Blockchain-Based Security Mechanisms for MANETs: A Review of Performance and Challenges

Rachid Khalladi[1], Youcef Fekir[2], Mohammed Rebbah[1]
[1]Laboratory of Informatics and Intelligent Systems, Department of Computer Science, University of Mustapha Stambouli-Mascara.
[2]Department of Computer Science, University of Mustapha Stambouli-Mascara.
E-mail : r.khalladi@univ-mascara.dz, youcef.fekir@univ-mascara.dz, rebbahmed@univ-mascara.dz.

Keywords: blockchain, security, MANET, challenges

Received: March 26, 2025

Mobile ad hoc networks MANETs are networks composed of a finite set of nodes that connect to each other by self-organizing using wireless connections without a fixed infrastructure. These characteristics make this type of networks more vulnerable to different types of attacks. In 2008, a new technology appeared called Blockchain.
In recent years, this technology has become widespread as a means of implementing security in different applications. In addition, blockchain technology is introduced to overcome the vulnerabilities caused by the characteristics of MANETs, including the absence of a center of trust (Absence of a fixed infrastructure). To improve the security features, many blockchain-based security approaches are proposed for MANETs. The review delves into 16 recent blockchain-oriented security mechanisms, considering that blockchains can improve MANETs security (from 2019 to 2024). Our inclusion criteria were defined as technical relevance, MANET focus, and experimental validation.
Performance was evaluated in terms of latency, scalability, energy consumption, and security effectiveness. A comparison was made to find examples of common themes, strengths, and outstanding issues.
Our findings confirmed that although blockchain enhances data integrity, node authentication, and trust relationships, it causes computational overhead and latency. This paper emphasizes the trade-offs and outlines future research to optimize security benefits versus resource limitations in MANETs.

Povzetek: Narejen je pregled 16 blockchain-varnih mehanizmov za MANET-e (2019–2024), ocenjuje učinkovitost glede latence, porabe energije, razširljivosti in zaupanja. Izpostavi prednosti, izzive ter prihodnje raziskovalne smeri.

1 Introduction

Blockchain as an infrastructure could be extended to trust systems including intrusion detection methods, to obtain scalable and transparent solutions, benefiting from its extraordinary attributes, such as tamper-proof data. Blockchain in securing nodes leads to an increase in computational complexity. Consequently, the validation overhead increases, making it incompatible with dynamic network topology. Ultimately, multi-signature has come associated with an additional data overhead that is increasingly long during the lifetime. Following the previous reviews, many problems still persist and many demands need to be studied in this work [4] [6].

Nevertheless, several approaches based on trust management or intrusion detection systems have been proposed to mitigate these challenges. Trust management systems often rely on trust centralization. Intrusion detection systems that focus on fuzzy logic usually raise the issue of reliability. Moreover, although existing solutions have proven effective in several network attributes, improving the implementation rigor related to security and trust in intra-domain MANET environments, their definition of trustworthiness encounters vulnerabilities that make trustworthiness ambiguous to assess and thus remain debated. However, due to the decentralized nature and weaknesses of existing trust management systems, the use of blockchain for security augmentation is highly motivated [1] [7].

Mobile ad hoc networks (MANETs) are a type of decentralized wireless network without a fixed infrastructure. Therefore, they offer flexible networking solutions at the cost of increased security risks [2]. Existing security measures mainly focus on routing protocols. They often incur significant overhead and introduce vulnerabilities such as selfish behavior, black hole attacks, or data manipulation [8] [11].

Generally, MANET security problems are classified into three (3) schemes; Figure 1 illustrates the classification of MANET security strategies into approaches:

- Reactive: These are security solutions that act only after an incident, such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and firewalls.
- Proactive: They attempt to solve the problem before it occurs, but they are usually highly complex.
- Hybrid: They usually cover both reactive and proactive functionalities. For example, blockchain

solutions integrate monitoring and reputation systems.

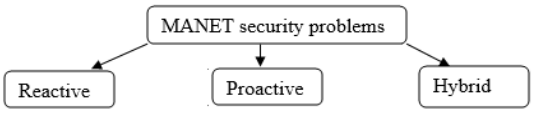

Figure 1: MANET security problems classification.

In recent years, the security problem in mobile ad hoc networks (MANETs) has become attractive to many researchers. MANET has become a focus of study due to its following characteristics: infrastructure-free, dynamic topology, rapid deployment, and self-organized assignments. Various attacks target MANET vulnerabilities and lack secure boundaries. Several techniques have emerged, each of which has its own advantages and disadvantages. Blockchain is a solution that can secure MANET more effectively if the concept of pre-membership can be ignored in MANET, and all member nodes can dynamically join or leave the network without centralized management [3] [6] [10]. Blockchain addresses key MANET vulnerabilities:

- Lack of centralized trust
- Susceptibility to routing attacks (e.g., blackhole, wormhole)
- Tampering with control messages
- Unreliable node reputation systems

Recent studies suggest that blockchain technology, due to its decentralization and tamper-proof data management, could solve a large number of security problems. On the other hand, the integration of blockchain into MANETs poses new problems: computational overhead, latency and energy consumption, which must be evaluated.

This study reviews the use of Blockchain technology to address various vulnerabilities in MANET networks, which can cause serious security problems. This review provides a structured and comparative analysis of recent solutions. It highlights design patterns, quantifies performance indicators, and identifies open research issues. It serves both as a reference for researchers and as a basis for the future development of efficient and blockchain-secured MANET protocols.

2 Background

2.1 MANETs in modern communication

MANETs represent one of the most important paradigms of modern communication. Among the main features of MANETs are a totally decentralized architecture, no fixed infrastructure, and self-forming and self-reconfiguring capabilities. These flexible features make MANETs especially indispensable in those environments where conventional systems for communication cannot work properly or simply are not available, such as in disaster recovery or in some military scenarios. As communication needs continue to grow, so does the need for resistant, efficient, and adaptive network solutions.

2.2 Blockchain technology

The emergence of blockchain technology is a revolutionary shift in how data integrity and security are managed across networks, including MANETs. Fundamentally, at its core, blockchain works as a decentralized and distributed ledger system that autonomously verifies and records transactions across a network of nodes, ensuring transparency and immutability [9]. This feature addresses critical security challenges intrinsic to MANETs due to dynamic topology and absence of any centralized authority, enhancing the network's vulnerability to data tampering and unauthorized access. It is this security provided by blockchain that gives way to a robust framework for the protection of data integrity across heterogeneous environments that usually characterize MANETs. It would greatly enhance operational efficiency, with much-enhanced data sharing capability, along with improving safety [9]. Hence, blockchain becomes one of the prime allies while dealing with MANET infrastructures against recent emerging threats. Figure 2 gives a general overview of how Blockchain technology works in security.

In this review, we focus primarily on private and consortium blockchains for MANET applications. These types provide permissioned access, allowing control over participant nodes, which is crucial in resource-constrained and trust-sensitive MANETs.

- **Public blockchains** (e.g., Bitcoin, Ethereum) offer full decentralization but are generally unsuitable for MANETs due to high computational and communication overhead.
- **Private blockchains** ensure faster consensus but rely on centralized management.
- **Consortium blockchains**, governed by a group of nodes, offer a balanced trade-off between decentralization and efficiency, which is more aligned with MANET constraints.

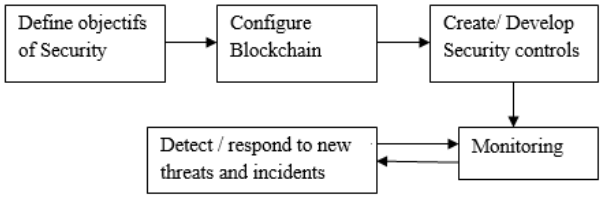

Figure 2: A security assessment process for blockchain solutions.

2.3 Key features of blockchain relevant to network security

The integration of blockchain technology adds to the network security in MANET a number of key features that are very important. The first one is the decentralized nature of blockchain; this reduces the risk of single-point failures and makes the system resistant to malicious attacks [34]. Blockchain brings in immutability into each transaction or interaction resulting across the nodes, especially due to constantly changing nodes in MANET and the chance of unauthorized access [35]. Since blockchain focuses on reinforcing not only security features of interaction between these nodes but also a well-developed trust of one another, it opens a new window toward operating despite continuous threat incidents [36].

Although immutability is a key advantage of blockchain, it may be a challenge for very dynamic MANETs that need frequent updates.

To address this:

- Off-chain data manipulations: flexibility can enable updates without changing the base chain.
- Smart contract versioning and timestamped overrides blocks can be useful technologies to handle the state of a network that is continuously changing.

Table 1: Key features of blockchain relevant to network security.

Feature	Description	Impact on Security
Decentralization [34] [35]	Reduces single points of failure. Enhances resilience.	Increases security against attacks as there is no central authority to target.
Transparency [35]	All transactions are recorded on a public ledger that is accessible to all participants.	Enhances traceability and accountability, making it easier to detect fraudulent activities.
Immutability [34] [35]	Once recorded, information on the blockchain cannot be altered or deleted.	Prevents tampering and ensures data integrity, making the network more secure.
Cryptographic Security [34]	Uses advanced encryption methods to secure data transmission and storage.	Protects sensitive information from unauthorized access and cyber attacks.
Smart Contracts [36]	Self-executing contracts with the terms of the agreement directly written into code.	Automates processes and reduces human errors, thereby increasing security and trust in transactions.

3 Overview

Blockchain technology is considered as one of the most promising solutions for improving the security of MANETs by addressing the vulnerabilities associated with malicious nodes to ensure reliable routing. The integration of blockchain will help in decentralizing trust mechanisms and improving routing efficiency thereby reducing various types of attacks. Here are some key aspects of how blockchain secures MANETs.

In [13] a blockchain-based reliable distributed routing scheme for MANETs has been proposed. The latter, uses blockchain technology to establish a fair proof-of-reputation system that guarantees reliable and decentralized routing through authenticated blockchain token transactions, which helps to improve security and efficiency in mobile ad hoc networks.

BC-SDOR-MANET-AGNN (Blockchain-Controlled Secure Distributed Optimal Routing with Auto-Metric Graph Neural Network) incorporates a GNN (Graph Neural Network) for recommending suitable routes using node reputation, link stability and energy. A proof-of-reputation mechanism is employed in the blockchain to maintain integrity and trust of routing decisions among nodes. Simulation results demonstrated not only increase in packet delivery ratio but also less routing overhead than classical AODV. [14].

Blockchain can secure MANETs with node authentication and data/control packet protection via a secure routing algorithm (SRA) [15]. It generates hash (SHA256) codes for transactions, to improve network integrity, reduce latency, and improve performance metrics such as packet delivery ratio and throughput.

Blockchain-assisted Secure Routing (Block-Sec) protocol is a blockchain-based protocol for authenticating mobile nodes via a distributed one-time passcode (DOT) system, which provides enhanced security in MANETs by preventing unauthorized access and makes data transmission secure using the Efficient Elliptic Curve (E2C2) algorithm [16].

LB-IDS is a lightweight blockchain-assisted intrusion detection system for MANETs. It uses a blockchain-based multi-factor authentication scheme for node authentication and preventing malicious ingress, which

increases the overall network security level through continuous monitoring and trust value updates. [17]

DAG-Blockchain is a novel system for securing MANETs. It uses PUF multi-factor authentication and a Jelly Fish optimization algorithm to transmit trusted data, which results in improved security, packet delivery rate, and overall network performance in a WSN-IoT environment [18].

To improve the security of a MANET, blockchain technology is used to establish trust control between nodes, addressing the inherent lack of trust. The current limitations of blockchainhave been discussed in [19] and strategies for improving the application of cooperation in multi-hop MANETs through blockchain integration have been proposed.

A blockchain-based secure communication model for smart home networks is proposed in [20]. It improves user authentication and data integrity. However, it does not specifically address the application of blockchain to secure mobile ad hoc networks.

VABLOCK is a blockchain-based solution for improving the security of vehicle-to-vehicle (V2V) networks. In order to ensure secure communication, it leverages information-centric networks (ICNs). The vulnerabilities of mobile ad hoc networks (MANETs) are addressed through decentralized trust and data integrity [21].

Blockchain-based mobile ad hoc networks (MANETs) have become increasingly popular in recent years due to their high reliability and secure transactions. In a MANET, the dynamic nature of the network makes nodes more vulnerable to attacks, thus, it is difficult to maintain network security. Proof-of-work (PoW) can be an effective way to maintain consensus in a MANET environment, but it presents several challenges such as limited resources, network latency, security, energy consumption, and scalability. Byzantine Fault Tolerance (BFT) is a concept in distributed computing that refers to the ability of a system to tolerate failures or attacks from nodes that behave maliciously or fail unexpectedly. In [22], the challenges faced in Software Defined Networking (SDN) in Blockchain MANET are discussed. SDN and BFT are two different approaches to improve the performance, resilience, and security of distributed networks.

Blockchain secures MANET networks by providing immutability, consensus, and smart contracting, which ensures data integrity and authorized participation. The BSLS algorithm is proposed to improve communication security while addressing challenges such as selecting valid nodes and managing complexity in blockchain deployment [23].

To improve data security and immutability, a directed acyclic graph (DAG)-based distributed vehicular network using advanced blockchain technology is proposed. The vulnerabilities of mobile ad hoc networks (MANETs) against malicious attacks are addressed through a robust communication framework [24].

[25] Proposes a blockchain-based model that improves the security of mobile IoT networks by addressing vulnerabilities such as Man-in-the-Middle attacks. This model aims to reduce the risks associated with centralized architectures and ensures reliable interconnection in mobile IoT environments.

The Floyd-Warshall algorithm is proposed to secure MANET networks based on blockchain. This algorithm makes a miner node generate a common routing table with the shortest paths of all pairs. This results in improved security while managing energy consumption, but it incurs additional computational costs [26].

B4SDC implements a Proof-of-Stake consensus mechanism, which ensures fairness through cooperative reception reporting and by preventing spoofing and collusion attacks with secure digital signatures, and thus improves security and encourages data collection between nodes [27].

Blockchain improves the security of MANETs by ensuring data integrity through smart contracts. Smart contracts verify and enforce conditions during data processing. The “MPR Blockchain” approach aims to improve security and communication in IoT systems and ad hoc networks.[28]

The proposed Time Interval Based Blockchain Model (TIBBM) improves security in MANETs. It uses a Blockchain information structure for identifying malicious nodes. A Network Block Monitoring Node (NBMN) monitors routing blocks, which improves the detection of malicious nodes and overall network performance.[29]

A consortium blockchain-based decentralized trust management architecture for improving security in Software Defined Vehicular Networks (SDVN) is proposed. It addresses vulnerabilities by evaluating vehicle trust values and improves resource allocation, thus ensuring safer communication in the network.[30]

Blockchain can secure MANETs by implementing decentralized security models that improve data integrity and authentication. A blockchain-based routing system is proposed to improve trust and resilience in these

infrastructure-less networks, especially in emergencies where traditional security measures may fail [31].

Blockchain secures MANETs by providing a decentralized and tamper-proof trust management system. The latter, uses a lightweight consensus algorithm, which allows efficient transaction validation and collaboration among nodes, thereby solving security issues and enhancing trust in dynamic and resource-constrained environments [1].

To improve security and privacy in intelligent transportation systems, a secure distributed computing network architecture is proposed leveraging blockchain technology for this. It includes user/IoT device registration, authentication algorithms, and smart contracts to effectively secure the network.[32]

Blockchain technology can improve the security of mobile ad hoc networks (MANETs) by eliminating malicious nodes. This is done through the verification of data packets. This model increases the robustness of data transmission by analyzing blockchain parameters, such as the number of blocks generated and malicious node rates.[33]

Table 2: Summary table of the most popular solutions

Solution	Key Features	Benefits
BC-SDOR-MANET-AGNN [14]	Blockchain-based fair proof-of-reputation system	Reliable and decentralized routing, improved security and efficiency
Blockchain-assisted Secure Routing (Block-Sec) [16]	Distributed one-time passcode (DOT) system, E2C2 algorithm	Enhanced security, prevents unauthorized access, secure data transmission
LB-IDS [17]	Blockchain-based multi-factor authentication, continuous monitoring, trust value updates	Increased network security level, prevents malicious ingress
DAG-Blockchain [18]	PUF multi-factor authentication, Jelly Fish optimization algorithm	Improved security, packet delivery rate, network performance
VABLOCK [21]	Blockchain-based solution for V2V networks, ICNs	Decentralized trust, data integrity, addresses MANET vulnerabilities
BSLS [23]	Improves communication security, addresses node selection and complexity challenges	Enhanced security
DAG-based distributed vehicular network [24]	Advanced blockchain technology, robust communication framework	Addresses MANET vulnerabilities, improves data security and immutability
Blockchain-based model for mobile IoT networks [25]	Addresses Man-in-the-Middle attacks, reduces risks of centralized architectures	Reliable interconnection in mobile IoT environments
Floyd-Warshall algorithm [26]	Blockchain-based secure routing, shortest path calculation	Improved security, energy consumption management, additional computational costs
B4SDC [27]	Proof-of-Stake consensus mechanism, cooperative reception reporting, secure digital signatures	Fairness, prevents spoofing and collusion attacks, encourages data collection
MPR Blockchain [28]	Smart contracts for data verification and enforcement	Improved security and communication in IoT systems and ad hoc networks
Time Interval Based Blockchain Model (TIBBM) [29]	Blockchain information structure for identifying malicious nodes, Network Block Monitoring Node (NBMN)	Improved malicious node detection, network performance
Consortium blockchain-based decentralized trust management architecture [30]	Evaluates vehicle trust values, improves resource allocation	Safer communication in Software Defined Vehicular Networks (SDVN)
Blockchain-based routing system [31]	Decentralized and tamper-proof trust management, lightweight consensus algorithm	Efficient transaction validation, collaboration among nodes, solves security issues, enhances trust
Secure distributed computing network architecture [32]	User/IoT device registration, authentication algorithms, smart contracts	Improved security and privacy in intelligent transportation systems
Blockchain-based data packet verification [33]	Eliminates malicious nodes, increases data transmission robustness	Improved security and network robustness

4 Comparison of approaches and performance evaluation

The integration of blockchain into MANETs has led to various approaches aimed at enhancing security while mitigating constraints related to latency, energy consumption, and scalability. The following table compares the main solutions across five metrics: security strength, scalability, latency, energy use, and weaknesses. This allows cross-solution comparisons beyond individual descriptions

Table 3: Comparison and performance evaluation.

Solution	Security	Scalability	Latency	Energy Consumption	Strengths	Weaknesses
BC-SDOR-MANET-AGNN [14]	High (reputation proof)	Medium	High	High (blockchain validation)	Secure routing. Node authentication	High computational complexity. Increased latency
Blockchain-assisted Secure Routing [16]	High (DOT passcodes, E2C2)	Medium	High	Medium	Enhanced protection against intrusions	High validation delays due to passcodes
LB-IDS [17]	High (intrusion detection)	Medium	Medium	Medium	Continuous monitoring and enhanced authentication	Relies on frequent updates
DAG-Blockchain [18]	High (PUF authentication)	Good	Medium	Medium	Improved scalability with DAG. Better resource management	Complex block management and data consistency issues
VABLOCK [21]	High (reputation and trust management)	Medium	Medium	Medium	Secure V2V communication	Vulnerable to Sybil attacks if few honest nodes exist
BSLS [23]	High (secure communication)	Medium	Medium	Medium	Effective data flow security	Complexity management still needs improvement
DAG-based distributed vehicular network [24]	High (network attack protection)	Good	Medium	Medium	Enhanced transmission reliability	More complex block validation management
Floyd-Warshall algorithm [26]	High (optimized routing)	Medium	High	High	Improved routing security	High computational cost. Impact on node autonomy
B4SDC [27]	Medium (Proof-of-Stake and digital signatures)	Good	Low	Low	Optimized energy consumption. Good protection against spoofing attacks	Slightly lower security compared to more robust methods
MPR Blockchain [28]	High (data integrity via smart contracts)	Medium	Medium	Medium	Automated verification processes	Increased latency due to contract execution

Time Interval Based Blockchain Model (TIBBM) [29]	High (malicious node detection)	Medium	Medium	Medium	Continuous monitoring with Network Block Monitoring Node (NBMN)	May cause overhead in dense networks
Consortium blockchain-based decentralized trust management architecture [30]	High (trust value management)	Good	Medium	Medium	Improved reliability for connected vehicles	Requires a minimum infrastructure to operate
Blockchain-based routing system [31]	High (distributed trust management)	Good	Medium	Medium	Improved resilience against attacks	May require adaptation for high-mobility networks
Secure distributed computing network architecture [32]	High (authentication and smart contracts)	Good	Medium	Medium	Improved privacy and authentication	Computational overhead from smart contracts
Blockchain-based data packet verification [33]	High (elimination of malicious nodes)	Medium	Medium	Medium	Strengthened security of transmitted data	Requires constant traffic monitoring
Blockchain-based distributed ledger generation [35]	High (protection against MITM attacks)	Medium	Medium	Medium	Reduces risks associated with centralized architectures	May face integration issues in heterogeneous networks

Despite the large number of proposals, existing solutions remain unable to strike a balance between scalability, low power consumption, and robust security guarantees. The majority of the reviewed work focuses on complex authentication schemes, which are not always suitable for constrained MANET environments. Solutions rarely optimize all important factors simultaneously. A generalizable architecture, adaptable to low-resource and/or high-mobility scenarios, still remains lacking.

These shortcomings warrant further research into contextual trust metrics, lightweight consensus techniques, and adaptive security layers designed for dynamic MANET topologies.

5 Challenges of using blockchain to secure MANET

Using blockchain technology to secure mobile ad hoc networks (MANETs) presents several challenges. These challenges must be addressed to achieve effective security and performance. These challenges are primarily due to the inherent characteristics of MANETs, such as their dynamicity and decentralized nature, which complicate

the implementation of blockchain solutions. In the following, the most important challenges are discussed.

Malicious nodes can cause disruption in routing protocols that result in interception or manipulation of data [14] [15].

The dynamic nature of MANETs makes them susceptible to several types of attacks that target both data and control traffic (Blackhole, Grayhole and wormehole), which requires robust security measures [15].

The integration of blockchain technology can increase latency due to the overhead of transaction verification and consensus mechanisms, which can potentially influence throughput degradation [13] [15] . Blockchain can address the aforementioned attacks through:

- Immutable logging of routing behavior
- Decentralized reputation tracking
- Distributed validation of routing metrics

The mobility of nodes often decreases their computing power and energy, making it difficult to implement resource-intensive blockchain protocols [16].

As the network size increases, maintaining a blockchain can become more cumbersome, leading to scalability issues that affect performanceand security [13] [14].

Despite these challenges, the potential benefits of blockchain for improving security and trust in MANETs cannot be overlooked. In order to better meet the requirements of MANETs and address these challenges, future research is possible, especially focusing on the optimization of blockchain protocols.

6 Discussion

This research addressed blockchain integration for MANET security, offering significant potential to address the inherent security vulnerabilities of mobile ad hoc networks (MANETs) caused by their decentralized nature. MANETs are known for their dynamic topologies where nodes frequently join and leave each other, leading to security issues and potential attacks. In this case, blockchain improves trust and secure routing through decentralized verification.

The absence of a central authority is also an issue that influences the security of MANETs, blockchain eliminates the need for a trusted third party, aligning with the autonomous architecture of MANETs. Compared to the security of conventional MANETs (e.g., centralized or cryptography-based trust models), blockchain offers:

- A tamper-proof data records
- Decentralized trust without a central authority
- Auditability through distributed ledgers

These properties address the fundamental weaknesses of MANETs, including trust ambiguity, mobility-related disconnections, and vulnerabilities at central points.

Several studies have implemented blockchain to secure MANETs. In this research, we focus on the most recent and important works in this framework. A comparison was made to extract the advantages and disadvantages of each. Experimental results in the studied works show a reduction in the risks of forgery and an increase in packet delivery rates, as well as an improvement in trust and authentication.

The reviewed works can be categorized into one of three approaches:
Trust-based systems (e.g., [14], [21], [28]): Use reputation or behavior scores to validate node legitimacy. They are effective against insider attacks, but require frequent updates, which increases workload.
Intrusion detection (e.g., [17], [29]): Based on monitoring and anomaly detection using blockchain logs. They are effective at detecting new threats. However, they require high latency and energy consumption.
Routing-integrated systems (e.g., [16], [26], [18]): Integrate blockchain into routing decisions to select the secure path. These systems are highly resilient. However, their design is complex and validation is costly.

Although blockchain improves the security of MANETs, its implementation presents several challenges. Consensus mechanisms require significant computing power, which is not suitable for MANET nodes (limited resources).

Blockchain validation introduces delays, which hinders latency. This research can be a good raw material for other future works.

The following areas should be the focus of future research:

- Lightweight consensus designed for mobile environments
- Models of dynamic trust that adjust to shifting topologies
- Performance validation on real-world testbeds

Although the existing solutions are fragmented and incomplete, this review demonstrates that blockchain offers significant added value. There is still no integrated framework that combines intrusion detection, routing, and trust in a low-overhead, scalable design.

7 Conclusions

Mobile ad hoc networks (MANETs) are groups of devices forming a communication network without an established infrastructure. When deployed in ad hoc mode, most of the wireless devices can automatically discover and connect to each other directly using embedded antennas that mostly cover small regions but work well for the intended purpose. The decentralized nature of MANETs results in limited trust and makes security complex. Several methods to secure such networks have been proposed. This paper presents a comprehensive study of the suitability of blockchain technology for different security challenges of MANETs. This paper is an overview of the existing works on using blockchain in MANETs for security enhancement. In this work we focused on analyzing the performance of blockchain networks without infrastructure with emphasis on security and trust. This study showed that blockchain improves trust, authentication, and routing security in MANETs. Solutions such as BC-SDOR-MANET-AGNN and DAG-Blockchain have improved delivery rates. Remaining challenges include: proof-of-work consensus increases latency; node mobility limits trust consistency; and most models lack energy optimization.
This work can be a good reference that gives an overview of the latest blockchain-based solutions proposed to improve the security of MANETs.

In a future work, and based on the present work, we will try to propose a new system avoiding the limitations of existing systems and drawing inspiration from their advantages. Future research should explore:

- Adaptive consensus for mobile, low-power nodes
- Integrated trust + IDS frameworks
- Real-world deployment beyond simulation

References

[1] Lwin, May Thura, JinhyukYim, and Young-Bae Ko. 2020. "Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks" *Sensors* 20, no. 3: 698. https://doi.org/10.3390/s20030698

[2] Caballero-Gil, Pino, and Candelaria Hernández-Goya. "Self-organized authentication in mobile ad-hoc networks." *Journal of Communications and Networks* 11.5 (2009): 509-517.

[3] Xiaoyan Huo. "Blockchain-based distributed network security architecture with smart contract vulnerability detection using improved tree cnn." *Informatica Journal* Vol43, N 17 (2025). https://doi.org/10.31449/inf.v49i17.8050

[4] Rathod, T., Jadav, N. K., Alshehri, M. D., Tanwar, S., Sharma, R., Felseghi, R. A., &Raboaca, M. S. (2022). Blockchain for future wireless networks: A decadesurvey. *Sensors*, *22*(11), 4182.

[5] Soni, P. R., Joshi, C. A., Bhadra, D. R., Vyas, N. P., &Jhaveri, R. H. (2020). Various Secure Routing Schemes for MANETs: A Survey. *arXiv preprint arXiv:2004.06378*.

[6] Sangheethaa, S. (2023). A Comparative Study for Block Chain Applications in the MANET. *Int. J. AdHocNetw. Syst*, *13*(3).

[7] Liu, G., Fan, N., Wu, C. Q., & Zou, X. (2022). On a blockchain-based security scheme for defense against malicious nodes in vehicular ad-hoc networks. *Sensors*, *22*(14), 5361.

[8] Gajewski, P., Łopatka, J., &Łubkowski, P. (2022). Performance analysis of public safety cognitive radio MANET for diversified traffic. *Sensors*, *22*(5), 1927.

[9] Lo, S. K., Liu, Y., Chia, S. Y., Xu, X., Lu, Q., Zhu, L., & Ning, H. (2019). Analysis of blockchain solutions for IoT: A systematic literature review. *Ieee Access*, *7*, 58822-58835.

[10] Tanweer Alam, "IBchain: Internet of Things and Blockchain Integration Approach for Secure Communication in Smart Cities." *Informatica Journal*. Vol 54, N 3 (2021)

[11] Shukla, M., Joshi, B. K., & Singh, U. (2021). Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET. *Wireless Personal Communications*, *121*, 503-526.

[12] Wang, P., Zhou, M., & Ding, Z. (2021). A two-layer IP hopping-based moving target defense approach to enhancing the security of mobile ad-hoc networks. *Sensors*, *21*(7), 2355.

[13] Patil, Sandeep Jagonda, Lalita Sunil Admuthe, Ashwini Sandeep Patil, and Saurabh R Prasad. 2024. "Secure MANET Routing with Blockchain-Enhanced Latent Encoder Coupled GANs and BEPO Optimization." *Smart Science* 12 (4): 608–21. doi:10.1080/23080477.2024.2355750.

[14] Francis, H., Shajin., Muthusamy, Palaniappan., P., Rajesh. "Auto-metric Graph Neural Network based Blockchain Technology for Secured Dynamic Optimal Routing in MANET." International Journal of Computer Network and Information Security, 16 (2024).:123-132. doi: 10.5815/ijcnis.2024.01.10

[15] N., A., Ghodichor., Dinesh, K., Sahu., Gautam, M., Borkar., Ankush, D., Sawarkar. "Secure Routing Protocol to Mitigate Attacks by Using Blockchain Technology in Manet." abs/2304.04254 (2023). doi: 10.48550/arXiv.2304.04254

[16] ILAKKIYA, N. et RAJARAM, A. Blockchain-assisted secure routing protocol for cluster-based mobile-ad hoc networks. *International Journal of Computers Communications & Control*, 2023, vol. 18, no 2.

[17] Sugumaran, V. R., &Rajaram, A. (2023). Lightweight blockchain-assisted intrusion detection system in energy efficient MANETs. *Journal of Intelligent & Fuzzy Systems*, *45*(3), 4261-4276.

[18] Ilakkiya, N., &Rajaram, A. (2024). A novel DAG-blockchain structure for trusted routing in secure

MANET-IoT environment. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-20.

[19] Abdel-Sattar, A. S., &Azer, M. A. (2022, May). Using blockchain technology in MANETs security. In *2022 2nd International Mobile, Intelligent, and UbiquitousComputingConference (MIUCC)* (pp. 489-494). IEEE.

[20] Subhita, Menon., Divya, Anand., Kavita., Sahil, Verma., N.Z., Jhanjhi., Rania, M., Ghoniem., Sayan, Kumar, Ray. "Blockchain and Machine Learning Inspired Secure Smart Home Communication Network." Sensors, 23 (2023).:6132-6132. doi: 10.3390/s23136132

[21] Abid, Ali., Muhammad, Munwar, Iqbal., Sohail, Jabbar., Muhammad, Nabeel, Asghar., Umar, Raza., Fadi, Al-Turjman. "VABLOCK: A blockchain-based secure communication in V2V network using icn network support technology." Microprocessors and Microsystems, 93 (2022).:104569-104569. doi: 10.1016/j.micpro.2022.104569

[22] Sangheethaa, S, Arun, Korath. "Comparison of Algorithms used in Blockchain-based Mobile Ad Hoc Networks (MANETs)." International journal of science and research, null (2023). doi: 10.21275/sr23404135052

[23] Verma, Ravi., Sharma, K., Pramod., Jain, Neelesh., Agrawal, Chetan. "Enhancing MANET communication services through blockchain technology." Nucleation and Atmospheric Aerosols, null (2022). doi: 10.1063/5.0115134

[24] Hassija, V., Chamola, V., Gupta, V., &Chalapathi, G. S. (2020, June). A framework for secure vehicular network using advanced blockchain. In *2020 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 1260-1265). IEEE.

[25] Zhang, B., Li, J., Zheng, X., Ge, J., & Sun, J. (2019). A blockchain-based mobile IOT network interconnection security trusted protocol model. In *Cyberspace Safety and Security: 11th International Symposium, CSS 2019, Guangzhou, China, December 1–3, 2019, Proceedings, Part II 11* (pp. 372-381). Springer International Publishing.

[26] Biswas, A. K., &Dasgupta, M. (2020, October). Modification of DSDV and secure routing using blockchain technology. In *2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech)* (pp. 1-5). IEEE.

[27] G. Liu, H. Dong, Z. Yan, X. Zhou and S. Shimizu, "B4SDC: A Blockchain System for Security Data Collection in MANETs," in IEEE Transactions on Big Data, vol. 8, no. 3, pp. 739-752, 1 June 2022, doi: 10.1109/TBDATA.2020.2981438.

[28] Mouchfiq, N., Benjbara, C., &Habbani, A. (2020). Security in MANETs: The Blockchain Issue. In *Advanced Communication Systems and Information Security: Second International Conference, ACOSIS 2019, Marrakesh, Morocco, November 20–22, 2019, Revised Selected Papers 2* (pp. 219-232). Springer International Publishing.

[29] V., Lakshman, Narayana., Divya, Midhunchakkaravarthy. "A Time Interval based Blockchain Model for Detection of Malicious Nodes in MANET Using Network Block Monitoring Node." null (2020).:852-857. doi: 10.1109/ICIRCA48905.2020.9183256

[30] Ning, Zhao., Hao, Wu., Xiaonan, Zhao. "Consortium Blockchain-Based Secure Software Defined Vehicular Network." Mobile Networks and Applications, 25 (2020).:314-327. doi: 10.1007/S11036-019-01285-9

[31] S. Sangheethaa, "A study of applications of Blockchain in the MANET," *2023 9th International Conference on Smart Computing and Communications (ICSCC)*, Kochi, Kerala, India, 2023, pp. 355-359, doi: 10.1109/ICSCC59169.2023.10335032.

[32] P. K. Sharma and J. H. Park, "Blockchain-Based Secure Mist Computing Network Architecture for Intelligent Transportation Systems," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5168-5177, Aug. 2021, doi: 10.1109/TITS.2020.3040989.

[33] M. Baumgartner and J. Papaj, "Robust Data Transmission in 5G Networks Without Infrastructure Based on Blockchain Technology," *2022 32nd International Conference Radioelektronika (RADIOELEKTRONIKA)*, Kosice, Slovakia, 2022, pp. 01-04, doi: 10.1109/RADIOELEKTRONIKA54537.2022.9764944.

[34] S. Monga, P. Gupta, J. Logeshwaran and T. Thamaraimanalan, "Secure Decentralization: Examining the Role of Blockchain in Network Security," *2024 2nd World Conference on Communication & Computing (WCONF)*, RAIPUR, India, 2024, pp. 1-6, doi: 10.1109/WCONF61366.2024.10692123.

[35] Inzimam, A. K. Bishnoi and C. Menaka, "Enhancing Network Security with Blockchain Technology," *2024 International Conference on Optimization Computing and Wireless Communication (ICOCWC)*, Debre Tabor, Ethiopia, 2024, pp. 1-5, doi: 10.1109/ICOCWC60930.2024.10470901.

[36] BEGOÑA, MENDIZABAL, ELEZKANO., Ana, Prieto, Sánchez., LETICIA, MONTALVILLO, MENDIZABAL., AITOR, URBIETA, ARTETXE. *"Smart contracts: an opportunity to move towards new business models in industry."* Dyna, 99 (2024). pp. 557-559, doi: 10.52152/d11124