JCBI
Journal of Computing & Biomedical Informatics Volume 03 Issue 02
ISSN: 2710 - 1606 2022

Research Article
https://doi.org/10.56979/302/2022/51

Analysis Study of Routing Protocols in MANET for Disaster Management

Abdul Majid Soomro[1*], Muhammad Saim[2], Awad bin Naeem[3], Muhammad Asad Soomro[4], Imran Khurshid[3], and Muhammad Ashad Baloch[3]

[1]Department of Computer Science (FSKTM), University Tun Hussein Onn Malaysia, Malaysia.
[2]Department of Computer Science, Riphah International University Lahore Campus, Lahore, Pakistan.
[3]Department of Computer Science, National College of Business Administration &Economics, Multan, Pakistan.
[4]Department of Computer Science, Lahore University of Management Sciences, Lahore, Pakistan.
[*]Corresponding Author: Abdul Majid Soomro. Email: gi180004@siswa.uthm.edu.my

Received: April 21, 2022 **Accepted:** September 10, 2022 **Published:** September 27, 2022

Abstract: A unique instance of a wireless ad hoc network that is non-centralized, self-organized, and self-managed is known as a mobile ad hoc network(MANET). MANET used in different areas of life like a rescue operation, real-time information, interpersonal communication, information sharing and network portioning. MANET has dynamic change in nature of both its topology and nodes in order to deliver data quickly. Due to Mobility nature in nodes, there is a lot of chances of routing design issues between the nodes. There is a list of routing protocol each one has its special characteristic in Specific areas have been designed and compared their attributes on different parameters. This report gives a clear picture and a comparison of various MANET routing techniques with their limitation in ad-hoc routing network.

Keywords: MANET; Routing Protocol; Mobility; Ad-Hoc Networking; Topology.

1. Introduction

In recent years, technology has moved incredibly quickly. This attests to the current successes in a variety of sectors, including information security, information processing systems, and information technology and computer science. Information technology has made more advancements recently than in other sectors, particularly in wireless and ad-hoc technologies. The development of wireless technologies in the 1980s marked the beginning of wireless networks, which later opened new doors in every aspect of human life. Ad-hoc network technology has made a number of commendable contributions and exceptional advancements in the field of research during the last 14 years. For the objective of conducting more extensive research and learning, many researchers looked into this subject. A lot of problems and addressable challenge exist in this area because of continues topology change in MANET. New areas in recent research of MANETs are optimal routing, data management, energy efficiency, multicasting, clustering, and mobility management. Without infrastructure networks is called as Mobile Ad-hoc Networks (MANET) [1]. In networks without a fixed access point, each node can serve as a router. All nodes have unrestricted freedom of movement and are joined to one another dynamically and arbitrarily. The entire network must be controlled, managed, and organized by the terminals themselves. The entire network is mobile, and each terminal is free to roam around [2].

MANET (Mobile Ad- Hoc Network) is most popular without infrastructure wireless network where each node behaves like a router and do self-configuration. Such kind of network formed for particular special situation and purpose and wrap out after achievements of its purpose [3]. Wireless links are using in MANET for its self-configuration. MANET not rely on any fixed infrastructure such as base station. Instead, the dependency of mobile nodes exists between each other to keep the network stay in connec-

tion. In MANET movement of nodes or devices free in any direction, it often changes the link between nodes. Maintenance of traffic through nodes make the better performance of the network. Due to which behave of each node is like a router [4].In disaster management communication different routing protocols are use, so our main problem is that in disaster commination how we control and manage different routing protocols. Second in disaster situation we want to communicate in efficient way so how many pro-active and re- active are used. Third in disaster situation how we get better efficiency.

This work is organized as follows: Section 2 contains the literature review. Section 3 presents the methodology of the study. Section 4 discusses the results. In last, conclusion and future work is described in section.

2. Literature Review

In this research study, a quick description of prior research efforts on Wireless Mobile Ad-hoc Net-work. By contrasting various multiple path routing protocols in mobile Ad-hoc networks, Thakker and Kumar [11] used an ideal routing protocol. Through evaluation of many multiple routing of path security protocols in MANET, they chose an appropriate Multi Secure Routing Protocol (MSR). Here, writer's use (AODV, DSR, DSDV, MSR, ZRP) routing protocol strategies to compare and explore various proactive, reactive, and hybrid routing types. Result acquired following the test with simulated software (NS-3). In order to reduce the total number of route discoveries, Goswami [12], the author, offered multiple routing utilizing the AODV reactive base technique. One route should be there as an alternate path. The author used a Monte Carlo method to update packets on a regular basis using a sample of the full path between the source and destination nodes. Simulated outcomes raise the network's overall quality. With the aid of numerous paths and the (ECC) el-liptic curve cryptographic technology, Sultana and Ahmed discussed the AOMDV reactive Protocol in their paper [13]. This protocol is an extension of AODV that provides secure data packet transfer against the threat of black holes. Simulated software like NS-2.35 maintain configuration results. Such simulated type software can be used in different environments as parametric way. A dynamic secure routing technique called OLSE (optimized link state routing for optimal routing performance) was proposed by Thiagarajan and Moorthi in their paper [14]. It is an efficient proactive method of routing protocols through periodic metrics, and it offers better optimal results in overburden of traffic in the network, throughput, through simulated software. In this paper by Utpal Kumar et al. [15], many potent and security-based approaches are used to check node authentication in the MANET. They provide a protocol for validation and authentication on the basis of certificate sending and receiving between the nodes, for this purpose they use a digital signature with a hash style of information functions to manage the authority and validity of certificates. Simulation software results proofs the improved performance in terms of the throughput of protocol controlling, its end to end delay time and drop ratio of packet in the presence of mail function nodes in MANET. The Hybrid-Cryptography-Technique (DES, RSA Algorithms) on SAODV was used in this paper by Ashish Sharma et al. Only discussion concerning attacks on the network layer. Authors. Also compared AODV Ad-Hoc network On Demand Vector Routing protocol (AODV)) with SAODV (Secure Ad-hoc on demand routing protocol) based on a trust model for the MANET with diverse parameters like packet delivery, energy efficiency. Raj Kamal and Sunil Kumar [17] in This Paper Authors employed a recommended technique to make sure transition of data in extremely secure manner using symmetric way and asymmetric way of cryptography. They used encrypted technique of data using the symmetric style of cryptography. Authors use the asymmetric cryptography way from the Hash of the information. Make a data or piece of information's digital signature. Proposed approach has been validated by AES algorithm. Shreyas and Vidya [18] in paper they introduced a system, that base on highly secure information transition from one point to other point. They refer the system as Hybrid Cryptographic system for better security. they tried to minimize network over burden, secure delivery of packet percentage that is at high level in existing system, they are using the idea of (RSA) , Data Encryption standard(DES) along with the usage of a digital type signature algorithm. Ms.Trupti Patil and Dr.Bharti [19] in the paper they used dynamic nature of topology and system did not have high altitude static type architecture. Each node worked as the transmitter of routing mechanism. Communication between nodes occur through a node at its neighbor. It is easy way to attack the MANET through open medium of its access. They used RSA and AES algorithm through hybrid techniques to make the system more admirable.

For the management of text using encryption, Ajay Kushwaha et al. [20] presented the Selective Significant Data Encryption (SSDE) approach. From the entire message, just the most important type of data was worked on for SSDE. By using this method, encryption time is used as little as possible, and standardization is improved. In the study, the symmetric key algorithm (SKA) and BLOWFISH are the primary factors that play a crucial part in the accomplishment of encryption. To reduce the Quality of service-based issues in MANET, Sherin Zafar et al. [21] offer an optimal genetic stowed biometric approach. Their proposed method uses an algorithm that uses both iris biometrics and genetics. A cluster-based routing protocol called SHARP (Secure Hierarchical Anonymous Routing Protocol) was developed by Remya and Lakshmi [22]. Anonymity between source and destination nodes is a problem that is lessened by the provided solution. Compared to other routing protocols, this protocol offers higher safety. For secure data transfer in MANET, Deore Suvarna et al. [23] created the Enhanced Adaptive Acknowledgement (EAACK) method. This paper's major goal is to reduce the issue of bad behavior, finite transmission power, and receiver collision.In order to create a secure, legitimate, and reliable routing strategy in MANETs to tackle node misbehavior, Anjali Annand et al. [24] proposed a distributed dynamic model. Utilize the overhead to assess performance. The network's throughput and packet movement. Authors compared many modern techniques, including LMRSA, LARS, OCEAN, and the conventional DSR methodology suggested a cluster algorithm with a digital signature for secure transmission. Anjali Annand et al [24] suggested a Distributed Dynamic Model in order to make secure, valid and reliable Routing technique in MANETs to handle misbehavior nature of nodes in a network system. Evaluate the performance through overhead. Throughput and packet transition over the network. Authors compared with different current technique such as LMRSA, LARS, OCEAN, and traditional DSR protocol. Archana et al [25] Maintain valid, trusty and reliable Path in MANET with the help of SRP technique (safe, Reliable Routing Protocol) which manage safe and sound path of route with reliability for transmission of data. Priyanka Patil et al [26] develop the ALERT protocol to safeguard the MANET's anonymity. MITM and Dos attacks are already protected by the SHA-1 algorithm. For data transport with security from malicious node indication, Nachammai and Radha [27] proposed a cooperative bait detection system (CBDS). The attacks from black holes and grey holes can be distinguished. The algorithms used for encryption are RC$ and MD5. Garima Jain, In order to protect MANET against pollution attacks, Dr. Gajendrasingh Rajawat [28] proposed an improved version of AODV. This version uses homographic encryption. The Secure Acknowledgement (ACK) System was introduced by Rasika and Sudhir [29] as a means of identifying node misbehavior in MANET. A approach that works best is one called ACK. Letter Shape-based encryption was provided by A. Maheswary and Baskar [30] in order to transport data via networks. The proposed Method-ology takes less time to encrypt the data when compared to DES, AES, and RSA, which give proof. It is protected from a medium-level attack. A trust-based, full-security-based routing scheme for MANET was suggested by V. Sesha Bhargavi and S. Viswanadha Raju [31] to get better packet delivery percentage and throughput results.. A Trust-based threshold revocation mechanism for increasing the security of routing in MANET has been devised by Banoth Rajkumar and Dr. G. Narsimha [32]. This has been accomplished through the calculation of trust values and the distribution of a secret key among the nodes. Eliminate the nodes that act badly as a result of this system. The doctors S. Harihara Gopalan and R. Radha Krishnan [33] Three methods—a trust aware model, fuzzy aided, and the Ant Colony Optimization (ACO) algorithm—were proposed to find the best routing with excellent security. Suveg Moudgil, Three types of Dos attacks (Spoofing assault, Route flooding, and HELLO flooding) were added to the OLSR reactive routing protocol by Dr. Sanjeev Rana [34]. The system's main objective is to differentiate between these flooding and spoofing attacks while also enhancing general network performance.. A cutting-edge intrusion detection system was created by Rohit Chourasia and Rajesh Kumar Boghey [35] to recognize when ping packets are dropped in error and select another, more secure path for data transmission. Performance indicators for the suggested system include the packet delivery ratio, routing overhead, throughput, and average latency.. In order to improve the security of the network in MANET, Sherin Zafar [36] created a revolutionary biometric signature type technique. To implement these methods, MATLAB is needed. To evaluate the approach's dependability, performance is compared with analogous earlier strategies. To save energy in MANET, P. Sathya et al. [37] developed a multicast routing method in comparison to the current protocol. Performance evaluation metrics included throughput, latency, PDR, and network longevity.

An innovative method using a genetic algorithm for energy-efficient routing in mobile ad hoc networks has been reported by Neha Agarwal and Neeraj Manglani [38]. When one path fails, this algorithm offers the best option for transmitting data. The proposed GA-based routing and conventional flooding-based routing were contrasted by the author. Rohit Chourasia, Rajesh Kumar Boghey [39] built a cutting-edge intrusion detection system that recognizes the improper behavior of packet dropping and prefers another path for data transmission. The proposed system's efficiency is measured in terms of the packet delivery ratio, routing overhead, throughput, and average delay in routing. Dr.B.RosilineJeetha, K.Sivakamipriya [40] developed a zone-based routing protocol for MANET's secure routing. In order to address cluster-related issues, he proposed the BAT method. Table 1 illustrates how existing protocols and techniques should be used.

Table 1. Explain Protocols and Technique

Author /year	Protocol/Technique used	Issues	Limitation/ Advantages
Bairwa in 2022	Naive revamped variant of the AODV algorithm	Emergency	improve the QoS
Kachooei in 2021	In terms of latency and packet delivery ratio, the CALAR-DD protocol is superior.	Latency issue solution	Only OLSR and AODV in use
Alameri in 2020	AODV , DSDV	Comparative analysis	Limited measurement metrics
Nor Aida Mahiddin in 2019	Efficient GWRS Route selection Scheme	Traffic congestion	Flexible determination of loop
Thakker, and kumar in 2018	Ideal Multi Secure Routing Protocol(IMSRP)	Optimal secure routing	secure routing
Rohit Chourasia and Rajesh in 2017	Intrusion detection and Prevention System	Misbehave of packet dropping	Improved data receiving minimize data droping
Rajesh Kumar Boghey in 2017	prevention system	packet dropping	Minimizes dropping data
Sherin Zafar in 2017	Iris cryptography technique	DoS	FRR= 0% with accuracy 100 percent
P.sathya et al in 2017	PUMA(protocol for unified Multicasting Through Announcement)	Mail functioning of nodes	Routing Over is extremely minimized throughput increased and network achieve high level life time

Dr.B.Rosiline et al in 2017	(AOMDV)Ad-hoc on demand Multipath distance vector(AOMDV)Hybrid BAT Algorithm	Hybrid Attacks	reduce hot spot Problem with routing overheads about 5-10 percent
Utpal Kumar et al,, in 2016	authentication protocol with digital signature in a hash data certificates	delay and dropping of packets	Malicious node identification
AnjaliAnand et al in 2016	DSR Protocol Dynamic Chips Allotment (DCA) Mechanism	Misbehavior of nodes	Secure Routing Improve the network performance.
Priyanka and VimlaJethani in 2016	ALERT protocol SHA-1 algorithm	DoS Attack	100 percent delivery of packet
Nachammai. M, Dr. N. Radha, Rasika R. Mali, and Sudhir T in 2016	Cooperative bait detection Secure ACK Algorithm	Gray hole black Misbehavior of Nodes	routing path can be Highly secured
Garima Jain and Dr.Gajendra singhRajawat in 2016	HAODV protocol Homographic Encryption Scheme	Pollution Attack	40% greater than existing protocol in throughput
A.Maheswary and Dr.S.Baskar in 2016	Letter-Shape Encryption	Man in middle	Use minimum timespan for encryption and decryption
Suveg Moudgil and Dr. Sanjeev in 2016	OLSR routing protocol	Flooding and Spoofing attack	Reduce end to end delay
Rasika and Sudhir in 2016	Secure ACK Algorithm	Misbehavior of	Highly Security in
Ajay Kushwaha et al. 2016	Text data encryption with Selective significant data encryption (SSDE) and blowfish algorithm	Minimize the encrypted data timing and control overhead of network and enhancement in performance	Significant data
V.Sesha Bhargavi and S.Viswanadha Raju in 2016	Trust Aware Routing Protocol(TARP)	worm hole and black hole Attacks	Maximum Packet delivery Ratio and Throughput
Banoth Rajkumar and Dr.G.Narsimha in 2016	Trust based threshold revocation method(TTRM)	Malicious types of nodes	Elimination of node misbehavior

S. Harihara Gopalan and Dr. R Radha Krishnan in 2016	AODV Fuzzy Integrated Ant Colony Optimization	Control End-to-end delay, bandwidth, network lifetime and energy	Improve Packet delivery ratio.
Archana and Sujata in 2016	SRP (Secure and Reliable) routing protocol delivery ratio	Packet loss Break routes	Increase packet
Neha Agarwal and Neeraj Manglani in 2015	Energy efficient routing protocol Genetic algorithms	Path fails	Increases the overall lifespan of the network
SherinZafar, M.K.Soni, M.M.S Beg, 2015	Ad-hoc On-demand Distance Vector Routing (AODV) Genetic Algorithm Iris	Quality of Service(QoS) based attacks	Accuracy=0.98889
Remya S, Lakshmi K S in 2015	Secured Hierarchical Anonymous Routing Protocol (SHARP) RSA	Anonymity	High Security
Deore Suvarna et al, 2015	Enhanced Adaptive Acknowledgement (EAACK) Digital signature with clustering algorithm	Malicious behavior, finite transmission Range and receiver Collisions.	Secure routing
Ashish Sharma et al..2015)	SAODV (Secure Ad-hoc on demand routing technique Hybrid Cryptography ,DES, RSA	Active Attack on network layer	High Packet Delivery ratio, throughput
Raj Kamal and Sunil Kumar in 2015	Ad-hoc on Demand Distance Vector Routing(AODV) Symmetric, Cryptography and Asymmetric technique	Modification ,Snooping and Fabrication Attack	Confidential information integrity
Shreyas and Vidya in 2015	Hybrid Cryptography , RSA , Data Encryption standard techniques(DES) with digital signature	Packet of data delivery.	Efficient packet delivery and network overhead
Ms.Trupti Patil and Dr.Bharti, in 2015	RSA and AES Hybrid Routing technique with Cryptography	Network Security	security and overhead of network

3. Materials and Methods

Routing protocol routes show the direction of a route between nodes and provide information to help network nodes choose a route. [5]. Proactive, reactive, and hybrid routing protocols are the three different categories of routing protocols. Proactive is essentially thought of as the table-driven routes of protocol, Reactive is thought of as on-demand routing of protocol, and Hybrid has both proactive and reactive routing protocols advantages.

3.1. Proactive Routing Protocol (PRP)

These routing protocols make use of routing algorithms that constantly send related data to neighboring nodes. Every node in the proactive-routing-protocol (PRP) has a table that manages ongoing change [6]. DSDV and WRP are two prominent instances of proactive routing protocols (PRP)..

3.1.1. Destination Sequence Distance Vector Routing Protocol (DSDV)

Destination Sequence Distance Vector Routing (DSDV) is proactive vector routing protocol using hop by hop technique [6]. It is one of the proactive protocol where each node has a table that indicate information about switching of next-node and maintain number of movements to every accessible destination. It has periodic broadcast nature of reforms in routing in order to make the routing table active and streamline, revise it all the time. Benefits of DSDV are its reactions during the topology changes are fast and its freeness about loop structure. The main issue that we can say demerit of DSDV not maintains network over crowdedness because not use routing information properly.

3.1.2 Link-State-Routing-Protocol (LSR)

LSR is another main proactive routing protocol (PRP). The main aim of this protocol is to search a route on the basis of current active situation. It reforms of Dijkstra's SPF scheming algorithm, where in entire network each node has desirable information about view of topology. In the Network each node has fresh knowledge about topology information road map that reforms itself frequently and creates a Link State Packet (LSP) in connection to other state through direct link and broadcast all information to nearest nodes [7].

3.1.3 Wireless Routing Protocol (WRP)

Four tables perform Maintains of each node which are in the form for the purpose of routing, distance tables, routing tables, link-cost tables, and message retransmission lists are used. In WRP, updating of messages are performed through the neighbors of a node.

Table 2. Some Proactive Routing Protocol (PRP) comparison.

Challenges	DSDV	OLSR
Balance of Load Issue	Negative	Negative
Reliability and validity issue	Positive	Positive
Throughput issue	Reduced with mobility	Better result as compare to DSDV
Scale controlling issue	Negative	Negative
Control Management Issue	Positive	Negative

3.2 Reactive Routing protocol (RRP)

A route can only be designed in Reactive Routing (RRP) when it is necessary in order to meet the primary aim. The method for distance-vector routing only manages the path to a specific destination station when a node needs and requests it. The proactive routing protocol (PRP) has several challenges, and the major goal of these protocols is to reduce the amount of traffic that needs to be routed. Table 02 compares the proactive routing protocols.

3.2.1 Ad-Hoc On-Demand Distance Vector Routing Protocol (AODV)

One of the reactive-routing-protocols is called Ad-hoc On-Demand Distance Vector (AODV) (RRP). It is specifically created for mobile ad-hoc networks where wireless technology is used for work. Its primary function is the on-demand creation of routes from source to destination, and it supports both unicast and multicast routing protocols. The AODV protocol creates routes between nodes in response to source node requests. As a result, it was referred to as an on-demand nature technique. It serves the objective of communication without adding more traffic to the link [8].

3.2.2 Dynamic-Source-Routing Protocol (DSR)

This routing protocol used for wireless mesh networks. It is quite same like AODV protocol in the manner it develops a route on demand base due to request of transmitting node. DSR has fully self-maintain and self-organized nature, without any administration and network infrastructure existing network. Route Discovery and Route Maintenance are two mechanisms of DSR, which work together to give permission to nodes to find out and manage main source to random choice destinations route in the ad- hoc network.

3.2.3 Temporally-Ordered-Routing-Algorithm (TORA)

In TORA each node uses a parameter altitude which measures the distance in the form of hops from source to destination. The source node utilizes the height altitude to provide help to the source node in selection criteria of the best route in order to achieve the required destination. It is without iteration multipath routing to destinations in order to minimize communication overhead, Table 03 below shows the reactive routing protocol comparison.

Table 3. Some Reactive Routing Protocol (RRP) comparison

Challenges	AODV	DSR
Complexity Issues	Moderate	Moderate
Balance of Load Issue	Negative	Negative
Reliability and validity issue	Positive	Positive
Configuration of routes	After use delete the route give information to source	After use delete the route give information to source
Throughput issue	For above 20 nodes it islow	Reduction on increment in mobility
Scale controlling issue	Negative	Negative
Control Management Issue	Negative	Negative
Management of routes	Through Table	Through cache
Loop issues	Free	Free
Delete Route Information timing	Positive	Negative
Multi Routing System support	Negative	Positive
Types of protocol	Distance base routing	Source base routing
Burden on Route	Low	Moderate

3.3 Hybrid Routing Protocol (HRP)

A protocol that combines the advantages of proactive routing protocol (PRP) and reactive routing protocol is known as hybrid routing protocol (HRP) (RRP). The primary advantage is that the routing initially handles some proactive routes before presenting its demand request from highly activated nodes using reactive routing strategies. [9]. Demerits of hybrid routing technique is, it depends on a amount of other activated nodes and its reaction according to the demand of traffic depends upon traffic volume.

3.3.1 Sharp Hybrid Adaptive Routing Protocol (SHARP)

SHARP has automatic process of finding balance point between both proactive and reactive routing protocol through adjustment the proportion of route information that is communicated proactively versus that which must be discovered reactively

3.3.2 Zone-Routing Protocol (ZRP)

It is hybrid base routing protocol (HRP). It uses benefits of proactive routing in the discovery of neighbor nodes and it use Reactive Protocols for routing between these neighbor nodes. In Zone-routing protocol (ZRP) each node has their own zone (region) of routing that mentation a range as far as hop where every node needs to maintain network availability (Sharma and Trivedi in 2016). Zone (region) inner side of routing is performed through Intra-zone routing protocols (IARP) and to communicate that occur with various other zone (region) is performed through Inter-zone routing protocols (IERP). Table 04 shows the information about merits and demerits of routing protocol.

Table 4. Have Information about Merits and Demerits of Routing Protocol.

Protocol	Merits	Demerits
Proactive Routing Protocol	Lateness reduce and have update information	Over burden in traffic high
Reactive Routing Protocol	On demand path is always available no iteration with low burden of traffic	High rate of late-ness
Hybrid Routing Protocol	Suitable for a Large network with timely information	More complex

4. Results and Discussions

In Table 5, various forms of routing protocols, including proactive-routing protocols (PRP), reactive-routing protocols (RRP), and hybrid-routing protocols (HRP), are compared. Different approaches used in routing such as scalability, energy efficiency, Network overhead and throughput, Latency issues, Power requirement, Storage requirement and Bandwidth requirement issues.

Table 5. Comparative Analysis of Different Types of Routing Protocols

Main Features	Proactive Protocol	Reactive protocol	Hybrid Protocol
Routing issues for Acquis ion	Table Driven base	On demand base	Both combine
Scalability Issues	Less Level	Not accurate for large network	Have best design for large network
Latency issues	Less due to use of table for routing	Its High Peak due flooding environment	Less inside Zone High outside zone
Band width Re-quirement Issues	High	Less	Medium

Periodically updating	Needed when change occur in network topology	Not needed	Needed
Routing Overhead Issues	High	Less	Medium
Power Requirement Issues	High	Less	Medium
Storage requirement issues	High	Less	Medium
Mobile nature of nodes	Updating perform periodically	Maintain Route on demand basis	Combine both together
Routing Information issues	High level Availability	Availability on requirement	Combine both together

From table no 5, it is clear through comparative analysis of routing approaches like proactive technique, reactive technique [10] and hybrid approach. Table Compare and evaluate the result-oriented performance of proactive and reactive routing protocols in MANET. In discussion, Reactive on-demand routing protocols performance is more acceptable under data management, energy efficiency, routing, bandwidth management issues and it provides less network overhead environment as compare among routing techniques.

In the literature review, we studied and discussed different kinds of routing protocol and their issues related to security, energy, routing, attacks on security on the physical structure of data and layers and also try to resolve e-security issues. Different kind of routing protocols are discussed above are very useful and efficient for new research work to recognize current challenges for further research. Several different kinds of new techniques, rules, and algorithms, protocols are proposed for obtaining routing solution nowadays but still after a lot of achievement there are many research issue problems like which kind of protocol, technique or method, algorithm or procedure shows the best performance in which environment. Till yet a lot of contribution has done in this area but still, a lot of problems and issues need to be address. MANET networking is most significant and necessary technique that support upcoming computing scheming mechanism. Nowadays, MANET has becalmed interesting research article and a lot of research projects and issues employed by academic-related and companies related all over the world.

5. Conclusion and Future Work

In this paper, study compared diverse routing protocol techniques and highlight different problems such techniques used. We believe that this can provide further direction to researchers in improving routing performance. Study plan in future to compare other Routing techniques on the basis of network overhead

Funding: No funding was received.

Data Availability Statement: The authors declare that all data supporting the findings of this study are available within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Soomro, A. M., Fudzee, M. F. B. M., Hussain, M., Saim, H. M., Zaman, G., Atta-ur-Rahman, H. A., & Nabil, M. (2022). Comparative Review of Routing Protocols in MANET for Future Research in Disaster Management. Journal of Communications, 17(9).
2. Alameri, I. A., &Komarkova, J. (2020, June). A multi-parameter comparative study of manet routing protocols. In 2020 15th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6). IEEE.
3. Kachooei, M. A., Hendessi, F., Ghahfarokhi, B. S., &Nozari, M. An OLSR-based Geocast Routing Protocol for Vehicular Ad Hoc Networks. Peer-to-Peer Networking and Applications, (2021), pp.1-21.
4. Kaur, J., & Singh, G. (2017). Review study on MANET Routing Protocols: Challenges and Applications. International Journal of Advanced Research in Computer Science, 8(4).
5. Bheemalingaiah, M., Naidu, M., Rao, D. S., & Moorthy, P. S. (2017). Survey of Routing Protocols, Simulation Tools and Mobility Models in Mobile Adhoc Networks. International Journal of Innovations & Advancement in Computer Science (IJIACS) ISSN (2017), 2347-8616.
6. Daas, A., Mofleh, K., Jabr, E., & Hamad, S. (2015, February). Comparison between AODV and DSDV routing protocols in mobile Ad-hoc Network (MANET). In 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW) (pp. 1-5). IEEE.
7. Malwe, S. R., & Biswas, G. P. (2015, October). Location aware sector-based routing in wireless ad hoc networks. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 154-159). IEEE.
8. Goswami, M. M. (2017, March). AODV based adaptive distributed hybrid multipath routing for mobile AdHoc network. In 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 410-414). IEEE..
9. Sharma, A. K., & Trivedi, M. C. (2016, February). Performance comparison of AODV, ZRP and AODVDR routing protocols in MANET. In 2016 Second International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 231-236). IEEE.
10. Bai, Y., Mai, Y., & Wang, N. (2017, April). Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs. In 2017 Wireless Telecommunications Symposium (WTS) (pp. 1-5). IEEE.
11. Thakker, V. M., Reddy, G. M., Kumar, K. V., & Moses, D. (2018, January). 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.
12. Goswami, M. M. (2017, March). AODV based adaptive distributed hybrid multipath routing for mobile AdHoc network. In 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT) (pp. 410-414). IEEE.
13. Sultana, J., & Ahmed, T. (2017, February). Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography. In 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE) (pp. 539-543). IEEE.
14. Thiagarajan, R., &Moorthi, M.Efficient routing protocols for mobile ad hoc network. In Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), 2017 Third International Conference on (2017, February). (pp. 427-431). IEEE.
15. Verma, U. K., Kumar, S., & Sinha, D. (2016, March). A secure and efficient certificate based authentication protocol for MANET. In 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) (pp. 1-7). IEEE.
16. Sharma, A., Bhuriya, D., & Singh, U. (2015, September). Secure data transmission on MANET by hybrid cryptography technique. In 2015 International Conference on Computer, Communication and Control (IC4) (pp. 1-6). IEEE.
17. Kapur, R. K., & Khatri, S. K. (2015, September). Secure data transfer in MANET using symmetric and asymmetric cryptography. In 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions) (pp. 1-5). IEEE.
18. Jathe, S. S., &Dhamdhere, V. (2015, December). Hybrid cryptography for malicious behavior detection and prevention system for MANETs. In 2015 International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 1108-1114). IEEE.
19. Patil, T., & Joshi, B. (2015, October). Improved acknowledgement intrusion detection system in MANETs using hybrid cryptographic technique. In 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 636-641). IEEE.
20. Kushwaha, A., Sharma, H. R., &Ambhaikar, A. (2016). A novel selective encryption method for securing text over mobile ad hoc network. Procedia Computer Science, 79, 16-23.
21. Zafar, S., Soni, M. K., & Beg, M. S. (2015). An optimized genetic stowed biometric approach to potent QOS in MANET. Procedia computer science, 62, 410-418.
22. Suvarna, D., Pallavi, E., Sumitra, L., Chhaya, D., &Korade, M. (2015, October). Acknowledgement security for MANET using EAACK. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 671-678). IEEE.
23. Anand, A., Aggarwal, H., & Rani, R. (2016). Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks. Journal of Communications and Networks, 18(6), 938-947.
24. Mandhare, A. P., & Kadam, S. V. (2016, October). E-TWRP: Establishing trust worthy reliable path in Mobile Adhoc Network. In 2016 International Conference on Emerging Technological Trends (ICETT) (pp. 1-5). IEEE.

25. Patil, P., Marathe, N., &Jethani, V. (2016, September). Improved ALERT protocol in MANET with strategies to prevent DOS & MITM attacks. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) (pp. 372-377). IEEE.
26. Nachammai, M., & Radha, N. (2016, October). Securing data transmission in MANET using an improved cooperative bait detection approach. In 2016 IEEE International Conference on Advances in Computer Applications (ICACA) (pp. 292-297). IEEE.
27. Jain, G., &Rajawat, G. S. (2016, December). Secure AODV routing protocol based on homomorphic digital signature. In 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I) (pp. 307-311). IEEE.
28. Mali, R. R., & Bagade, S. T. (2016, December). Detection of misbehaving node using Secure Acknowledgement in MANET. In 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 611-616). IEEE.
29. Maheswary, A., & Baskar, S. (2016, December). Letter to shape encryption for securing MANET routing protocols. In 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-4). IEEE.
30. Bhargavi, V. S., & Raju, S. V. (2016, March). Enhancing security in MANETS through trust-aware routing. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 1940-1943). IEEE.
31. Rajkumar, B., & Narsimha, G. (2016). Trust based certificate revocation for secure routing in MANET. Procedia Computer Science, 92, 431-441.
32. Gopalan, S. H., & Krishnan, R. R. (2016). Trust based fuzzy aided ACO for optimal routing with security in MANET. Asian Journal of Research in Social Sciences and Humanities, 6(cs1), 529-544.
33. Moudgil, S., & Rana, S. (2016). A secure & robust scheme to isolate DDoS attacks over MANET. International Journal of Computer Science Issues (IJCSI), 13(3), 31.
34. Chourasia, R., &Boghey, R. K. (2017, January). Novel IDS security against attacker routing misbehavior of packet dropping in MANET. In 2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence (pp. 456-460). IEEE.
35. Zafar, S. (2017). Enhancing Security of Networks Through a Novel Biometric Signature Based Approach. International Journal of Wireless Communications and Mobile Computing, 5(1), 1-5.
36. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering ,Vol. 6, Special Issue 1, March 2017.
37. Rai, S., Boghey, R., & Yadav, P. R. (2017, November). Cluster based energy efficient authentication scheme for secure IDS over MANET. In 2017 7th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 200-205). IEEE.
38. Agarwal, N., &Manglani, N. (2015). A New Approach for Energy Efficient Routing in MANETs Using Multi Objective Genetic Algorithm. International Journal of Science, Engineering and Technology Research (IJSETR), 4(6), 1780-1784.
39. Dr.B.Rosiline Jeetha, K.Sivakamipriya, "Secure Routing and Detection of Hybrid Attacks in MANET", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2017.