Machine Learning for Human Intelligence
2024, Vol. 2, Issue 1

Research Article

Analytical Study of Routing Protocols in Mobile Ad Hoc Networks for Disaster Management

Muhammad Sarfraz[1], Adnan Abid[2], Irfan Khan[3], and Majid Mehmood[4,⋆]

[1,2,3,4]Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore, 54000, Punjab, Pakistan.; Email: sarfraz@umt.edu.pk,adnan@umt.edu.pk, irfan.khan@umt.edu.pk, majidmehmood@umt.edu.pk
⋆Corresponding author: Majid Mehmood (majid.mehmood@umt.edu.pk)

Article History

Academic Editor:
Dr. Muhammad Sajid
Submitted: March 21, 2023
Revised: May 19, 2023
Accepted: March 1, 2024

Keywords:
Mobile Ad-Hoc Network (MANET); Routing Protocol; Mobility; Ad-Hoc Networking; Topology

Abstract

A mobile ad hoc network (MANET) is a distinctive example of a decentralized, self-organizing, and self-managing wireless ad hoc network. MANET is utilized in several domains such as rescue operations, real-time information dissemination, interpersonal communication, information exchange, and network partitioning. MANET exhibits dynamic alterations in both its structure and nodes to facilitate rapid data transmission. The mobility of nodes presents numerous opportunities for routing design difficulties among them. A list of routing protocols exists, each with unique characteristics, developed for certain locations and compared based on various metrics. This study provides a comprehensive overview and comparison of several MANET routing strategies, along with their limitations in ad-hoc routing networks.

1 Introduction

The emergence of wireless technology in the 1980s initiated the advent of wireless networks, subsequently transforming various facets of human existence. Ad-hoc network technology has made significant contributions and remarkable achievements in research during the past 14 years. Many researchers investigated this subject to perform more comprehensive study and learning. Numerous issues and addressable challenges arise in this domain because to the ongoing topological changes in MANET. Recent research in MANETs focuses on efficient routing, data management, energy efficiency, multicasting, clustering, and mobility management. Networks lacking infrastructure are referred to as Mobile Ad-hoc Networks (MANET) [1]. In networks lacking a fixed access point, each node may function as a router. All nodes possess unfettered mobility and are dynamically and arbitrarily interconnected. The entire network must be governed, administered, and structured by the terminals themselves. The entire network is movable, allowing each terminal to navigate freely.

MANET (Mobile Ad-Hoc Network) is a widely utilized infra structureless wireless network in which each node functions as a router and performs self-configuration. A network established for a specific context and purpose, which disbands upon the fulfillment of its objectives [3]. Wireless links are utilized in MANET for self-configuration. The interdependence of mobile nodes is essential for maintaining network connectivity. A critical concern in MANETs is the requirement for routing protocols to swiftly adapt to topological alterations inside the network. Simultaneously, owing to the restricted bandwidth of mobile radio interfaces, it is essential to minimize the control traffic produced by routing protocols [4]. Numerous protocols are available that tackle the challenges of routing in mobile ad-hoc networks. Protocols are generally categorized into two types based on the timing of a node's acquisition of a route

to a destination. Reactive protocols are defined by nodes obtaining and sustaining routes as needed [5]. Typically, when a node necessitates a route to an unfamiliar destination, a query is disseminated throughout the network, and responses, comprising potential routes to the destination, are received.

In a Mobile Ad Hoc Network (MANET), the mobility of nodes or devices in any direction frequently alters the connections between them. The maintenance of traffic through nodes enhances network performance. Each node functions similarly to a router [6, 7, 8]. In disaster management communication, various routing protocols are employed; thus, our primary challenge is how to govern and manage these multiple routing protocols during disaster communication. In a catastrophe scenario, it is imperative to communicate efficiently; therefore, we must assess the utilization of both proactive and reactive strategies. Thirdly, in emergency situations, how can we achieve enhanced efficiency? Neighbor sensing refers to the mechanism by which a node identifies alterations in its vicinity.

2 Literature Review

This research study provides a concise overview of previous investigations into Wireless Mobile Adhoc Networks [9, 10, 11]. After evaluating various routing path security protocols in MANET, they selected a suitable Multi Secure Routing Protocol (MSR). The author use routing protocol techniques (AODV, DSR, DSDV, MSR, ZRP) to compare and examine different proactive, reactive, and hybrid routing types. Outcome obtained from the simulation test using NS-3 software. To diminish the overall frequency of route discoveries, Goswami [12] proposed multiple routing employing the AODV reactive-based technique. An alternative approach should be available. The author employed a Monte Carlo approach to periodically update packets by sampling the complete path between the source and destination nodes. Simulated results enhance the network's overall quality. Sultana and Ahmed examined the AOMDV reactive Protocol in their article [13], utilizing various pathways and elliptic curve cryptography (ECC) technology.

This is an effective proactive routing protocol solution utilizing periodic measures, yielding superior ideal results in network traffic congestion and throughput, as demonstrated through simulated software [14]. This study by Utpal Kumar et al. [15] employs various robust and security-oriented methods to verify node authentication in the MANET. In GSR, each node sustains a link state table derived from current information obtained from adjacent nodes and regularly shares its link status data exclusively with neighboring nodes [16]. This has considerably diminished the quantity of control messages transmitted throughout the network. Nonetheless, the magnitude of update messages is quite substantial, and as the network expands, their size will increase more. Consequently, a significant portion of bandwidth is utilized by these update messages. In this paper, Raj Kamal and Sunil Kumar [17] utilized a proposed strategy to ensure the secure transmission of data across both symmetric and asymmetric cryptographic methods. They employed an encrypted method of data with symmetric cryptography. Authors employ asymmetric cryptography based on the hash of the information. Create a digital signature for a data set or piece of information. The proposed approach has been validated using the AES algorithm.

Shreyas and Vidya [18] proposed a system in their article that is based on highly secure information transmission from one point to another. They designate the system as a Hybrid Cryptographic System for enhanced security. They attempted to reduce network congestion and ensure a high proportion of secure packet delivery in the existing system by employing RSA, the Data Encryption Standard (DES), and a digital signature technique [19]. Ajay Kushwaha et al. [20] introduced the Selective Significant Data Encryption (SSDE) method for text management through encryption. Only the most critical data was utilized for SSDE from the full message. This solution minimizes encryption time and enhances standardization. The symmetric key algorithm (SKA) and BLOWFISH are important components in the success of encryption in the study. Sherin Zafar et al. [21] propose an optimal genetic-stowed biometric method to mitigate service quality difficulties in MANET. Their proposed solution employs an algorithm that integrates iris biometrics and genetic data.

Remya and Lakshmi devised a cluster-based routing protocol known as SHARP (Secure Hierarchical Anonymous Routing Protocol) [22]. The method mitigates the issue of anonymity between source and destination nodes. This protocol provides superior safety compared to alternative routing

techniques. To ensure secure data transport in MANET, Deore Suvarna et al. [23] developed the Enhanced Adaptive Acknowledgment (EAACK) approach. The primary objective of this research is to mitigate the challenges of misconduct, limited transmission power, and receiver interference. To provide a safe, legitimate, and reliable routing approach in Mobile Ad Hoc Networks (MANETs) to address node misbehavior, Anjali Annand et al. [24] developed a distributed dynamic model. Employ the overhead to evaluate performance. The network's bandwidth and packet transmission. Authors evaluated various contemporary methodologies, including LMRSA, LARS, OCEAN, and the traditional DSR methodology, proposing a clustering algorithm with a digital signature for secure transmission [25, 26, 27].

Garima Jain, to safeguard MANET from pollution attacks, Dr. Gajendrasingh Rajawat [28] presented an enhanced variant of AODV. This iteration employs homographic encryption. The Secure Acknowledgement (ACK) System was proposed by Rasika and Sudhir [29] to detect node misbehavior in MANET. An effective method is referred to as ACK. Letter shape-based encryption was offered by A. Maheswary and Baskar [30, 31] for the purpose of transmitting data over networks. The proposed methodology requires less time to encrypt data compared to DES, AES, and RSA, as seen by the results. It is safeguarded against a moderate-level assault. Rohit Chourasia and Rajesh Kumar Boghey [32, 33, 34] developed an advanced intrusion detection system that identify erroneous ping packet drops and select an alternative, more secure data transmission route. These methods need the use of MATLAB. To assess the approach's reliability, performance is compared with similar prior tactics [36]. P. Sathya et al. [37] devised a multicast routing approach to conserve energy in MANET, contrasting it with the existing protocol. Performance evaluation metrics encompassed throughput, latency, packet delivery ratio (PDR), and network lifetime. [40] devised a zone-based routing system for secure routing in MANETs. To resolve cluster-related challenges, he suggested the BAT methodology. Table 1 demonstrates the application of current protocols and approaches.

Table 1: Current Protocols and Techniques

Author/Year	**Methodology employed**	**Concerns**	**Constraints/Benefits**
Bairwa 2022	Naïve restructured version of the AODV algorithm	Urgent situation	Enhance Quality of Service
Kachooei 2021	CALAR-DD protocol	Solution for latency issues	Only OLSR and AODV employed
Alameri 2020	AODV, DSDV	Comparative examination	Restricted measurement metrics

3 Materials and Methods

Routing protocols indicate the direction of a route between nodes and furnish information to assist network nodes in selecting a route [5].

3.1 Wireless Routing Protocol (WRP)

Four tables facilitate the maintenance of each node, namely for routing purposes: distance tables, routing tables, link-cost tables, and message retransmission lists are utilized. In WRP, message updates are executed via the neighbors of a node.

3.2 Reactive Routing Protocol (RRP)

A route may only be formulated in Reactive Routing (RRP) when required to achieve the primary objective. The distance-vector routing approach exclusively handles the route to a certain destination

Table 2: Comparison of Proactive Routing Protocols (PRPs)

Obstacles	**DSDV**	**Optimized Link State Routing**
Load Balancing Issue	Adverse	Adverse
Concerns regarding reliability and validity	Favorable	Affirmative
Throughput problem	Impaired mobility	Superior outcome in comparison to DSDV
Issue with scale control	Adverse	Adverse
Management of Control Problem	Favorable	Adverse

station upon a node's request and necessity. The proactive routing protocol (PRP) has numerous problems, with its primary objective being the minimization of traffic requiring routing.

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

One of the reactive routing protocols is known as Ad-hoc On-Demand Distance Vector (AODV). It is specifically designed for mobile ad-hoc networks utilizing wireless technologies for operations. The core function is the on-demand generation of routes from source to destination, supporting both unicast and multicast routing protocols. The AODV protocol establishes routes between nodes in reaction to requests from the source node. Consequently, it was designated as an on-demand nature technique. It fulfills the purpose of communication without increasing traffic on the link [8].

Table 3: Comparison of Various Reactive Routing Protocols (RRP)

Obstacles	**AODV**	**DSR**
Issues of Complexity	Average	Temperate
Load Balancing Issue	Adverse	Adverse
Dependability and accuracy problem	Affirmative	Affirmative
Route configuration	Delete post-usage	Delete post-usage
Throughput problem	For individuals above 20 nodes it is low	Reduction in-increment in mobility
Scale management issue	Adverse	Adverse
Management of Control Problem	Adverse	Adverse
Route management	Via Table	Via cache
Loop complications	Complimentary	Complimentary
Remove Route Information timing	Affirmative	Adverse
Support for Multi Routing System	Adverse	Favorable
Categories of protocols	Distance-based routing	Source base routing
Load on Route	Minimal	Temperate

3.3 Hybrid Routing Protocol (HRP)

A protocol that integrates the benefits of proactive routing protocols (PRP) and reactive routing protocols (RRP) is referred to as a hybrid routing protocol (HRP). The disadvantages of the hybrid routing strategy are that it relies on the number of active nodes, and its response to traffic demand is contingent upon traffic volume.

3.3.1 Sharp Hybrid Adaptive Routing Protocol (SHARP)

SHARP employs an automatic mechanism to identify the equilibrium between proactive and reactive routing protocols by adjusting the ratio of route information supplied proactively compared to that which must be ascertained reactively.

Table 4: Advantages and Disadvantages of Routing Protocols

Procedure	**Advantages**	**Disadvantages**
Proactive Routing Protocol	Minimize tardiness and provide updated information	Excessive traffic congestion
Reactive Routing Protocol	On-demand approach is consistently accessible, requiring no iterations and experiencing minimal traffic burden	Elevated incidence of tardiness
Hybrid Routing Protocol	Appropriate for extensive network with prompt information	Increased complexity

4 Results and Analysis

In the literature review, we scrutinized various routing protocols together with their security concerns, energy efficiency, routing challenges, weaknesses in the physical data structure and layers, and endeavored to tackle e-security issues. The aforementioned routing protocols are advantageous and efficient for current research focused on identifying existing challenges for further examination. A plethora of innovative techniques, rules, algorithms, and protocols have been introduced for routing solutions; nevertheless, despite considerable progress, several research challenges remain, especially concerning which protocol, technique, method, algorithm, or procedure exhibits optimal performance in particular environments.

5 Conclusions and Future Research

This paper examines various routing protocol strategies and emphasizes the distinct challenges associated with these methods. We contend that this may offer more guidance to researchers in enhancing routing performance. A mobile ad hoc network (MANET) is a distinctive example of a decentralized, self-organizing, and self-managing wireless ad hoc network. MANET is utilized in several domains such as rescue operations, real-time information dissemination, interpersonal communication, information exchange, and network partitioning. MANET exhibits dynamic alterations in both its structure and nodes to facilitate rapid data transmission. The mobility of nodes presents numerous opportunities for routing design difficulties among them. A list of routing protocols exists, each with unique characteristics, developed for certain locations and compared based on various metrics. This study provides a comprehensive overview and comparison of several MANET routing strategies, along with their limitations in ad-hoc routing networks. Future study aim will compare various routing algorithms based on network overhead.

Table 5: Comparative Examination of Various Routing Protocol Types

Primary Characteristics	**Proactive Procedure**	**Responsive protocol**	**Hybrid Protocol**
Routing complications for Acquisition	Table-Driven Base	On a demand basis	Both amalgamate
Challenges of Scalability	Reduced Level	Inaccurate for extensive networks	Possess optimal design for extensive networks
Latency challenges	Reduced owing to the utilization of a table for routing	Its elevated peak owing to flooding conditions	Reduced interior zone, elevated exterior zone
Bandwidth Requirement Issues	Elevated	Reduced	Moderate
Regularly updating	Required when alterations occur in network topology	Unnecessary	Required
Challenges in Routing Overhead	Elevated	Reduced	Moderate
Power Demand Concerns	Elevated	Fewer	Moderate
Storage capacity challenges	Elevated	Reduced	Moderate
Mobility of nodes	Periodic updates	Maintain route as required	Integrate both components
Routing Information Concerns	Elevated Availability	Availability based on requirement	Integrate both elements

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. (2021). An OLSR-based geocast routing protocol for vehicular ad hoc networks. *Peer-to-Peer Networking and Applications*, 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)*, 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. (2017, February). Efficient routing protocols for mobile ad hoc network. In *Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), 2017 Third International Conference* (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] Remya, S., & Lakshmi, K. S. (2015). Secured hierarchical anonymous routing protocol (SHARP) with RSA anonymity. *International Journal of Computer Applications*, *120*(14), 1-5.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] Rajkumar, B., & Narsimha, G. (2016). Trust based certificate revocation for secure routing in MANET. *Procedia Computer Science*, *92*, 431-441.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] Sathya, P., Kamalakkannan, S., & Shanthi, K. (2017). Performance analysis of energy efficient multicast routing protocols in mobile adhoc networks. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *6*(1), 427-434.

[38] 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.

[39] 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.

[40] Jeetha, B. R., & Sivakamipriya, K. (2017). Secure routing and detection of hybrid attacks in MANET. *International Journal of Innovative Research in Computer and Communication Engineering*, *5*(2), 1654-1661.