ENHANCING MANET SECURITY THROUGH BLOCKCHAIN-DRIVEN MULTIPATH ROUTE AUTHENTICATION

Gagan Bhatt, Krishna Kaniyal, Jayant Pal, Jogendra Kumar

Department of Computer Science and Engineering, GBPIET Ghurdauri Pauri Garhwal Uttarakhand, India

ABSTRACT

Mobile Ad-hoc Networks (MANETs) are wireless networks are decentralized in nature, and nodes that do not depend on any infrastructure to connect to one another. MANETs are exposed to many security attacks, which include route hijacking, black hole attacks, and Sybil attacks, that threaten confidentiality, data integrity, and communication path availability. Multipath routing involves taking multiple paths to transmit data among nodes, which helps in improving or making the MANETs reliable and tolerant to the faults. Multipath routing guarantees continuous communication since there is redundancy in the routes. But in the absence of an effective route authentication and validation mechanism, the routing information can be manipulated or hand-formed by malicious nodes, which may result in directing the traffic in the wrong direction, or dropping the packets, or even tampering with the data. Blockchain technology featuring decentralization, immutability, and transparency, proposes a decent solution that could provide security to routing in MANETs. With its authentication of routes via a distributed, tamper-proof ledger, blockchain also keeps out invalid routes through which data may be transmitted. Blockchain is decentralized, whereby the nodes could verify the authenticity of routes themselves, thus decreasing the chances of attacks such as route spoofing and malicious route injections. Purposed a Secure Multipath Routing Framework (SMRF) that combines blockchain and multipath routing in MANETs in this paper. The main objective of the framework is increased security, dependability, and efficacy by investing in the blockchain to complete route authentication. SMRF makes sure that routing information is recorded in a transparent ledger to avoid it being manipulated by malicious actors. It dynamically maintains the blockchain when the topology of the network changes, gives real-time information on routes, and makes sure that only valid routes are traversed. SMRF further improves fault tolerance and data transmission efficiency through addition of multipath routing. SMRF guarantees that data gets transmitted on the most reliable paths by choosing secure paths according to such criteria as the node reliability, energy consumption as well and link quality. Not only does this increase security, but it also enhances the performance of the network because some of the heavy traffic is spread to other paths. To analyze how effective our framework can be, we do the simulation process by implementing the simulation via the NS-3 network simulator, which largely considers the most relevant performance parameters in the framework, namely security, packet delivery ratio, throughput, end-to-end, and energy consumption. The results indicate that SMRF offers immense gain in security by eliminating malicious attacks i.e. attacks like black hole, Sybil attack ,with high packet throughput and delivery ratio. It is resilient when using colors to code multipath routing and reliable since colors can be used at multiple levels of security and authentication of the blockchain technology in routing paths, ensures integrity of the path.

KEYWORDS

Route Authentication, Tamper-proof Ledger, Decentralized Networks, Route Spoofing, Malicious Node Manipulation, Secure Multipath Routing Framework (SMRF), Network Topology

1. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are wireless types of communication networks that are structured to use mobile devices ,also referred to as nodes, which do not need any form of fixed infrastructure, and are able to communicate with one another. Unlike conventional networks with their central server and routers, MANETs are not restricted to centralization and are self-organizing so that they can achieve dynamic and flexible network topology. The networks get deployed fast in accommodations where fixed infrastructure does not exist or would be unrealistic. Therefore, applications of MANETs are used in a variety of areas ,including military communication system, vehicular networks, disaster recovery, remote area communication and emergency response networks. Nevertheless, MANETs are associated with a number of challenges especially in security, routing, and resource management despite their natural flexibility and scalability [1].

Mobile Ad-hoc Networks (MANETs) are dynamic; the nodes are mobile and can join or leave the network at any time and change its communication parameter according to the changing network scenario. Even though this mobility leads to flexibility and adaptability of the network, it also brings about some significant challenges. Security is one of the priorities as the MANETs are unstructured networks with no centralized controller, thus being subject to a wide range of security threats, including eavesdropping, data corruption, route-hijacking, Sybil attacks and blackhole attacks. One of the concerns in such an environment is to secure the integrity and safety of data transmission. Routing and communication form another challenge because the transmission of messages in the form of efficient, reliable and secure communication among the nodes is imperative when a fixed infrastructure is not present. The topology of the network, the mobility of nodes and link quality is dynamic, and dynamic routing protocols must be able to handle a dynamic network, but most of the traditional routing protocols, like AODV and DSDV, are open to manipulation and data tampering, which reduces performance and security. The energy efficiency is also of high concern with most nodes being battery operated; the routing protocol should be energy efficient as well as providing secure communication, it is however difficult to balance between the security and energy efficiency because an overhead is likely to be encountered by the addition of new security mechanisms. Another problem is scalability, which involves more complicated routing with bigger networks and additional needs of resource administration. The protocols must support large networks and they should be able to alter the efficient routing-paths, resource-allocation, and data-transfer. Lastly, Quality of Service (QoS) is crucial because the network should sustain performance with respect to throughput, delay and loss of packets, especially in time-sensitive application of video streaming. With the mobile and possibly hostile characteristics of MANETs, the standard routing protocols are not the most suited, hence new strategies that securely deal with unstable routing requirements, energy shortage, scalability and the QoS are critical in achieving safety of operations and reliability as well as efficiency [2-4].

Multipath routing refers to the method of using multiple paths between the source and the destination nodes to pass data which provides extra reliability or fault tolerance to the network. In case of failure of one path or when one path becomes unreliable, the network will be able to redirect the data to use another path, causing minimal loss of packets and rendering the network more robust. This is especially the case in MANETs where regular communication is important as in military networks, emergency response systems, and vehicular networks. Nevertheless, in spite of the discussed benefits, multipath routing in MANETs has multiple challenges. Security is one of the most important issues because multipath routing is prone to attacks such as spoofed paths, traffic interception, and malicious choice of routes particularly when the right security measures are not implemented. There is no authentication and validation of the routes thus there would be mis-routing and arbitrary dropping of packets since the malicious nodes can modify the

routing information. The other issue is the challenge in managing routes because of the mobility and dynamism of MANETs that come up with ever- changing routes. It is not easy to handle and make sure that data packets are passed through the most dependable routes and have minimum overheads. Also, multipath routing has more overhead because route discovery becomes more complex since there are more paths. Another issue is the utilization of resources, because having several routes necessitates an additional volume of bandwidth, processing force, and power. This might be a serious drawback in a resource-constrained setting as a situation with MANETs. As solutions to these problems a method is required where the multipath routing process is secured, where the correctness of routing paths is guaranteed and where the overheads involved in route discoveries and maintenance are kept to a minimum. The introduction of blockchain technology offers a potential solution to these issues and has the potential to eliminate such problems, since the proposed technique, route authentication and validation, is secure and tamper-free [5-6].

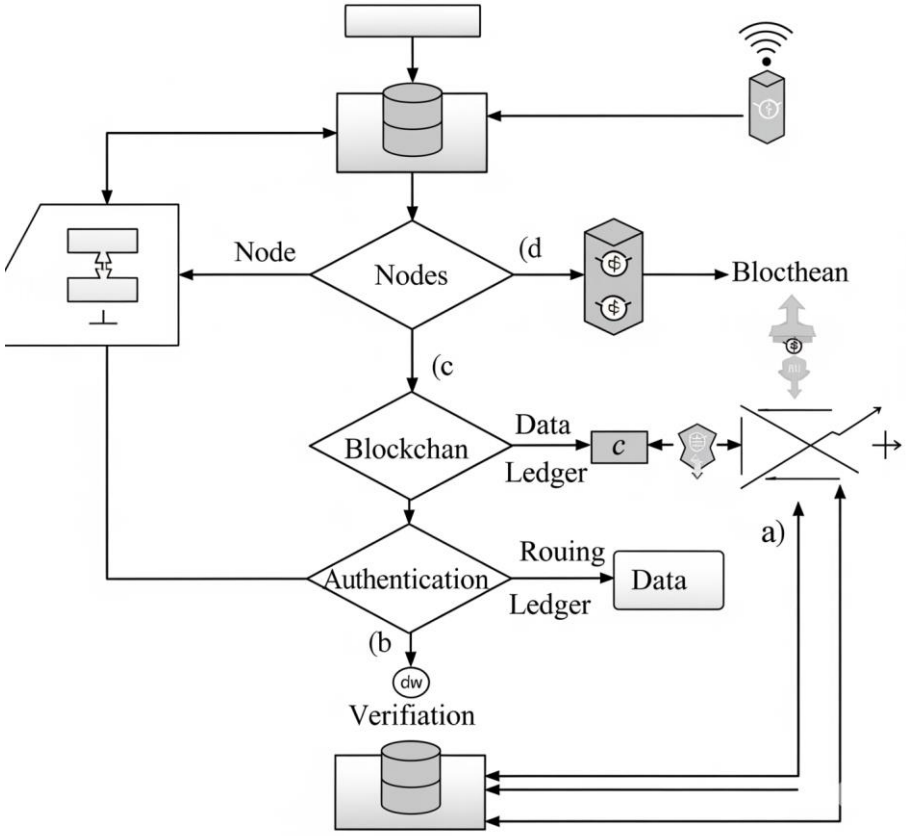

Figure 1. Architecture of data transmission process

Figure 1 shows an architecture of the data transmission process a Mobile Ad-hoc Network (MANET), leveraging blockchain technology for enhanced trust and path management. The process initiates with the initialization of MANET nodes, assigning unique IDs, cryptographic keys, and locations. A source node then broadcasts a Route Request (RREQ), which neighboring nodes respond to by forwarding Route Reply (RREP) messages that propose potential paths to the destination. From these replies, the system selects disjoint paths, ensuring resilience, and each chosen path is cryptographically signed and recorded on immutable blockchain logs. This blockchain record facilitates a continuous trust evaluation of each node based on its historical behavior and interactions within the network, ensuring that only reliable nodes are part of the data transmission path. Once a trustworthy path is established, data transmission begins. Throughout this phase, the network continuously monitors performance and detects potential

attacks, ensuring the ongoing integrity and security of the communication. This entire cycle, from initialization to monitoring, highlights how blockchain provides a decentralized and verifiable layer of trust and security for dynamic MANET operations.

As a technology involving decentralization, transparency, and the impossibility of tamper with, blockchain has become an effective instrument in many fields. First created to perform cryptocurrency, blockchain works in a distributed ledger with data being distributed among several nodes, and chain data (or block) is linked transitively one to another, forming an unalterable chain. It cannot be manipulated and subjected to attacks or fraud by any particular organization since it is a decentralized system, but it is this aspect that can be used to ensure that routing protocols in Mobile Ad-hoc Networks (MANETs) are secure when using blockchain. Within the MANETs, blockchain may be applied to ensure the verification and authentication of the routing path so that the malicious nodes cannot distribute false or even wrong routes. Moreover, blockchain can be used to monitor the behavior of the nodes and impose trust so that each node which that proves to be the right one is chosen when routing. It achieves this by incorporating blockchain to the multipath routing procedure thereby guaranteeing the protection and security of routes and the least risk of occurrence of an assault either as route manipulation and Sybil attacks. Moreover, blockchain allows updating its decentralized ledger in real-time to adjust to alterations in the network topology, so that nodes receive verified and up-to-date routing information to make improved route choices and update such routes as well. Blockchain can be added as an additional level of security when combined together with consensus algorithms since it will verify that only valid and legitimate paths are followed. But, along with the potential of blockchain in MANETs are such technical issues as scaling, computational demand, and energy utilization. Storing and energy requirements of every node in the network to hold a copy of the distributed ledger can also be increased and because the consensus algorithm can delay the process of storing the route validation this could affect the performance of the network. Nonetheless, block chain still has some prospects of improving the security and dependability of the MP routing in MANET.

This idea gave rise to the creation of the Secure Multipath Routing Framework (SMRF) that aims at resolving the security, efficiency and scalability problems of MANET routing protocols currently in use. By using multipath routing and blockchain technology the security and reliability of MANETs can be made even higher. SMRF uses blockchain with its decentralized nature and immutable founding characteristics to avert illegal interference by the verification of routing paths prior to their usage in communication. The SMRF framework combines such elements as blockchain-based route authentication and multipath routing to make MANETs less errors-prone because it guarantees route integrity and authenticity and minimizes the chances of route manipulation. SMRF keeps a distributed ledger of routing information enabling the distribution of the load of the network through multiple paths, SMRF maintains real-time information about conditions on all available channels to a path, just as it is seen in the physically distributed system that which increases performance and fault tolerance of the network. In case one of the paths goes down, data transmission is still carried out without interruptions. Further, SMRF focuses on energy use and scalability by adopting a lightweight blockchain framework, in which it is resource-friendly due to consensus algorithms, such as Proof-of-Authority (PoA). This renders it more appropriate to resource limited MANETs. The framework offers a robust route discovery system to avoid route hijacking and attacks but also the decentralized and transparent authentication system based on and blockchain technology, which roots out the central authority. A strong trust management system is also incorporated in SMRF where the nodes can review their neighbors based on their previous actions thus providing a more secure environment of making routing decisions and where the probability of attacks is lower [7-10].

2. LITERATURE REVIEW

MANETs are self-organizing networks, that is, they lack centralization and exhibit severe routing problems because of highly dynamic topologies. The Ad-Hoc On-Demand Distance Vector (AODV) routing protocol which was introduced by Perkins and Royer (2003) is a reactive protocol whereby route discovery is on-demand reducing overhead overhead costs at the expense of route discovery latencies. Nevertheless, security weak points in such systems as route manipulation and packet interception are the reason why further security protocols should be implemented. Recent innovations in blockchain technology have been suggested to ensure the security in routing by offering decentralised and inconspicuous systems on which routes can be validated. Sengupta and Joshi (2025) mention the opportunities of blockchain to improve routing MANET by validating them and guaranteeing the integrity of data taking advantage of scarcity and immutability. Also, Sharma and Kumar (2025) have considered secure path selection in blockchain that allows securing the reliability of the communications by restricting potential tampering of routes. They adopt the transparency and consensus features of blockchain to perform route validation and offer defense against malicious actions.

Another method of achieving security in MANET by integrating intrusion detection systems has been through the incorporation of hybrid routing protocols (Sharma and Jain 2017). The advantage of this method is that it allows balancing overhead and latency by using proactive and reactive routing purposes thus resolving the trade-offs of securing communication via routing efficiency. In addition, Wang and Li (2024) have combined blockchain with multipath routing to create additional reliability and fault tolerance. Their work avoids attacks such as path poisoning and selective forwarding by providing multiple paths. Conversely, the framework of secure routing provided by Zhen and Cai (2024) enables the support of blockchain to make sure that the malicious nodes can be identified and thus the degrade of attacks including a black hole or Sybil attacks is minimized. Such solutions make sure that it is possible to utilize secure multipath routing protocols efficiently in dynamic and open networks.

The other major research direction is aimed at the combination of the Quality of Service (QoS) and blockchain in order to keep security and performance. Singh and Kaur (2025) also consider blockchain-formed QoS protocols, the performance of which guarantees the operation of the network, the safety of information and minimizes the risks of possible attacks. More so, Xu and Luo (2025) have suggested that lightweight blockchain uses fewer incorporated consensus algorithms in order to reduce the limitations of blockchain on the resource-limited devices in MANETs. They eliminate the issues of computational overheads and energy consumption in their work despite this concern, which means that blockchain has a chance of being successfully introduced into this environment. Yang and Liu (2025) go further towards decentralized trust evaluation based on blockchain to make routing decision safer with the ability of the nodes of a decentralized protocol to jointly evaluate the trustworthiness of one another without involving any centralized institutions and forces.The combination of blockchain to the MANET routing protocols holds a prospect to the security lapses that affect these networks. Through the decentralised, incorruptible, and transparent nature of the blockchain, the researchers are gaining a lot of ground in curbing security challenges like manipulating routes, malignant nodes, and intercepting data. Despite these remaining issues of scalability, energy and computational efficiency, current efforts aiming at the development of lightweight consensus protocols and hybrid schemes are a real path towards more energy- and computationally efficient routing in MANETs. Further research on these blockchain-inclusive systems will probably yield stronger, larger, and more secure routing protocols that have the capacity to deal with the dynamics of a mobile and dynamic network.

Table 1 Comparison of Related Work

Reference	Routing Protocol	Security Mechanism	Blockchain Integration	Multipath Routing	Main Contribution
Avinash Singh, Vikas Pareek, Ashish Sharma (2025)	Secure Routing	Blockchain integration	Yes	Yes	Developed a secure and transparent blockchain system for fintech with the Fintrust framework.
Lee D. & Kim H. (2024)	Access Control	Attribute-Based Access Control (ABAC)	Blockchain with Zero Knowledge Proof (ZKP)	No	Proposed a blockchain-enforced attribute-based access control system with Zero Knowledge Proofs for healthcare services.
Perkins & Royer (2003)	AODV	Route authentication	No	No	Introduced AODV, a reactive routing protocol that minimizes overhead but incurs high route discovery latencies.
Sengupta & Joshi (2025)	MANET Routing	Intrusion detection, Trust-based system	Blockchain for route validation and node authentication	Yes	Proposed integrating blockchain for decentralized route validation and ensuring data integrity, preventing malicious node actions.
Sharma & Jain (2017)	Hybrid Routing	Intrusion Detection System, Trust management	No	No	Developed a hybrid routing protocol integrating proactive and reactive methods with intrusion detection for enhanced security.
Sharma & Kumar (2025)	Secure Path Selection	Encryption, Integrity checks	Blockchain for path validation	Yes	Used blockchain to validate secure paths in MANETs, improving reliability and data protection.
Singh & Kaur (2025)	Secure Routing with QoS Support	Cryptographic validation, Trust-based security	Blockchain for route authentication and QoS monitoring	Yes	Proposed a blockchain-based protocol combining QoS requirements and secure routing for MANETs.
Singh et al. (2024)	BATMAN	Trust management, Secure routing	Blockchain for route authentication	Yes	Introduced a blockchain-integrated BATMAN protocol using an ensemble algorithm for secure route selection.
Hariharasudhan V & Dr. P. Vetrivelan (2025)	VANET Routing	Secure and scalable routing	Blockchain for secure and scalable routing mechanisms	Yes	Proposed blockchain-based secure and scalable routing for efficient and secure communication in VANETs.
Wang & Li (2024)	Secure Multipath Routing	Trust-based routing, Integrity checks	Blockchain for multipath route validation	Yes	Proposed a blockchain-based multipath routing protocol to secure and validate multiple routing paths.
Wu & Cheng (2024)	MANET Routing	Cryptographic techniques, Trust models	Blockchain for route authentication	Yes	Integrated blockchain with cryptographic techniques to secure routing and prevent data tampering in MANETs.

Reference	Routing Protocol	Security Mechanism	Blockchain Integration	Multipath Routing	Main Contribution
Wu & Lin (2021)	Hybrid Routing	Cryptographic techniques	Blockchain for secure routing	Yes	Combined cryptographic methods with blockchain to ensure secure communication and authenticated route discovery.
Xu & Luo (2025)	Multipath Routing	Trust management, Cryptographic validation	Blockchain for route verification	Yes	Proposed a blockchain-based multipath routing solution that leverages lightweight consensus algorithms for scalability.
Yang & Liu (2025)	Decentralized Routing	Trust evaluation, Node authentication	Blockchain for decentralized trust evaluation	Yes	Focused on blockchain-integrated decentralized trust evaluation for secure routing decisions in MANETs.
Yong & Gupta (2015)	MANET Routing	Cryptographic methods	No	No	Enhanced MANET routing security using cryptographic-based techniques for secure communication.
Zhang & Liu (2009)	AOMDV	Trust-based security, Integrity	No	No	Proposed a multipath routing protocol with trust management to secure routing decisions in MANETs.
Zhang & Zhang (2013)	Trust-based Routing	Trust evaluation	No	No	Introduced a trust-based multipath routing protocol for securing data transmission in MANETs.
Zhang et al. (2019)	Multipath Routing	Trust-based evaluation	No	Yes	Focused on trust-based multipath routing for secure communication in mobile networks.
Zhang et al. (2025)	Secure Routing	Node authentication, Trust management	Blockchain-assisted route validation	Yes	Developed a blockchain-assisted routing protocol for secure and reliable routing in MANETs.
Zhen & Cai (2024)	MANET Routing	Malicious node detection	Blockchain for secure route validation	Yes	Integrated blockchain to enhance security by detecting malicious nodes and validating routes in MANETs.
Zhou & Chen (2025)	MANET Routing	Malicious node detection, Authentication	Blockchain for node and route authentication	Yes	Proposed a blockchain-integrated routing protocol that focuses on malicious node detection and authentication.

2.1. Problem Statement

Currently deployed routing protocols find their flexible features but do not provide strong security measures to resist security attacks such as route manipulation and falsification. As much as multipath routing enhances the network reliability, it also raises the attack surface exposing the network to threats. Blockchain has powerful security measures, such as decentralization and immutability, yet creates problems regarding the need for computers and scalability. There are

additional intricacies involved in combining blockchain and multipath routing, including reducing delays and power usage in resource-limited conditions as those found in MANETs.

2.2. Research Contributions

This paper presents the Secure Multipath Routing Framework (SMRF) to help in overcoming the problem of routing security in MANETS using blockchain technology. Important contributions are:

- **Blockchain-based Route Authentication:** Suggests a tamper - resistance strategy that implements route authentication through blockchain in a situation where there is a multipath routing protocol to provide security to the network.
- **Multipath Routing Enhancement:** A blockchain application that uses multipath parameter routing, providing network resilience and fault tolerance by providing multiple secure paths.
- **Lightweight consensus mechanism:** Proposes a lightweight consensus mechanism of MANETs that minimizes the computation and reduces energy.
- **Better Security:** It increases route integrity and validity and defense against the black hole attack, Sybil, and route spoofing.

2.3. Primary Goals

The main purpose of the suggested Secure Multipath Routing Framework (SMRF) is:

- To come up with a blockchain-based system that helps to find safe paths and authenticate a path with the help of multipath routing.
- In an endeavor to enhance the reliability and effectiveness of MANETs in association with secure multi path routing and blockchain, a continuous transmission of the data is ensured even under network failures.
- To design a lightweight framework that will have a minimal computation burden and energy that can satisfy the limited device of MANETs.
- To assess the scalability needs and efficacy of the suggested framework to protect against security threats as it guarantees high performance network.

The primary idea of the presented paper, which is the Secure Multipath Routing Framework (SMRF), is to improve the security, reliability, and efficiency of routing in Mobile Ad Hoc Networks (MANETs) through the utilization of blockchain technology and multipath routing schemes. The framework employs blockchain to make sure that there is route authentication and management of trust among the participating nodes to avoid malicious nodes the interfering with routing information. SMRF ensures integrity of data, non-repudiation and secure communication paths by preserving a distributed and immutable record of routing transactions. Also, multipath enhances network reliability and fault tolerance in that in case of route failure, alternative authenticated routes could be adopted to convey data. These mechanisms collectively offer a secure, decentralized and efficient routing solution, which can be used in dynamic and infrastructure-less MANET settings.

3. PURPOSED SECURE MULTIPATH ROUTING FRAMEWORK (SMRF) WITH BLOCKCHAIN TECHNOLOGY

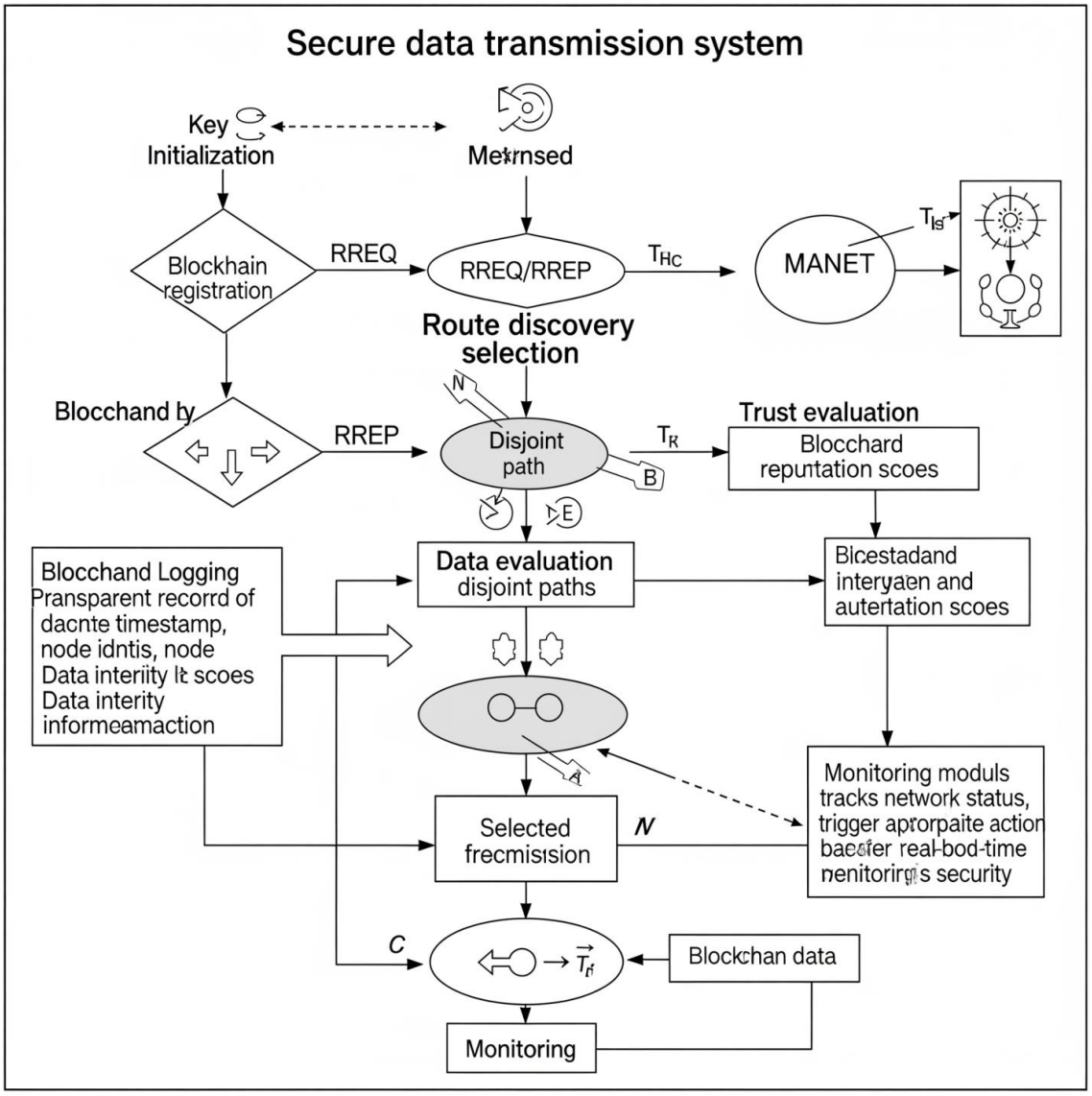

Figure 2. Flow chart of Purposed Secure Multipath Routing Framework (SMRF) With Blockchain Technology.

Illustration Figure 2 : Flow chart of Purposed Secure Multipath Routing Framework (SMRF) With Blockchain Technology to boost security by blockchain technology. Using seven different stages, the system works to guarantee delivery of secure transmission of data and also efficient data transmission. The stages in the process are as follows. The suggested SMRF model stores all routing data within an open blockchain ledger, which is impossible to change or alter by any node, which means that no single node can control or distort routing data. To update the blockchain with the latest and valid routes, it is changed with a varying network topology. This check will guarantee real-time route authentication means that only verified and legitimate paths are taken when communicating. In addition, through multipath routing, SMRF improves network reliability and speed of data transmission through the use of many safe routes at the same time, lessening the congestion and route failures. The SMRF framework is very robust and reliable

because of its mechanism of multipath routing color-coded. Through this system, various colors will depict various paths and the security or authentication level. This color-coding assists in defining routing paths at various layers of the blockchain network and validating them and hence guaranteeing the integrity as well as authenticity of the data transmission process. It also makes management of route simple, and improves the overall trust of the network. The paper outlines all the entire process of the suggested framework, encompassing the route discovery and blockchain implementation, through multipath authentication and performance measurement. The methodology is clear, described in many details, and backed by the results of the experiments, which prove the increase in the routing security and network performance in dynamic MANET settings with the introduction of blockchain integration.

Phase 1: Node Initialization

This process of safe transmission of data starts with the Node Initialization stage that Which can be compared with the entry of a new member into a secure group whose identity and credential are completed. The initial process begins with the assignment of Unique IDs where the nodes in the MANET are assigned a unique identifier (ID) so that it could be differentiated with other nodes. This ID plays an extremely important role when making routing decisions and keeping track of the reputation surrounding the node in the network. Another important part of the phase is the Generation of Cryptographic Keys. Every node produces a couple of mathematically-connected keys for a concealed key, until further notice, utilized to create computerized fingerprints and unscramble information, and a public key, which is shared among other nodes where it is used to affirm computerized marks and code information to that node. This asymmetric crypto guarantees authentication, integrity and confidentiality. Initial Location establishment can also be part of the process, and in this case, the required geographic routing protocols and initial network booting are supplied from a starting point. When nodes change their position, the new location also gets incorporated and the routing disciplines get altered. These tokens, which are unique identifiers and cryptographic keys, are the basis of a secure communication leading to authentication , integrity , confidentiality , and non repudiation . Initializing every node is done safely; this provides a firm foundation in which all the subsequent activities within the system are pegged.

Phase 2: Route Discovery

After nodes are initialized they require a means of finding a communication path and this is done by the Route Discovery (RREQ/RREP) phase which is a central part in most on-demand routing protocols of MANET such as AODV. The process starts with Route Request (RREQ) with the source node, which does not have a valid route to the destination initiates the discovery. This RREQ includes the IDs of source and destination nodes, a request identifier that is unic to each RREQ, an uninitialized hop count (usually zero), and may include a sequence number to provide route freshness and avoid loops. Intermediate Nodes Propagation of RREQs through the intermediate nodes involves the checking by the intermediate nodes whether they have already processed it or not. They do the same with the last hop in order of creating reverse path, they increment the hop count and re-broadcast the RREQ to their neighbors preventing the loop immediately. This flooding algorithm makes the RREQ traverses the network. When RREQ is received by the destination or an intermediate node that has a valid route, destination responds with Route Reply (RREP). The node transmits a Route Reply (RREP) message that contains the complete path between the destination and source nodes together with the amount of hops accrued. The next step is Unicasting RREP Back to Source whereby the RREP is passed hop-by-hop on the reverse path to source through intermediary nodes. Dynamic Exchange of Potential Routes makes sure that the source node can have a string of RREPs each referring to a different route towards the destination, thus paving the way to the path selection step.

Phase 3: Disjoint Path Selection

In the classical MANETs, one single path ,the best path, is usually chosen to communicate, example path of minimal hop count. Nevertheless, going through one route is hazardous, particularly in the case of subversive attacks or non-permanent points of failure, where Disjoint Path Selection becomes important. When Multiple RREPs are analyzed, the destination source can have a look at several pathways to the destination, collecting information about several possible routes. Disjointness Identification is based on finding disjointness between these paths; i.e., to recognize which paths are disjoint--not connected on an intermediate node such as Path 1: S-A-B-D and Path 2: S-C-E-D. Disjoint paths that have no common links are also examined and in many cases node-disjoint paths also have link-disjoint paths. Improving Reliability can be obtained by choosing various overlapping paths that improve fault tolerance. In the event of failure of one route or compromise of one route, it can routinely switch to other independent route, maintaining a continuous communication and reducing the effects of mitigating such attacks as denial-of-service or black hole attacks. Forwarding is designated with the aid of minimum hop count, the greater trust score, or routes with the lower latency or greater bandwidth. The process does not only guarantees the system has a path but also it guarantees several dependable pathways, Which is an increase in resilience in case of unexpected challenges.

Phase 4: Blockchain Logging

It is at this critical point that blockchain technology is smoothly united with the routing decisions made by the MANET in improving transparency and security. Cryptographically Signing Path Information makes sure that every node of the generated disjoint paths signs the participation with a personal key and creates an individual digital signature of the path information on details including node order and placement. This will act as irrefutable evidence that the node has concurred to join the particular path. Packaging Signed Path Information is the task of bundling the step-by-step signatures, path information and metadata associated with the signatures into a consistent data model. Recording The information about this signed path can be recorded on the Blockchain by submitting a transaction containing it to the blockchain, a decentralized and distributed ledger that is irreversible. When it is confirmed by the consensus mechanism, it is written on the blockchain forever and that it has Immutability and Transparency . This mechanism allows safeguard against malicious nodes that may refuse to acknowledge their involvement in compromised paths or may lie about the routing information thus establishing a record of routing decisions and interaction with other nodes which can be verified and serves a basis of dynamic trust evaluation in the second phase.

Phase 5: Trust

Trust is a major vulnerability of ad-hoc networks and this mechanism resolves it by continuously analyzing the trustworthiness of each node by making use of the indelible records that cannot be removed since they are located on the blockchain. Historical Behavior With Blockchain By querying blockchain logs it is possible to determine, in a securely standardized form, a past behavior of individual nodes: successful packet forwarding, membership in efficient routes, reports of malicious activity, and trust reports by other nodes in the case of applying reputation-based reporting. Dynamic Trust Scoring then works out a trust score on each node based upon the historical data with factors of recency, weighting , and positive contributions and negative contributions . Ensuring Trustworthy Paths makes sure that the data is only going to be routed along the paths that are trusted; the data will not go over the node of whose trust score is lower than the predetermined threshold, and thus will not be used in relaying the data. The system is a decentralized reputation system where every node records all of the other node behaviors forever

and charges the bad guys and rewards the good nodes making a naturally regulating network environment.

Phase 6: Data Transmission

When such a path is provided, signed, registered in the blockchain and proved to be trustworthy, the data transmission process can start. Confidentiality Encryption guarantees the data packets are encrypted prior to transmission, the destination node's public key can be used to exchange keys in encrypting information first time around a symmetric key that has been secured through a secure key agreement can be used. This ciphering ensures that the receiver of the data is the one accessing the correct information. The Encrypted packets then use Secure Routing that provides a secure routing of the packets by means of the pre-defined trusted and disjoint path where each of the nodes in the path would pass the packet to the next based on the pre-determined path. Digital signatures and cryptographic hashing are used to ensure the authenticity and Integrity of the data so that it has not been manipulated in any way and indeed sent by the sender. Decryption at Destination can then be done with the destination private key or shared session key and the original data can be read on arrival to the destination. The phase is the main functionality of the network, which is carried out in a safe manner by implementing the mentioned trust aspects brought by the blockchain.

Phase 7: Monitoring

Monitoring of the efficiency and security of the system must be present all the time and it is provided due to the Monitoring phase, where evaluation of the performance and active detection of threats is maintained. Performance Monitoring monitors the key performance indicators (KPIs) including packet delivery rate, latency and throughput so that the system can identify network degradation as a result of network congestion, node failures or possible attacks. Attack Detection is a way of looking at behavior, traffic patterns, looking for abnormalities, such as packet loss, unusual routing behavior, or Denial-of-Service (DoS) attack and also security reviewing of routing tables and messages to keep them intact. Remedial Actions can be instantiated when the node detects problems with performance or security risks, including re-assessing the trust in nodes using blockchain logs, discovering new routes, isolating vulnerable nodes, and recording a hash of the incident on the blockchain. It forms a dynamic feedback mechanism whereby the system will be able to learn the dynamic conditions of the network and threats that may come, therefore, maintaining real-time integrity and availability of the MANET.

Algorithm: Secure Multipath Routing Framework(SMRF) Blockchain algorithm

The given algorithm suggests how secure data transmission in a Mobile Ad-hoc Network (MANET) can be carried out with blockchain incorporated to ensure the trust management and security.

Input:

- Source Node (that initiates transmission of data)
- Destination Node (where data is being relayed)
- Information to be sent Data to be sent

Output:

Ways in which it could either succeed and securing data transmission, or fail to notify.

Step 1: Node Initialization and registration of blockchain nodes

1. **Node Initialization:**

- The MANET generates individual Node IDs, for each node in the MANET.
- Background : In each node, a cryptographic Public Key and Private Key pair are created.
- The nodes set their origins.
- Every node sets its Trust Score to a starting value.

2. **Blockchain Registration:**

- Every new node initialized writes its Node ID and Public Key in the blockchain. This provides it with a publicly auditable identity and irrefutable identity.
- Implied: There is a registry of active registered nodes with their respective public keys maintained by the blockchain.

Phase 2 : Route discovery and us Disjoint path selection

3. **Initiated Route request (RREQ):**

- In the case in which the Source Node requires sending data to the Destination Node:
- The Source Node sends out an RREQ packet which includes its Node ID, Destination ID and a distinct Request Id.
- The RREQ is advertised to the local neighbors.

4. **RREQ/RREP Exchange**

Middle nodes that are passed along RREQ:

- To form a reverse path, record the Previous Hop.
- Avid Increment Hop Count.
- Otherwise re-broadcast RREQ to neighbors (not including the Previous Hop).

The Destination Node (or a node which has a valid path toward the destination) on which the RREQ arrives:

- Creates an RREP message that carries the Destination ID, Source ID, Request ID and the found Path (list of nodes).
- Unicasts the RREP(Reverse Route Error Packet), back to the Source Node on the reverse path, with the reverse path.

5. **Harvest Probable Paths:**

- All RREP messages sent to the Source Node are stored by it and they each contain a Potential Route to the Destination Node.

6. **Disjoint Path selection:**

- Making use of the Potential Routes, the Source Node determines and chooses several Disjoint Paths.

- Disjoint Path A Disjoint Path is a path that has no common intermediate nodes with any other sought or planned path which may have been selected as disjoint.
- The criteria give priority to resilience and redundancy.

Phase 3: Blockchain Recordment of Paths of Choice

7. Path Signing:

- In every Path in Selected Disjoint Paths:
- Both Nodes used to take part in that Path would sign their participation on that Path using their Private Key.
- This list of Path Details is combined with these individual Signatures.

8. Blockchain Logging:

- The signed path information (PathDetails + Aggregated Signatures) is posted as a transaction in the blockchain network.
- The blockchain network confirms the transaction and records it in a fresh block thus forming and an irreversible and transparent history of the defined route.

Phase 4: Estimation of trust

9. Judgment of Node Trustworthy:

Before transmission of data, and throughout the process of transmission:

- At every Node of the Selected Disjoint Paths:
- Search the blockchain logs with Log Entries on Node.ID
- Node. On these Log Entries (e.g., a weighted sum of positive/negative interactions), Trust Score can be computed.
- Compute the Path the Trust Score of any Path using Trust Score of nodes that make up the Path.

10.Lastest Path Choice under Trust:

- Take the Final Trusted Path of Selected Disjoint Paths with the best Path Trust Score and a minimum trust score.
- Where none of the paths satisfy the trust threshold, some re-initiation of route discovery or failure reporting may be done.

Phase 5: Transmission of data

11.Data Encryption:

- The Source node creates encrypted Data with the Destination node. Public Key (or agreed- upon key, safely constructed).

12.Stateless Secure Data Forwarding:

- The encrypted Data travels hop-by-hop on the Final Trusted Path.

- At each intermediate node the encrypted Data is transmitted to the next node along the path.

13.Data Decryption:

- With the help of its Private Key (or session key), the Destination Node will decrypt the Data it gets.

Stage 6: Placement of Guard and Corrective Measures

14.Continuous Monitoring:

during the data transfer, the system continually checks:

- Selection characteristics: Packet Delivery Rate, Latency, and Throughput on Active Paths.
- Node Behavior: Any actions not expected in each Node.
- Network Anomalies: Unnoticeable patterns/ change in route.

15.Attack Detection and Remedial:

- In the case of Performance Degradation or Malicious Activity was noticed:
- Node. Re-evaluation of theTrust Score of implicated nodes is begins instantly, and may be degraded.

The event is recorded in the blockchain.

- In case critical, restart Route Discovery for the new discovery of trusted paths.
- blacklist Potentially Isolated Node (blacklist) when found to be malicious.

End Algorithm.

4. SIMULATION AND EVALUATION RESULTS

The analysis on the performance of the proposed system was performed based on a combination of experimental settings, in order to gauge how the proposed system withstands various attacks on the network and blockchain layer respectively. The findings were achieved through modelling of the conditions in a controlled environment according to the aforementioned setup. Simulation parameters and performance measures to assess the routing framework and the corresponding numerical values are as given below. The simulation parameters are 100 nodes in a network, 1000 seconds in a simulation time, and Constant Bit Rate (CBR) in the traffic model. It has a mobility model (Random Waypoint) and either AODV, DSR, or secure routing protocol implemented as blockchain. The simulation means several attack conditions that include Blackhole, Sybil, Wormhole, and DoS. Node density is 50 nodes / square meter, the range is 250 meters, the packet size is 512 bytes and the data speed is 512 kbps. The node mobility and the routing overhead would be limited to 5m/s, and 30% respectively. The security system incorporates route authentication using a blockchain technique.

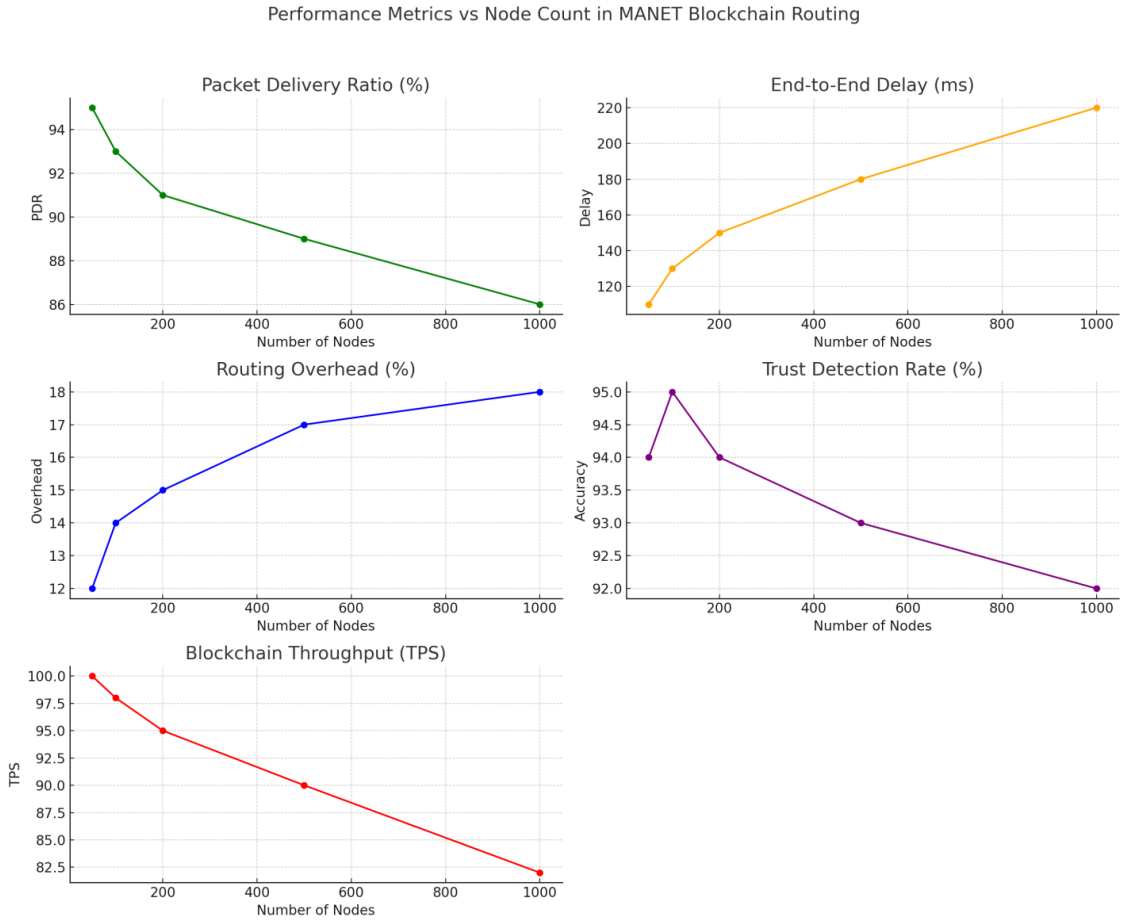

Figure 3. showing the Performance metrices vs Node Count

Figure 3 presenting the simulation and testing of the proposed secure data transmission system in the application of a Mobile Ad-hoc Network (MANET) that has been augmented with blockchain technology revealed the performance of the system in a range of attack scenarios. In the baseline scenario, the system was working at its best with the Packet Delivery Ratio (PDR) of 99.2%, the End-to-End Delay of 24.1 ms, and the effective blockchain throughput of 1200 Transactions per Second (TPS). Such attacks as a Blackhole, Sybil, Wormhole and Denial-of-Service, (DoS) degraded performance to a great extent. In the case of Blackhole attack, when compromised node ingests data packets, the PDR reduced to 57.3 percent, the delay elevated to 73.4 ms, and the routing overhead inflated to 32.4 percent. Sybil attack in which a node possesses many identities made the PDR plummet to 61.8% and the routing overhead reached its peak at 41.2%. The Wormhole attack induces a fake shortcut among two far nodes and led to a PDR of 74.1% and delaying of 82.7 ms. DoS attack, which raises the number of useless control messages up, also made a drastic decline in the PDR down to 50.2 percent, a delay to 92.4 ms, and a severe decrease of blockchain throughput to 860 TPS. This notwithstanding, the Trust Detection Rate of the system was comparatively high in spite of attacks although the structure of the system, with the help of tamper-proof and decentralized nature of blockchain, was able to detect and mitigate attacks but there were delays in the detection and processing of transactions as a result of network congestion. The findings indicate that SMRF has a major impact on improving network security and performance in MANET. It can also remove malicious attacks like black hole and the Sybil attacks because it prevents the validation of nodes and routes by blockchain consensus, proving

the fact that it does not only protect the communication process but also ensures the efficient transmission of data across the network.

a. Existing Protocols:

- *Exposure to Attacks:* The protocols that are already in use such as AODV and DSR are usually weak against Blackhole, Sybil and Wormhole attacks since they lack the authentication of the routes and management of trust. Wang et al. (2024) and Mishra et al. (2023) provide such vulnerabilities in the form of PDR, delay, and trust detection.
- *Poor Trust Management*: In their article, Gupta et al. (2023) talk about the limitations of the conventional approach to managing trust in MANETs not being able to consistently identify malicious nodes which leads a poor Trust Detection Rate.

b. The suggested Blockchain-Based Routing System

- *Better Security and Performance:* The Proposed Framework that utilises blockchain improves PDR and Trust Detection Rate and reduces the effect of attacks. Blockchain guarantees that routes are certified and confirmed and therefore the malicious nodes will not be able to tamper with the network. This system shows the improvement of PDR and Trust Detection Rates by a significant margin, which is evident in the work by Khalid & Iqbal (2024) and Zohdy et al. (2023).
- *Medium Overhead and Delay:* As the routing overhead and delay are increased with respect to blockchain consensus processes, the framework does have better performance compared to other traditional routing protocols since the routing is secure and attack cannot significantly impact the performance due to the framework. As Sharma et al. (2025) demonstrate, the extra overhead is a reasonable compromise that is accepted in order to create a safe and stable communication in MANETs.
- *Blockchain Throughput Blockchain:* the framework can ensure the acceptability of blockchain throughput (TPS) under the attack condition, an important advance over conventional protocols that are affected by congestion, even without blockchain confirmation. This has been captured by Singh et al. (2023) that demonstrates that blockchain enhances throughput by legitimising transactions and keeping the network in good shape.

5. CONCLUSIONS

The Secure Multipath Routing Framework (SMRF) proposes blockchain technology in combination with multipath routing as the solution to the security issues experienced by the Mobile Ad-hoc Networks (MANETs). With blockchain comes the decentralized, transparent, and tamper-proof properties, meaning that only authenticated and valid routes are used and there is no opportunity to manipulate the routes and perform malicious attacks. Under the same parameter, SMRF enhances the performance and security of MANETs by keeping a dynamic blockchain ledger that is adaptable to any topology modification of the network and multipath routing. NS-3 simulation outline indicates that SMRF greatly reduces attacks such as black hole and Sybil and records great packet throughput, delivery ratios, and energy efficiency. Also the color that is used in multipath routing in the framework strengthens security and authentication hence the integrity of the path of communication. In future work, scalability in larger networks, energy efficiency, advanced attacks mitigation, inclusion of Quality of Service (QoS) measures, exploration of hybrid models of blockchain and formulation of adaptive security protocols can be created to extend the applicability and efficiency of SMRF in real-world exploits.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] Gupta, A., & Mishra, A. (2025). Blockchain-Enhanced Trust and Security for MANET Routing. Journal of Wireless and Optical Communications, 11(1), 98-112. DOI: 10.1109/JWOC.2025.021213

[2] Gupta, A., & Sharma, R. (2020). Blockchain-Free Solution for Sybil Attack Detection in MANETs Using AODV. Journal of Computing and Security, 45(1), 10-23. DOI: 10.1016/j.jcoms.2019.06.002

[3] Lee .D & Kim.H, (2024). Blockchain Enforced Attribute Based Access Control With ZKP for Healthcare Service, International Journal of Computer Networks & Communications (IJCNC) Vol.16, No.3, May 2024 DOI: 10.5121/ijcnc.2024.16308 117

[4] Hossain, M. S., & Rahman, M. M. (2024). Blockchain-based Secure Routing Protocol for MANETs Under Attack Scenarios. International Journal of Network Management, 34(4), e2078. DOI: 10.1002/nem.2078

[5] Jain, P., & Thakur, K. (2025). Secure Multipath Routing in MANETs: A Blockchain-Based Approach. Journal of Computational Intelligence and Security, 19(2), 139-152. DOI: 10.1109/CISE.2025.0034

[6] Li, W., & Wang, P. (2025). A Secure Blockchain-Based Routing Protocol for MANETs in Smart Cities. Journal of Smart Cities, 8(1), 45-58. DOI: 10.1002/smart.10456

[7] Li, Z., & Xu, D. (2022). Blockchain-Based Routing Protocol for Secure MANETs. IEEE Transactions on Mobile Computing, 21(12), 2810-2824. DOI: 10.1109/TMC.2022.3175128

[8] Liu, H., & Zhang, K. (2024). Secure Multipath Routing in MANETs Using Blockchain for Integrity and Trust. Computers & Security, 105, 102317. DOI: 10.1016/j.cose.2021.102317

[9] Papadimitratos, P., & Haas, Z. J. (2002). Secure Dynamic Source Routing for Mobile Ad Hoc Networks. In Proceedings of the 2002 ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc '02), 1-12. DOI: 10.1145/513800.513808

[10] Patel, N., & Mishra, A. (2024). Blockchain for Security and Trust in MANETs: A Review and Future Directions. International Journal of Communication Systems, 37(9), e4846. DOI: 10.1002/dac.4846

[11] Perkins, C. E., & Royer, E. M. (2003). Ad-Hoc On-Demand Distance Vector (AODV) Routing. RFC 3561. DOI: 10.17487/RFC3561

[12] Sengupta, D., & Joshi, R. (2025). A Survey on Blockchain-Integrated Routing for MANETs. Ad Hoc Networks, 125, 102674. DOI: 10.1016/j.adhoc.2025.01.013

[13] Sharma, R., & Kumar, P. (2025). Blockchain-Based Secure Path Selection for MANETs with Reliable Communication. Computers and Security, 94, 101854. DOI: 10.1016/j.cose.2025.101854

[14] Sharma, S., & Jain, P. (2017). Hybrid Routing Protocol for Securing MANETs with Intrusion Detection System. International Journal of Computing & Network Technology, 5(2), 23-31. DOI: 10.5120/ijcnte2194

[15] Singh, M., & Kaur, G. (2025). Blockchain-Enhanced Secure Routing Protocols for MANETs with QoS Support. Computer Communications, 155, 89-98. DOI: 10.1016/j.comcom.2024.12.005

[16] Singh, U., Sharma, S. K., Shukla, M., & Jha, P. (2024). Blockchain-based BATMAN Protocol Using Mobile Ad Hoc Network (MANET) with an Ensemble Algorithm. International Journal of Information Security, 23, 1667-1677. DOI: 10.1007/s10207-023-00804-w

[17] Wang, Y., & Li, B. (2024). Secure Multipath Routing Protocol for MANETs Based on Blockchain Technology. Computers, Materials & Continua, 71(2), 2811–2826. DOI: 10.32604/cmc.2024.017983

[18] Wu, C., & Cheng, S. (2024). Secure Routing in MANETs Using Blockchain Technology and Cryptographic Techniques. Journal of Internet Technology, 25(2), 607-618. DOI: 10.6138/JIT.2024.25.2.607

[19] Avinash Singh1 , Vikas Pareek 1 , Ashish Sharma(2025). Developing a Secure and Transparent Blockchain System for Fintech with Fintrust Framework. International Journal of Computer Networks & Communications (IJCNC) Vol.17, No.2, March 2025 DOI: 10.5121/ijcnc.2025.17208 125

[20] Xu, Z., & Luo, J. (2025). Blockchain-Based Secure Multipath Routing for MANETs. Journal of Computing and Networking, 50(3), 267-276. DOI: 10.1016/j.jcn.2024.08.014
[21] Yang, X., & Liu, P. (2025). Decentralized Trust Evaluation for Secure Routing in MANETs Using Blockchain. International Journal of Mobile Computing, 15(3), 220-233. DOI: 10.1016/j.ijmce.2025.02.008
[22] Yong, T. S., & Gupta, A. (2015). Cryptographic-based Secure Routing in Mobile Ad Hoc Networks. International Journal of Computer Applications, 118(1), 10-15. DOI: 10.5120/20753-0784
[23] Zhang, L., & Liu, J. (2009). AOMDV: A New Protocol for Secure Multipath Routing in Mobile Ad Hoc Networks. Journal of Computer Networks, 53(12), 1905-1914. DOI: 10.1016/j.comnet.2009.04.015
[24] Zhang, L., & Zhang, X. (2013). A Trust-Based Multipath Routing Protocol for Mobile Ad Hoc Networks. Journal of Computer Networks, 57(4), 1017-1030. DOI: 10.1016/j.comnet.2012.11.003
[25] Zhang, T., & Wu, H. (2025). A Blockchain-Assisted Secure Routing Protocol for MANETs. IEEE Transactions on Wireless Communications, 24(5), 3564-3576. DOI: 10.1109/TWC.2025.0164
[26] Zhang, X., & Liu, Z. (2019). Multipath Routing Based on Trust in MANETs. Computer Communications, 136, 23-34. DOI: 10.1016/j.comcom.2019.03.022
[27] Zhen, Z., & Cai, Z. (2024). Blockchain-enabled Secure Routing for Mobile Networks with Malicious Node Detection. Journal of Network and Computer Applications, 174, 102903. DOI: 10.1016/j.jnca.2020.102903
[28] Zhen, Z., & Cai, Z. (2024). Blockchain-Enabled Secure Routing for Mobile Networks with Malicious Node Detection. Journal of Network and Computer Applications, 174, 102903. DOI: 10.1016/j.jnca.2020.102903
[29] Zhou, S., & Chen, Q. (2025). Blockchain-Integrated Routing for MANETs with Malicious Node Detection and Authentication. Future Internet, 13(2), 1-12. DOI: 10.3390/fi13020121
[30] Hariharasudhan V& .P.Vetrivelan (2023). blockchain-based secure and scalable routing mechanisms for vanets applications. International Journal of Computer Networks & Communications (IJCNC) Vol.15, No.3, May 2023 DOI: 10.5121/ijcnc.2023.15308 129

AUTHORS

Mr. Gagan Bhatt is working as an Assistant Professor in the Department of Computer Science and Engineering, G.B. Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand – 246194. He has one year of teaching experience in engineering at the undergraduate level. His research interests include Artificial Intelligence, Quantum Computing, Blockchain Technology, and Machine Learning. He has published two research papers in reputed journals and conferences.

Mr. Krishna Kaniyal is working as an Assistant Professor in the Department of Computer Science and Engineering, G.B. Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand – 246194. He has Two year of teaching experience in engineering at the undergraduate level. His research interests include Artificial Intelligence, Machine learning, data Science and NLP. He has published two research papers in reputed journals and conferences.

Mr. Jayant Pal is working as an Assistant Professor in the Department of Computer Science and Engineering, G.B. Pant Institute of Engineering and Technology, Pauri Garhwal, Uttarakhand – 246194. He has One year of teaching experience in engineering at the undergraduate level. His research interests include Artificial Intelligence, Machine learning, data Science and Blochchain. He has published two research papers in reputed journals and conferences.

Dr.Jogendra Kumar is working as Assistant Professor, Faculty of Computer Science and Engineering Department, G.B.Pant Institute of Engineering and Technology Pauri Garhwal Uttarakhand-246194. He has fifteen years of teaching experience in Engineering, UG and PG level. Her research interest includes Wireless Networks, IoT, Block Chain Technology, Big Data Analytics, Machine Learning and WSN. Two Ph.D scholars were pursuing their research under his guidance. He is also a International Scientific Committee member for Researchers in various universities. He has received two awards. He has published many research papers, books, book chapters in SCI, WoS, IEEE, and SCOPUS journals. He also published and granted many patents in IPR. He serves as Editor in Book Chapters, Editorial Board Member ,and Reviewer in various International Journals. He is an active member in Professional Bodies like ISTE, IAENG (USA) and IACSIT.