of Innovations & Advancement in Computer Science, 2017.

[6] A. Daas, K. Mofleh, E. Jabr, and S. Hamad, ―Comparison between AODV and DSDV routing protocols in mobile Ad-hoc Network (MANET),‖ in Proc. 5th National Symposium on Information Technology: Towards New Smart World, 2015,pp. 1-5.

[7] S. R. Malwe and G. P. Biswas, ―Location aware sectorbased routing in wireless ad hoc networks,‖ in Proc. International Conference on Green Computing and Internet of Things, 2015, pp. 154-159.

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

[9] A. K. Sharma and M. C. Trivedi, ―Performance comparison of AODV, ZRP and AODVDR routing protocols in MANET,‖ in Proc. Second International Conference on Computational Intelligence & Communication Technology, 2016, pp. 231-236.

[10] L. N. Hung and V. K. Quy, ―A review: Performance improvement routing protocols for MANETs,‖ Journal of Communications, vol. 15, no. 5, pp. 439-446, May 2020.

[11] V. M. Thakker, G. M. Reddy, K. V. Kumar, and D. Moses, ―Choosing optimal routing protocol by comparing different multipath routing protocols in mobile Adhoc networks,‖ in Proc. 2nd International Conference on Inventive Systems and Control, 2018, pp. 1284-1290.

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

[13] R. Thiagarajan and M. Moorthi, ―Efficient routing protocols for mobile ad hoc network,‖ in Proc. Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bioinformatics, 2017, pp. 427-431.

[14] U. K. Verma, S. Kumar, and D. Sinha, ―A secure and efficient certificate based authentication protocol for manet,‖ IEEE, 2016.

[15] A. Sharma, D. Bhuriya, and U. Singh, ―Secure data transmission on MANET by hybrid cryptography technique,‖ IEEE, 2015.

[16] R. K. Kapur and S. K. Khatri, ―Secure data transfer in MANET using symmetric and asymmetric cryptography,‖ IEEE, 2015.

[17] S. S. Jathe and V. Dhamdhere, ―Hybrid cryptography for malicious behavior detection and prevention system for MANETs,‖ IEEE, 2015.

[18] T. Patil and B. Jos, ―Improved acknowledgement intrusion detection system in MANETs using hybrid cryptographic Technique,‖ IEEE, 2015.

[19] A. Kushwaha, H. R. Sharma, and A. Ambhaikar, ―A novel selective encryption method for securing text over mobile ad hoc network,‖ ELSEVIER, 2016.

[20] S. Remya and K. S. Lakshmi, ―SHARP: Secured hierarchical anonymous routing protocol for MANETs,‖ in Proc. International Conference on Computer Communication and Informatics, 2015.

[21] D. Suvarna, et al., ―Acknowledgement security for MANET using EAACK,‖ IEEE, 2015.

[22] A. Anand, H. Aggarwal, and R. Rani, ―Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks,‖ IEEE Explore Journal of Communications and Networks, vol. 18, no. 6, December 2016.

[23] A. P. Mandhare and S. V. Kadam, ―E-TWRP: Establishing trustworthy reliable path in mobile adhoc network,‖ IEEE, 2016.

[24] P. Patil, N. Marathe, and V. Jethani, ―Improved ALERT protocol in MANET with strategies to prevent DOS & MITM attacks,‖ in Proc. International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology, 2016.

[25] M. Nachammai and N. Radha, ―Securing data transmission in MANET using an improved cooperative bait detection approach,‖ in Proc. IEEE International Conference on Advances in Computer Applications, 2016

[26] G. Jain and G. S. Rajawat, ―Secure AODV routing protocol based on homographic digital signature,‖ IEEE, 2016.

[27] R. R. Mali and S. T. Bagade, ―Detection of misbehaving node using Secure Acknowledgement in MANET,‖ in Proc. International Conference on Computing, Analytics and Security Trends, 2016, pp. 611-616.

[28] A. M. Swary and S. Baskar, ―Letter to shape encryption for securing MANET routing protocols,‖ in Proc. IEEE International Conference on Computational Intelligence and Computing Research, 2016.

[29] V. S. Bhargavi and S. V. Raju, ―Enhancing security in MANETS through trust-aware routing,‖ in Proc. IEEE WiSPNET 2016 Conference, 2016.

[30] B. Rajkumar and G. Narsimha, ―Trust based certificate revocation for secure routing in MANET,‖ in Proc. 2nd International Conference on Intelligent Computing, Communication & Convergence, 2016.

[31] S. H. Gopalan and R. R. Krishnan, ―Trust based fuzzy aided ACO for optimal routing with security in MANET,‖ Asian Journal of Research in Social Sciences and Humanities, vol. 6, pp. 529-544, 2016.

[32] S. Moudgil and S. Rana, ―A secure & robust scheme to isolate DDoS attacks over MANET,‖ International Journal of Computer Science Issues, vol. 13, no. 3, May 2016.

[33] S. Zafar, ―Biometric signature based approachenhancing security of networks through a novel,‖ International Journal of Wireless Communications and Mobile Computing, vol. 5, no. 1, pp. 1-5, 2017.

[34] Sathya, N. R. Sathiskumar, and K. Ramasamy, ―Effective multicast routing algorithm for MANET,‖ International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 6, March 2017.

[35] S. Rai, R. Boghey, and P. R. Yadav, ―Cluster based energy efficient authentication scheme for secure IDS over MANET,‖

in Proc. 7th International Conference on Communication Systems and Network Technologies, 2017, pp. 200-205.

[36] B. R. Jeetha and K. Sivakamipriya, ―Secure routing and detection of hybrid attacks in MANET,‖ International Journal of Innovative Research in Computer and Communication Engineering, vol. 5, no. 2, February 2017.