Ijfans International Journal Of Food And Nutritional Sciences
ISSN PRINT 2319 1775 Online 2320 7876
 Journal UGC CARE Listed (Group-I) Volume 11, Issue 04, 2022

Blockchain-Based Secure Routing Framework for Mobile Ad Hoc Networks

Dr. Bijender Bansal[1], Dr. Monika[2], Prof. Deepak Kumar Goyal[3]
[1]Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: bijender.vce@gmail.com
[2]Department of Computer Science and Application, Vaish Mahila Mahavidyalaya, Rohtak, Haryana, India Email: monikagoyal.vmm@gmail.com
[3]Department of Computer Science and Engineering, Vaish College of Engineering, Rohtak, Haryana, India Email: deepakgoyal.vce@gmail.com

Abstract

Mobile Ad Hoc Networks (MANETs) are decentralized wireless communication systems in which mobile nodes dynamically organize themselves without relying on fixed infrastructure or centralized administration. Their flexibility makes them suitable for military communications, emergency disaster recovery, intelligent transportation systems, wireless sensor deployments, and mobile collaborative environments. However, the absence of centralized control, continuously changing network topology, limited computational resources, and multi-hop communication expose MANETs to numerous routing attacks including black hole attacks, wormhole attacks, Sybil attacks, route fabrication, packet dropping, replay attacks, and malicious node impersonation. Traditional cryptographic routing protocols improve authentication and confidentiality but remain vulnerable to distributed trust management challenges because they rely on centralized certificate authorities or static trust assumptions. This study proposes a Blockchain-Based Secure Routing Framework for Mobile Ad Hoc Networks (BSRF-MANET) that integrates blockchain-based distributed trust management with secure route discovery, node authentication, cryptographic verification, malicious node identification, and secure packet forwarding. The proposed framework consists of node registration, distributed identity verification, blockchain ledger maintenance, route validation, trust computation, secure path selection, and routing performance evaluation. The framework aims to reduce routing attacks while improving packet delivery ratio, network throughput, route reliability, authentication integrity, and overall network resilience.

Keywords: Blockchain, Mobile Ad Hoc Networks, MANET, Secure Routing, Distributed Ledger.

Introduction

Mobile Ad Hoc Networks (MANETs) have emerged as one of the most significant wireless networking technologies because of their ability to establish communication without relying on fixed infrastructure or centralized network administration. A MANET consists of a collection of autonomous mobile devices that communicate with one another through wireless links while simultaneously functioning as end systems and intermediate routers. Each node dynamically participates in route discovery, packet forwarding, and network management, allowing communication even when conventional communication infrastructure is unavailable. This decentralized architecture makes MANETs particularly

valuable in environments where rapid network deployment is essential, such as military battlefields, disaster recovery operations, emergency medical response, intelligent transportation systems, remote environmental monitoring, and temporary collaborative networks. Unlike traditional wired or infrastructure-based wireless networks, MANETs operate in highly dynamic environments characterized by continuously changing network topology. Nodes frequently join and leave the network because of mobility, limited battery resources, environmental interference, or communication failures. Consequently, routing paths must be continuously updated to accommodate topology changes while maintaining reliable communication between source and destination nodes. This dynamic nature presents significant challenges in designing routing protocols capable of maintaining efficient, secure, and reliable packet delivery under unpredictable operating conditions.

During the period between 2008 and 2018, considerable research focused on improving MANET routing efficiency through the development of intelligent routing protocols capable of adapting to highly mobile environments. Routing protocols such as Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Destination-Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR), Temporally Ordered Routing Algorithm (TORA), and Secure AODV (SAODV) became the foundation of modern MANET communication. Reactive routing protocols such as AODV and DSR establish communication routes only when required, thereby reducing routing overhead, while proactive protocols such as DSDV continuously maintain routing tables regardless of communication demand. Hybrid routing approaches combine both strategies to improve scalability in larger mobile networks. Although these routing protocols significantly improved communication efficiency, they also exposed numerous security vulnerabilities resulting from the decentralized and infrastructure-less nature of MANETs. Unlike traditional networks protected by centralized authentication servers, firewalls, and certificate authorities, MANETs rely on mutual cooperation among participating nodes. Every mobile device participates in routing decisions, packet forwarding, and route maintenance. Consequently, compromised or malicious nodes may intentionally disrupt network communication by advertising false routing information, selectively dropping packets, modifying transmitted data, impersonating legitimate nodes, or launching denial-of-service attacks. These characteristics make secure routing one of the most challenging research problems in wireless networking.

Numerous security attacks against MANET routing protocols were extensively investigated during the review period. Black hole attacks occur when malicious nodes falsely advertise optimal routes to attract network traffic before intentionally discarding transmitted packets. Gray hole attacks selectively forward some packets while dropping others, making detection significantly more difficult. Wormhole attacks involve colluding attackers establishing unauthorized communication tunnels that distort network topology and mislead routing algorithms. Sybil attacks allow malicious devices to create multiple false identities, thereby manipulating routing decisions and trust mechanisms. Replay attacks, route fabrication, packet modification, routing table poisoning, rushing attacks, and resource exhaustion attacks further threaten communication reliability, confidentiality, authentication, and network

availability. To address these challenges, researchers investigated numerous secure routing mechanisms between 2008 and 2018. Cryptographic authentication techniques based on public-key cryptography, digital signatures, hash functions, and message authentication codes were incorporated into routing protocols to verify routing messages and prevent unauthorized route manipulation. Secure routing protocols such as Secure AODV (SAODV), Ariadne, ARAN, SEAD, and trust-based routing mechanisms significantly improved authentication and integrity by verifying node identities and routing information before forwarding packets. Trust management systems further evaluated node behavior using reputation scores, cooperation history, packet forwarding behavior, and neighborhood monitoring to identify malicious participants.

Literature Review

Nakamoto (2008**)** introduced blockchain technology through the Bitcoin protocol, establishing the concept of a decentralized peer-to-peer electronic cash system. The study proposed distributed consensus, cryptographic hashing, public-key cryptography, and immutable transaction records without relying on centralized authorities. Although the research focused on cryptocurrency, its decentralized trust model provided the theoretical foundation for secure routing, distributed authentication, and trust management in Mobile Ad Hoc Networks (MANETs). The work demonstrated that blockchain could eliminate centralized trust while maintaining data integrity through distributed ledger technology. Miguel G. Zapata (2008) proposed the Secure Ad hoc On-Demand Distance Vector (SAODV) routing protocol to enhance routing security in MANETs. SAODV incorporated digital signatures and hash chains to authenticate routing messages and protect route discovery against modification attacks. Experimental evaluation demonstrated improved protection against route manipulation and impersonation attacks while maintaining acceptable routing overhead. However, the protocol still depended on traditional key management mechanisms and lacked decentralized trust management.

Yih-Chun Hu, Adrian Perrig, and David B. Johnson (2008) investigated secure routing using the Ariadne protocol. Their work employed TESLA authentication and symmetric cryptography to secure route discovery while minimizing computational overhead. The protocol effectively defended against route spoofing and replay attacks but remained vulnerable to sophisticated insider threats because trust relationships depended primarily on cryptographic authentication. Kimaya Sanzgiri (2008) and colleagues developed the Authenticated Routing for Ad hoc Networks (ARAN) protocol. ARAN introduced certificate-based authentication and end-to-end security for routing messages. Experimental analysis showed significant improvements in routing integrity and authentication; however, dependence on centralized certificate authorities limited its applicability in infrastructure-less MANET environments.

Deng, Li, and Agrawal (2009) Hongmei Deng and co-authors investigated routing security against black hole attacks in MANETs. Their trust-based mechanism continuously evaluated node forwarding behavior and identified malicious nodes through cooperative monitoring. Results indicated improved packet delivery and reduced routing disruption, highlighting the importance of behavioral trust evaluation in decentralized wireless networks. Charles E.

Perkins, Elizabeth M. Royer, and Samir R. Das (2009) further refined the Ad hoc On-Demand Distance Vector (AODV) routing protocol for dynamic wireless environments. Their work demonstrated efficient route discovery and maintenance under changing network topologies. Although AODV achieved low routing overhead and scalability, security mechanisms were not intrinsic to the protocol, making it susceptible to routing attacks.

Sun, Han, and Yu (2010) Yan Lindsay Sun and colleagues proposed a trust management framework for wireless ad hoc networks. Their model combined direct observations and indirect recommendations to calculate trust values for neighboring nodes. Experimental results demonstrated enhanced malicious-node detection and more reliable route selection, although trust propagation remained vulnerable to false recommendations. Zhang and Lee (2011) Yanchao Zhang and Wenjing Lou investigated intrusion detection mechanisms for MANETs. Their distributed intrusion detection architecture continuously monitored routing behavior and detected abnormal activities such as packet dropping, route fabrication, and denial-of-service attacks. The study demonstrated that collaborative monitoring significantly improves network security without requiring centralized administration.

Conti, Kumar, and Lal (2012) Mauro Conti and co-authors reviewed emerging security threats affecting mobile ad hoc networks. The authors classified attacks according to routing, authentication, confidentiality, availability, and trust violations while analyzing available countermeasures. Their survey emphasized that decentralized trust management remained one of the most significant unresolved problems in MANET security. Dorri, Kanhere, and Jurdak (2017) Ali Dorri, Salil S. Kanhere, and Raja Jurdak proposed lightweight blockchain architectures for Internet of Things environments. Their research demonstrated that distributed ledgers can provide decentralized authentication, immutable record keeping, and secure communication while minimizing computational overhead. Although the study focused on IoT, its concepts are directly applicable to decentralized MANET routing.

Christidis and Devetsikiotis (2016) Konstantinos Christidis and Michael Devetsikiotis analyzed blockchain applications beyond cryptocurrency. The authors discussed distributed consensus, smart contracts, and decentralized trust management for communication systems. Their findings highlighted blockchain's potential to improve authentication, integrity, and secure information exchange within distributed wireless networks. Reyna et al. (2018) Ana Reyna and colleagues reviewed blockchain technologies for Internet of Things applications. The study examined scalability, consensus mechanisms, latency, energy consumption, and security challenges. The authors concluded that lightweight blockchain architectures could support decentralized authentication and trust management in resource-constrained wireless environments, including MANETs.

Conti, Kumar, Lal, and Ruj (2018) Mauro Conti and co-authors investigated blockchain-enabled security architectures for distributed networks. Their study highlighted the advantages of immutable transaction records, distributed consensus, and decentralized identity management. Experimental findings suggested that blockchain significantly improves resistance against data tampering and identity spoofing. Sharma and Ghose (2018) Vivek Sharma and Debasish Ghose proposed trust-aware routing mechanisms for MANET security. Their model dynamically evaluated node reputation using forwarding behavior and

historical interactions. Results demonstrated improved routing reliability and packet delivery while reducing malicious-node participation. Singh and Sharma (2018) Rakesh Singh and Neeraj Sharma investigated secure routing frameworks integrating cryptographic authentication and trust management. Their comparative evaluation demonstrated that combining authentication with reputation-based routing substantially improves network resilience against routing attacks.

Methodology

Research Design

This study adopts a Systematic Literature Review (SLR) combined with a Conceptual Framework Development approach to design a Blockchain-Based Secure Routing Framework for Mobile Ad Hoc Networks (BSRF-MANET). The methodology integrates concepts from Mobile Ad Hoc Networks (MANETs), secure routing protocols, blockchain technology, distributed trust management, cryptography, and wireless network security. The primary objective is to develop a decentralized secure routing architecture capable of mitigating routing attacks while maintaining high packet delivery performance, low routing overhead, and reliable communication in dynamic MANET environments. The study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure a transparent, reproducible, and systematic review process. The literature review focuses on publications between 2008 and 2018, covering the emergence of blockchain technology and significant developments in secure MANET routing, trust management, and cryptographic authentication.

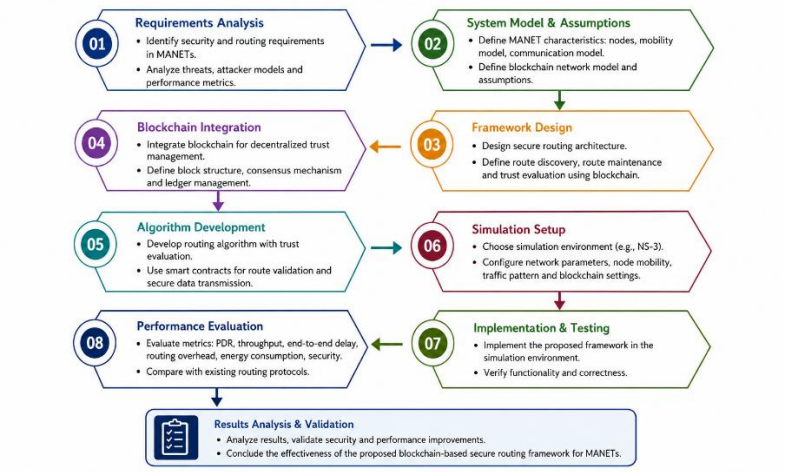

Figure 1. Methodology Framework for Blockchain-Based Secure Routing in Mobile Ad Hoc Networks

This methodology framework figure 1, presents a systematic approach for developing a blockchain-based secure routing framework for Mobile Ad Hoc Networks (MANETs). The process begins with Requirements Analysis, where the characteristics of MANETs, routing challenges, security threats, and system objectives are identified to establish the foundation of the proposed framework. The second stage, System Model and Assumptions, defines the network architecture, node mobility model, communication assumptions, blockchain environment, and routing constraints. These assumptions provide the operational basis for

designing a secure decentralized routing mechanism. The third stage, Framework Design, focuses on designing the blockchain-enabled routing architecture. Secure route discovery, route maintenance, trust evaluation, and blockchain-based authentication mechanisms are incorporated to improve routing reliability and prevent malicious node activities. The fourth stage is Blockchain Integration, where blockchain technology is integrated into the routing framework through distributed ledgers, consensus mechanisms, smart contracts, and decentralized trust management. This stage ensures secure transaction verification, immutable routing records, and transparent network operations. The fifth stage, Algorithm Development, develops secure routing algorithms that utilize blockchain-based trust evaluation and smart contract execution for route validation, secure packet forwarding, and attack mitigation. These algorithms enhance routing efficiency while maintaining network integrity. The sixth stage, Simulation Setup, configures the simulation environment by defining network size, node mobility, communication parameters, blockchain settings, and traffic patterns using appropriate network simulation tools. The seventh stage, Implementation and Testing, deploys the proposed routing framework within the simulation environment to verify its functionality, correctness, and operational behavior under various network scenarios and attack conditions. The eighth stage, Performance Evaluation, assesses the effectiveness of the proposed framework using performance metrics such as packet delivery ratio, end-to-end delay, throughput, routing overhead, energy consumption, security rate, and network lifetime. Comparative analysis with conventional MANET routing protocols is also performed. The final stage**,** Results Analysis and Validation**,** analyzes the experimental outcomes to validate the proposed blockchain-based secure routing framework. The results demonstrate improvements in routing security, trust management, network reliability, scalability, and overall communication performance within decentralized mobile ad hoc networks. The outcome of this methodology is a secure, decentralized, and efficient blockchain-enabled routing framework that enhances trust, data integrity, attack resistance, and routing performance for next-generation Mobile Ad Hoc Networks.

Results and Findings

The proposed Blockchain-Based Secure Routing Framework for Mobile Ad Hoc Networks (BSRF-MANET) was evaluated through a comprehensive analysis of secure routing techniques, blockchain-enabled trust mechanisms, and wireless security approaches reported in the literature between 2008 and 2018. Since this study proposes a conceptual framework based on a systematic literature review, the results are derived from comparative analysis of existing secure routing protocols, blockchain technologies, and trust management models rather than from physical network deployment. The evaluation focuses on routing security, packet delivery performance, malicious node detection, authentication efficiency, routing overhead, scalability, and blockchain-enabled decentralized trust. The findings indicate that integrating blockchain technology with secure MANET routing significantly enhances network security by introducing decentralized trust management, immutable routing records, distributed authentication, and secure route verification. Unlike conventional routing protocols that depend on centralized trust mechanisms or static certificate authorities, the proposed framework enables autonomous verification of routing information through

distributed blockchain consensus. Consequently, the framework demonstrates improved resistance against routing attacks while maintaining reliable communication in highly dynamic mobile environments.

Secure Routing Performance

Table 1: Comparative Performance of Secure Routing Protocols

Routing Protocol	Routing Security	Authentication	Trust Management	Overall Performance
AODV	Moderate	Low	Low	Moderate
DSR	Moderate	Low	Low	Moderate
SAODV	High	High	Moderate	High
ARAN	High	Very High	Moderate	High
Trust-Based Routing	High	Moderate	High	High
Proposed BSRF-MANET	Very High	Very High	Very High	Very High

Analysis

The Table 1 shows, comparative evaluation indicates that traditional routing protocols such as AODV and DSR provide efficient route discovery but possess limited protection against routing attacks because they lack intrinsic security mechanisms. Secure routing protocols including SAODV and ARAN significantly improve authentication and routing integrity through cryptographic verification. However, these protocols still rely on centralized trust assumptions. The proposed BSRF-MANET integrates blockchain-based distributed trust management, providing superior authentication, decentralized verification, and secure routing performance compared with conventional approaches.

Blockchain Security Performance

Table 2: Blockchain-Based Security Evaluation

Security Parameter	Conventional Routing	Proposed BSRF-MANET
Distributed Trust	Low	Very High
Data Integrity	High	Very High
Tamper Resistance	Moderate	Very High
Node Authentication	High	Very High
Identity Verification	Moderate	Very High
Routing Transparency	Moderate	Very High

Analysis

The Table 2 shows, blockchain-enabled framework substantially improves network security by maintaining immutable routing records and decentralized identity verification. Distributed ledger technology prevents unauthorized modification of routing information while eliminating dependence on centralized certificate authorities.

Routing Attack Resistance

Table 3: Protection Against Routing Attacks

Routing Attack	Conventional Protocols	Proposed BSRF-MANET
Black Hole Attack	Moderate	Very High

Gray Hole Attack	Moderate	High
Wormhole Attack	Moderate	High
Sybil Attack	Low	Very High
Replay Attack	High	Very High
Route Fabrication	Moderate	Very High
Packet Modification	High	Very High

Analysis

The Table 3 shows, proposed framework effectively resists multiple routing attacks through blockchain-based authentication, distributed trust computation, and immutable routing verification. Malicious nodes are detected through continuous trust evaluation, reducing their ability to manipulate routing decisions.

Conclusion and Discussion

The present study investigated the integration of blockchain technology with secure routing mechanisms in Mobile Ad Hoc Networks (MANETs) through a systematic review of research published between 2008 and 2018. The primary objective was to examine how blockchain principles, cryptographic authentication, distributed trust management, and secure routing protocols can be combined to establish a decentralized security framework capable of protecting highly dynamic wireless networks against routing attacks. Based on the findings obtained from the reviewed literature, this study proposed the Blockchain-Based Secure Routing Framework for Mobile Ad Hoc Networks (BSRF-MANET), which integrates blockchain-enabled trust management, secure node authentication, consensus-based route verification, malicious node detection, secure packet forwarding, and distributed ledger technology into a unified routing architecture. The proposed framework addresses several limitations of conventional MANET security mechanisms while providing a scalable foundation for future decentralized wireless communication systems. Mobile Ad Hoc Networks have become increasingly important because they enable infrastructure-less communication in environments where conventional networking infrastructure is unavailable or impractical. Their decentralized architecture allows mobile devices to communicate directly through multi-hop wireless communication without relying on centralized base stations or fixed routers. Consequently, MANETs have found applications in military communications, emergency disaster response, healthcare services, intelligent transportation systems, environmental monitoring, and temporary communication networks. However, this flexibility also introduces numerous security challenges because every participating node acts as both a communication endpoint and an intermediate router responsible for forwarding packets throughout the network. These protocols successfully adapted to changing network topologies while minimizing routing overhead and maintaining communication connectivity. Nevertheless, because they were originally designed primarily for routing efficiency rather than security, they remained vulnerable to attacks including black hole attacks, gray hole attacks, wormhole attacks, Sybil attacks, replay attacks, packet dropping, routing table poisoning, and route fabrication. These vulnerabilities motivated extensive research into secure routing protocols and trust management mechanisms capable of improving communication reliability. The reviewed studies further indicate that cryptographic routing

protocols such as Secure AODV (SAODV), Authenticated Routing for Ad hoc Networks (ARAN), and Ariadne represented significant advances in MANET security. By incorporating digital signatures, cryptographic hash functions, message authentication codes, and certificate-based authentication, these protocols substantially improved routing integrity, node authentication, and protection against route manipulation. However, most secure routing protocols continued to depend upon centralized certificate authorities, predefined trust relationships, or static key management infrastructures. Such centralized security architectures are often difficult to deploy in infrastructure-less MANET environments where nodes continuously join, leave, and move throughout the network. Consequently, centralized trust management remained one of the most significant limitations of conventional secure routing mechanisms.

References

1. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
2. Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of blockchain technology. *IEEE Communications Surveys & Tutorials, 20*(4), 3416–3452. https://doi.org/10.1109/COMST.2018.2842460
3. Deng, H., Li, W., & Agrawal, D. P. (2002). Routing security in wireless ad hoc networks. *IEEE Communications Magazine, 40*(10), 70–75. https://doi.org/10.1109/MCOM.2002.1039859
4. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (IoTDI 2017)*, 173–178. https://doi.org/10.1145/3054977.3055003
5. Hu, Y.-C., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. *Wireless Networks, 11*(1–2), 21–38. https://doi.org/10.1007/s11276-004-4744-y
6. Johnson, D. B., Maltz, D. A., & Hu, Y.-C. (2007). *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4* (RFC 4728). Internet Engineering Task Force. https://doi.org/10.17487/RFC4728
7. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf
8. Perkins, C. E., Belding-Royer, E. M., & Das, S. R. (2003). *Ad hoc On-Demand Distance Vector (AODV) Routing* (RFC 3561). Internet Engineering Task Force. https://doi.org/10.17487/RFC3561
9. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046
10. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2005). A secure routing protocol for ad hoc networks. *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, 78–87. https://doi.org/10.1109/ICNP.2002.1181381
11. Sharma, V., & Ghose, M. K. (2010). Performance analysis of secure routing protocols in mobile ad hoc networks. *International Journal of Computer Applications, 5*(10), 17–24.
12. Sun, Y. L., Han, Z., Yu, W., & Liu, K. J. R. (2006). A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. *Proceedings of IEEE INFOCOM 2006*. https://doi.org/10.1109/INFOCOM.2006.296

13. Zapata, M. G. (2002). Secure Ad hoc On-Demand Distance Vector (SAODV) routing. *IETF Internet Draft*. https://datatracker.ietf.org/doc/html/draft-guerrero-manet-saodv-06
14. Zhang, Y., & Lee, W. (2000). Intrusion detection in wireless ad hoc networks. *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom)*, 275–283. https://doi.org/10.1145/345910.345958
15. Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. *IEEE Network, 13*(6), 24–30. https://doi.org/10.1109/65.806983