DECENTRALIZED BLOCKCHAIN-BASED TRUST AND SECURITY FRAMEWORK FOR COOPERATIVE MULTIPATH ROUTING IN WSNS AND IOT NETWORKS

Jogendra Kumar [1] ,Himanshu Bartwal [2] , Neetu Prajapati [3] , Gagan Bhatt [1]
[1] Department of Computer Science and Engineering
G.B.Pant Institute of Engineering and Technology, Ghurdauri, Pauri Garhwal
Uttarakhand-246194, India
[2] Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh-209305, India
[3] Department of Computer Science and Engineering, Women Institute of Technology
Dehradun, Uttrakhand- 248198, India

ABSTRACT

Wireless sensor networks (WSNs) and Internet of Things (IoT) networks have applications in smart cities, industrial monitoring, healthcare, and environmental surveillance, but since the networks have open wireless communication, resource constraints, and decentralized architecture, they are very susceptible to security threats such as malicious routing, manipulation of trust, and interference with data. Although cooperative multipath routing enhances fault tolerance and reliability via distributing traffic among more than one path, identifying correct evaluation of trust and ensuring the safety of coordination between the involved nodes are critical factors of success. Currently used trust based routing methods are generally centralized or a model of trust that is not affected by dynamic attacks, which restricts the ability to scale as well as the ability to withstand such attacks. The present paper suggests a decentralized blockchain-based trust and security system in cooperative multipath routing within the WSN and IoT systems. The framework combines lightweight blockchain technology and cooperative routing in order to offer safe, transparent, and tamper proof trust management. Network nodes keep an unchangeable distributed registry of routing behavior, updates of trust, and history of cooperation, which means that malicious nodes cannot lie or modify trust information. Smart contracts apply to compute the trust and route validation depending on the key performance indicators, including packet forwarding success, compliance with latency, and consistency of behavior, which are useful in dynamically determining reliable routing paths. Results obtained through simulation shows that the suggested framework has a better packet delivery ratio, routing stability, and resistance to blackhole, gray hole, and Sybil attacks than regular trust-based routing schemes, and has acceptable computational and communication overhead. This is because these findings demonstrate that the solution under consideration provides a scalable, cost-effective, and secure means of cooperative routing in next-generation WSN and IoT networks.

Keywords

Network Blockchain, Wireless Sensor Networks, Internet of Things, Cooperative Multipath Routing, Trust Management, Network security

1. INTRODUCTION

Wireless Sensor Networks (WSNs) and Internet of Things (IoT) have become significant technologies to support intelligent, data-driven, and autonomous systems in various areas of application. These networks are made up of huge population of sensor enabled nodes with the

ability to sense environmental conditions, process data and transmit information wirelessly to assist in real-time monitoring, control and decision making. The development of low-power electronics, embedded systems, and wireless communication technologies has made the use of WSNs and IoT networks possible at the large scale, thus, becoming the part of the contemporary cyber-physical systems, i.e. smart cities and industrial automation, healthcare monitoring, environmental surveillance, and intelligent transportation systems [1]. Their capacity to work in distributed and frequently unattended places renders them essential in large scale sensing and actuation activities. IoT sensors are installed in urban systems in smart cities to continuously monitor data regarding the traffic flow, air quality, noise levels, energy usage, and health of infrastructures. This information-based method will enable the capital city managers to manage resources better, enhance the delivery of services to people, and the overall well-being. In the factory, a combination of WSNs and IoT technologies can serve as the basic infrastructure of Industry 4.0, providing predictive maintenance, automated process control, equipment health, and real-time tracking of assets [2]. On the same note, in healthcare, WSNs are used in remote patient monitoring, wearable health devices, where data reliability and timeliness is paramount because any break in communication could result in serious safety threats. Environmental monitoring WSNs are also an important application in the fields such as forests, agricultural fields, oceans, and disaster-prone areas. Parameters that are measured by these networks include temperature, humidity, pollution, soil moisture, seismic activities, and movement of wildlife, which is very relevant in protecting the environment, managing disasters, and precision agriculture [3]. Nevertheless, wireless communication medium that is open by nature, decentralized network topology, and the low level of computational and energy resources of the sensor nodes render the WSN and IoT networks extremely susceptible to security threats. One of the most important issues in WSNs and IoT networks is routing security. The routing protocols decide the routes by which the data packets pass via the source nodes to the destination nodes, usually by taking the path of more than one intermediate hop. Failure or malicious nodes may take advantage of routing protocols to attack the system via blackhole attacks, in which packets are discarded; gray hole attacks, in which packets are forwarded selectively; Sybil attacks, in which a node adopts more than one identity; or by propagating false routing updates. These attacks have great impacts as they cause a significant reduction in the performance of that network in terms of packet delivery ratios, latency and data integrity and confidentiality. Cooperative multipath routing has been researched extensively in order to make them more reliable and fault-tolerant in such hostile environments [4]. With cooperative multipath routing, the data traffic is spread over multiple possible alternate routes instead of using one route. This strategy brings in redundancy, load balancing and resistance to node failures, congestion and attacks. In case one route is unable to serve the purpose of delivery via failure or other ill intentions, data will be passed through the other existing routes. Multipath routing specifically works well with large-scale and dynamic WSN and IoT implementations in which the network topology often varies. Although it has its benefits, the success of cooperative multipath routing strongly depends on the good cooperation of the involved nodes. The routing algorithm is based on the assumption that the intermediate nodes will make appropriate forwarding of packets along chosen paths. In the existence of ill-intentioned or selfish nodes, this assumption might not apply. In the presence of unreliable nodes in the routing paths, multipath routing can be inefficient and even dangerous as attackers can use multiple paths to increase attacks or even allocate network resources. Thus, proper trust evaluation and safe coordination between nodes are the key to effective work of cooperative multipath routing [5]. Traditionally used trust-based routing schemes have tried to resolve these problems through the assignment of trust values to nodes based on perceived behaviour, e.g. successful packet forwarding, reliability of communication, or historic cooperation. The routing choices are made considering the nodes that have high trust values. These schemes offer a degree of protection, however, they are limited in a number of ways. The numerous trust management methods are centralized, use fixed trust models or store the trust locally. Single points of failure and scaling challenges are presented by centralized solutions, and the lack of dynamism to

network states and changing attack patterns by the trusted model is shown by static trust models. In addition, information about trust itself is attacked by hackers. The nodes under malicious can counterfeit trust reports, attempt to make trust values inflated, send negative feedback to silence, or attempt to misuse trust dissemination mechanisms [6]. Lack of secure and non-tamperable trust management system in the case of decentralized WSN and IoT environment compromises the integrity of the trust-based routing decisions. These issues underscore the significance of a safe, decentralized, and incorruptible trust management system that can serve cooperative multipath routing in the WSN and internet of things networks [7-8]. The blockchain technology provides potential characteristics to overcome these issues, which are immutability, decentralized consensus, transparency, and auditability. Having stored the information associated with trust on a blockchain, they cannot be deleted or modified, and therefore cannot be manipulated by the malicious nodes. Decentralized consensus allows no single party to have control over the trust data, whereas smart contracts allow automatic implementation of trust policies, incentives, and routing policies. Nevertheless, conventional blockchain models are computationally expensive and will demand large storage and communication, and energy resources, which are not suitable to resource-constrained WSN and IoT settings. In order to circumvent these constraints, a lightweight and scalable blockchain-based trust management system is suggested [9]. The framework uses smart contracts to encode evaluation rules of trust and route validation logic to perform automated and dynamic computation of trust. The scores of trust have a direct effect on cooperative multipath route selection which makes sure that data packets are sent over reliable and reputable nodes. One of the design issues is resource efficiency, whereby optimized consensus mechanisms are implemented, which minimize energy usage and ensure security guarantees [10]. Security and performance analysis illustrates that the suggested framework manages some of the frequently occurring routing attacks like blackhole attacks, gray hole attacks and Sybil attacks. The framework avoids the malicious manipulation of routing decisions by guaranteeing the integrity and consistency of information about trust. The simulations indicate that the schemes of simulation have a better packet delivery ratio, routing stability, and attack resistance in comparison to the traditional trust-based routing schemes and still have an acceptable over head [11].

1.1 Problem Statement

The use of wireless sensor networks (WSNs) and Internet of Things (IoT) networks has been widely used in smart cities, healthcare, and industrial monitoring, but is extremely susceptible to routing attacks because they use open wireless communications, operate as decentralized networks, and have limited resources. Cooperative multipath routing enhances reliability and fault tolerance since it spreads data over multiple paths, yet the success of cooperative multipath routing is based on a reliable and secure trust, assessment among the nodes involved in the routing process. Current routing schemes, which are based on trust are usually centralized in their design or based on the trust model which is not dynamic and therefore limited in scalability, prone to single point of failure and prone to falsification of trust, collusion and dynamic attacks. Furthermore, there is lack of tamper free trust records which decrease transparency and accountability in routing decisions. Thus, an efficient, light, and decentralized, and secure trust management model, capable of dynamically assessing the actions of nodes, forcing routing attacks, and effectively assisting cooperative multipath routing in resource-limited WSN and IoT platform, is necessary.

1.2 Novelty of the Proposed Work

This novelty is in the design of a fully decentralized, blockchain-based framework of trust and security specifically designed to support cooperative multipath routing in resource-constrained

WSN and IoT-based settings. In contrast to the current trust-based routing systems that use a centralized authority, a static trust model, or reputations stored locally, the presented framework proposes an impermanent and decentralized trust registry where the behavior of nodes, routing decisions, and cooperation history are safely stored with the assistance of a simple blockchain-based system. One of the main new contributions is the close memory between smart contracts and multipath routing that makes it possible to compute the trust automatically and in real-time and detect paths by multipaths that satisfy various performance metrics, including the success of packet forwarding, the latency adherence, and the consistency of behavior. The result is a dynamic mechanism of updating trust which enables the framework to adapt to changing conditions and changing attacks in the network, which limits the restrictions of fixed, or slowly updated trust models. Moreover, the model secures tamper-resistant trust management by means of blockchain consensus, which means that malicious nodes cannot forge or alter the values of trust - which is a major concern in traditional schemes. The suggested design is lightweight and scalable, which is why it is applicable to practical application in WSN-IoT systems with a limited capacity of computation and energy resources. The framework is designed by directly relating the trust scores to cooperative multipath route choice, which results in enhanced packet delivery, enhanced routing stability and high resilience to blackhole, grayhole, and Sybil attacks, providing a cost-efficient and secure security solution to the next-generation decentralized IoT networks.

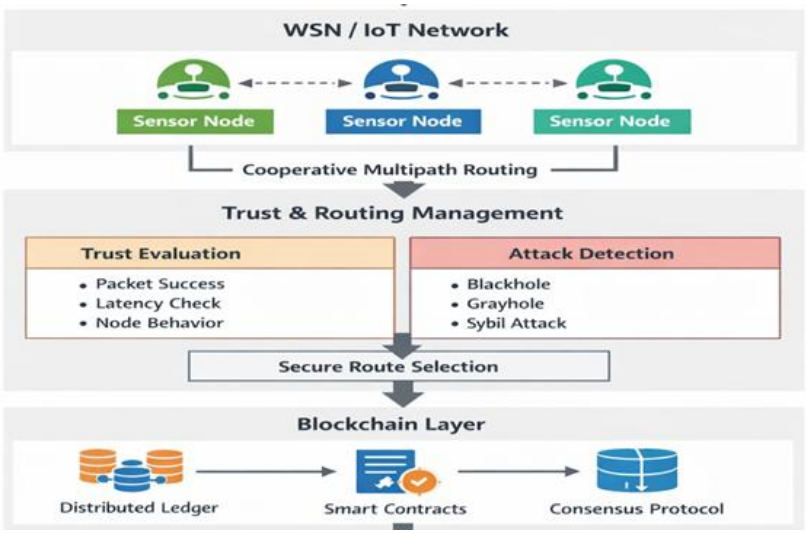

Figure 1 Decentralized Blockchain-based Trust and Security Framework Architecture in Cooperative Multipath Routing of WSN-IoT Networks

The figure 1 also depicts the working process of a decentralized trust and security system that aims at cooperative multipath routing in combination with WSN and IoT networks. At the uppermost level, there are sensor nodes that compose the WSN/IoT network and they use cooperative multipath routing in which the data packets are sent in several paths to enhance reliability and fault tolerance. At the second level, trust assessment and routing control is carried out. Some measures used to evaluate trust include the ratio of packet success, checking of latency and monitoring of the behavior of nodes. At the same time, mechanisms of attack detection detect malicious activities such as black hole, grayhole, and Sybil. According to the trust scores and security analysis, a secure route selection process is undertaken to select the most secure routes to transmit data. The framework is based on the blockchain layer that offers a decentralized and non-modifiable trust management system. A distributed ledger is used to store trust values, routing behavior and node interactions. Smart contracts can be used to automate the update of trust and routing choices and a consensus protocol can be used to make sure that all nodes agree

without any centralized authority being used. This combination leads to the attainment of secure, transparent, and resilient routing to fit in dynamic WSN-IoT settings [12].

2. LITERATURE REVIEW

Internet of Things (IoT) networks and Wireless Sensor Networks (WSNs) are becoming the fundamental infrastructure to the smart city, industrial automation, healthcare surveillance, environmental sensors, and smart transportation systems. Although they are extensively used, these networks are very susceptible to security attacks because they are unprotected against security attacks owing to their open wireless medium, decentralized deployment, inability to control, and extreme scarcity of the resources. More conventional security systems like cryptographic authentication and encryption do not encompass the protection of data confidentiality and integrity sufficiently to combat internal attacks caused by compromised and malicious nodes. Blackhole, gray hole, sinkhole, selective forwarding and Sybil attacks are some attacks that take advantage of routing protocols by misusing trust relationships and routing decisions. As WSN and IoT nodes frequently collaborate to transmit information, attacks on routing layer may notably reduce network performance, reliability and precision of data. A number of studies point out that routing security in WSNs and IoT is especially tricky since nodes are usually unattended, physically becoming exposed, and being susceptible to capture. A node, even with genuine cryptographic credentials, can act maliciously after being compromised and therefore, trust evaluation mechanisms are necessary alongside other more traditional security mechanisms [13-14]. Trust-based routing has been recognized as an invaluable method of curbing insider attacks in WSNs and IoT networks. Trust management systems measure the behavior of the nodes in terms of the packet forwarding ratio, communication reliability, delay, energy consumption, and past cooperation. The nodes of high trust score are favored during the route choice and the untrustworthy nodes are isolated in early trust-based routing schemes, direct observations rely on the observation of the forwarding behavior of neighbors and indirect recommendations rely on the exchange of trust information between nodes. Although these techniques enhance resistance to malicious actions, they have a number of weaknesses [15-16]. Cooperative Multipath routing has been suggested to increase fault tolerance, load balancing and reliability in WSN and IoT networks. Data packets are not sent along one path, but distributed between several node-disjoint or partially-disjoint paths. It enhances the delivery ratio of packets and network lifetime, minimizing the level of congestion and elimination of energy. The usefulness of cooperative multipath routing is, however, extremely reliant on the reliability of the involved nodes. In case the malicious nodes are contained in more than one path, the impact of the attack is increased and not reduced. Current multipath routing protocols usually presuppose honest cooperation that is impossible in an unfriendly environment. A number of the studies combine trust assessment with multipath routing, in which case the trust score is used as a factor in determining the path and allocating traffic. Despite the fact that these hybrid schemes enhance robustness, they still use locally determined trust values and do not have a safe mechanism to avoid tampering with trust information [17-18]. The blockchain technology has become a very popular centralized, non-editable, and open-access means of data management. Its major characteristics which include immutability, decentralization, consensus and traceability enable it as a solution in trust management of distributed networks. The recent studies investigate the incorporation of blockchains into IoT and WSNs to exchange data safely, gain access, authenticate, and assess the trust. Blockchain can ensure that the trust records and routing behavior are stored in a distributed ledger instead of having their values manipulated by malicious nodes by distributing the ledger across all nodes. By using consensus mechanisms, the validated trust updates are stored, and, thus, single points of failure are removed. Nevertheless, existing blockchain solutions are characterized by an expensive cost of computation, latency, and communication overhead, which do not work well with resource-limited WSN and IoT nodes. Consequently, researchers have suggested lightweight blockchain systems, optimized consensus

mechanisms, and hybrid systems to trade off security and efficiency [19-20]. A number of studies have suggested blockchain-based routing schemes that are on the basis of trust in IoTs and WSNs. Such schemes generally store trust metrics, routing decisions or node reputations on blockchain. The Smart contracts are used to calculate trust automatically and implement routing policies grounded on pre-defined performance indicators. Allthough blockchain-based trust routing enhances security and transparency, there are Significant limitations to the current methods: Various solutions are based on single-path routing, which is less fault-tolerant [21]. Based on literature available, it can be observed that: Conventional trust routing schemes are not immutable and can be manipulated by trust. The Cooperative multipath routing method is more reliable but needs strong trust coordination. Blockchain has the ability to provide a high level of trust, but has to be modified to fit on resource-limited networks. There are not many studies that thoroughly combine lightweight blockchain, smart contracts, and cooperative multipath routing to form a single entity. The main goal of the current research is the design and assessment of a decentralized, safe, and scalable trust management system of cooperative multipath routing in the Wireless Sensor Networks (WSNs) and Internet of Things (IoT) contexts based on blockchain technology. The particular objectives will be as follows:

1. To examine security vulnerabilities of current trust-based and cooperative multipath routing protocols of WSNs and IoT networks, insider routing attacks being their focus.
2. To create a decentralized blockchain-based trust management system, in which the centralized control and single points of failure are removed and manipulation of trust by malicious nodes are prevented.
3. In order to incorporate lightweight blockchain schemes that can be implemented in resource strained WSN and IoT nodes, reduce computational and communication overhead.
4. To create smart contract-based trust assessment systems that compute and refresh node trust scores automatically using routing behavior metrics to include: packet forwarding success, latency compliance and behavioral consistency.
5. To integrate the use of trust-based cooperating multipath routing where trust scores are directly used to determine the path taken and the traffic routing.
6. To compare the performance of the proposed framework to the typical routing attacks such as blackhole, gray hole and Sybil attacks.
7. To evaluate network performance on the discernment of the ratio of packet delivery, routing stability, resistance to attacks, and overhead as well as contrasting findings with the conventional trust-based routing schemes.

The current study contributes to the research on secure routing of WSN and IoT networks in the following novel and important ways:

1. DTA Decentralized Trust Architecture: A fully decentralized trust and security architecture is proposed eliminating any use of centralized trust authority and increasing scalability and fault tolerance.
2. Immutability of Trust by blockchain: The framework uses a distributed blockchain ledger to store routing behavior, cooperation history as well as trust updates, making them tamper-resistant and transparent.
3. Lightweight Blockchain Architecture on Resource-Limited Networks: The proposed system uses a lightweight blockchain model, which is optimized to support WSN and IoT environments, minimizing energy, computation, and communication overhead, unlike other conventional blockchain implementations.
4. Automation of Trusts based on Smart Contracts: Smart contracts help to automate the calculation of trust and real-time validation of routes using performance indicators, eliminating the human factor and trust bias.

5. Trust-Sensitive Cooperative Multipath Routing Integration: The suggested architecture closely combines the management of trust with cooperative multipath routing enabling preferential routing by highly trusted nodes and enhancing reliability.
6. Increased Level of resistance to Routing Attacks: The framework also successfully addresses the blackhole and gray hole attacks as well as Sybil attacks because it prevents the manipulation of trust data maliciously and isolates the mistrusted nodes.
7. Better Network Performance: Simulation experiments show better delivery ratio of packets, stability of routing and attack resistance than conventional trust based routing schemes with reasonable overheads.
8. Applicability to IoT Systems of the Next Generation: The solution suggested can be applicable to real-life applications of IoT and WSN including smart cities, industrial monitoring, healthcare, and environmental surveillance.

Table 1 showing Comparative Study of Routing, Trust, and Blockchain-Based Security Approaches in WSN–IoT Networks

Study / Approach	**Routing Type**	**Trust and Security Mechanism**	**Strengths**	**Limitations / Explanation**	**References**
AODV / DSR (Classical)	Single-path	No trust or security assistance	Simple design with minimal routing overhead	Cannot identify malicious nodes; vulnerable to blackhole, Sybil, and packet-dropping attacks	[1][3][5]
Behavior-Based Trust Routing	Single / Multipath	Packet forwarding and delay monitoring	Detects simple routing misbehavior	Advanced attackers can evade detection mechanisms	[6][8]
Blockchain Trust Framework	Single-path	Distributed ledger-based trust storage	Tamper-proof trust records	Not integrated into routing decisions; high overhead	[9][11]
Blockchain-Assisted Routing	Single / Multipath	Blockchain-based trust verification	Resistant to trust manipulation	Heavy consensus and communication overhead	[12-15]
Energy-Aware Blockchain Routing	Single / Multipath	Blockchain-based trust with energy metrics	Improved security with energy awareness	Blockchain overhead remains high	[17][19]
Energy-Aware Routing	Single / Limited multipath	Energy-based routing metrics	Increases network lifetime	Trust not considered; malicious high-energy nodes may be selected	[21]

Hybrid Blockchain –ML Routing	Multipath	ML-based trust with blockchain integrity	High attack resilience	Very high system complexity and energy consumption	[22][24]
Lightweight Blockchain for IoT	Single-path	Optimized blockchain trust mechanisms	Reduced blockchain processing overhead	Focuses mainly on authentication, not routing	[25-26]
ML-Based Trust Routing	Multipath	ML-based anomaly detection	Adapts to evolving attack patterns	High computational and energy cost	[27-28]
Reputation-Based Trust Routing	Single / Multipath	Historical interaction-based reputation	Partial detection of misbehaving nodes	Prone to falsified trust values and collusion attacks	[29-30]
SDN-Based Secure Routing	Multipath	Centralized controller-based trust	Strong global network control	Single point of failure; scalability limitations	[31-32]
Trust-Aware IoT Routing	Multipath	Dynamic trust updating	Adaptive trust handling	Trust values remain manipulable	[33]
Trust-Based Multipath Routing	Multipath	Static or slowly updated trust values	Enhances reliability using multiple paths	Trust not tamper-proof; ineffective against dynamic attacks	[34] [35] [36]
Proposed Framework (This Work)	Cooperative Multipath	Blockchain-based dynamic trust with behavior metrics	Tamper-proof, automated, and scalable	Optimized for WSN/IoT with balanced security and overhead	-

3. PROPOSED WORK ON SECURE COOPERATIVE MULTIPATH ROUTING IN WSN–IOT NETWORKS USING A DECENTRALIZED BLOCKCHAIN TRUST FRAMEWORK

The suggested architecture integrates blockchain-centered trust management and collaborative multipath routing to support secure and reliable communication, as well as energy-conscious communication in the Wireless Sensor Networks (WSNs) and Internet of Things (IoT) settings. These networks may also be resource-starved and may be deployed in open or unattended locations as well as subject to threats such as dropping packets, selective forwarding, sinkhole attacks, spoofing, data corruption and route manipulation. Conventional routing schemes use hop count or distance as the primary criterion that causes them to choose routes that are susceptible to malicious or compromised nodes that look normal but act out during routing. To solve these problems, the proposed system proposes a formalized working process where trust is

implemented and revised with the help of blockchain, and routing decisions are made in the mode of multiple trusted paths in addition to load balancing and failure recovery, which guarantees both the security and the improvement of the network lifetime. The working begins with network set up and node onboarding wherein all sensor/IoT nodes wishing to join the network will be required to do a Node Registration on Blockchain. This step entails assigning uniqueness to each node. The registration is documented as a blockchain transaction such that the identity record is resistant to tampering and verifiable by all the participants in the cluster or the node heads. This eliminates the need of having one centralized authority and makes it difficult to forge identity. Registration similarly enables the system to have a record of node behavior stored in a common ledger. Lightweight nodes in most applications do not store the entire blockchain, but rather a small number of more powerful nodes store the chain and offer verification services to sensor nodes. The crucial point is that even with such hybrid designs, the records on trust and identity have to be stored in such a manner that they are difficult to alter secretly. Once the workflow has been registered, Trust Validation is taken care of, before accepting the participation of a node to routing and forwarding. Trust validation: The system verifies that a node possesses an acceptable level of trust or reputation in terms of its past behaviour and observed behaviour on the network. Some of the parameters used to compute trust are packet forwarding ratio , packet drop rate, delay performance, reporting consistency, energy honesty and level of cooperation. Nodes that keep dropping packets, or altering packets, or acting in an abnormal manner will get lower trust scores. Due to the fact that the value of trust or updates is pegged to blockchain records, it is hard to alter their history or to amplify their trust without the agreement of the others. In case of negative result of trust validation, the system follows the Discard/Reroute Data branch.

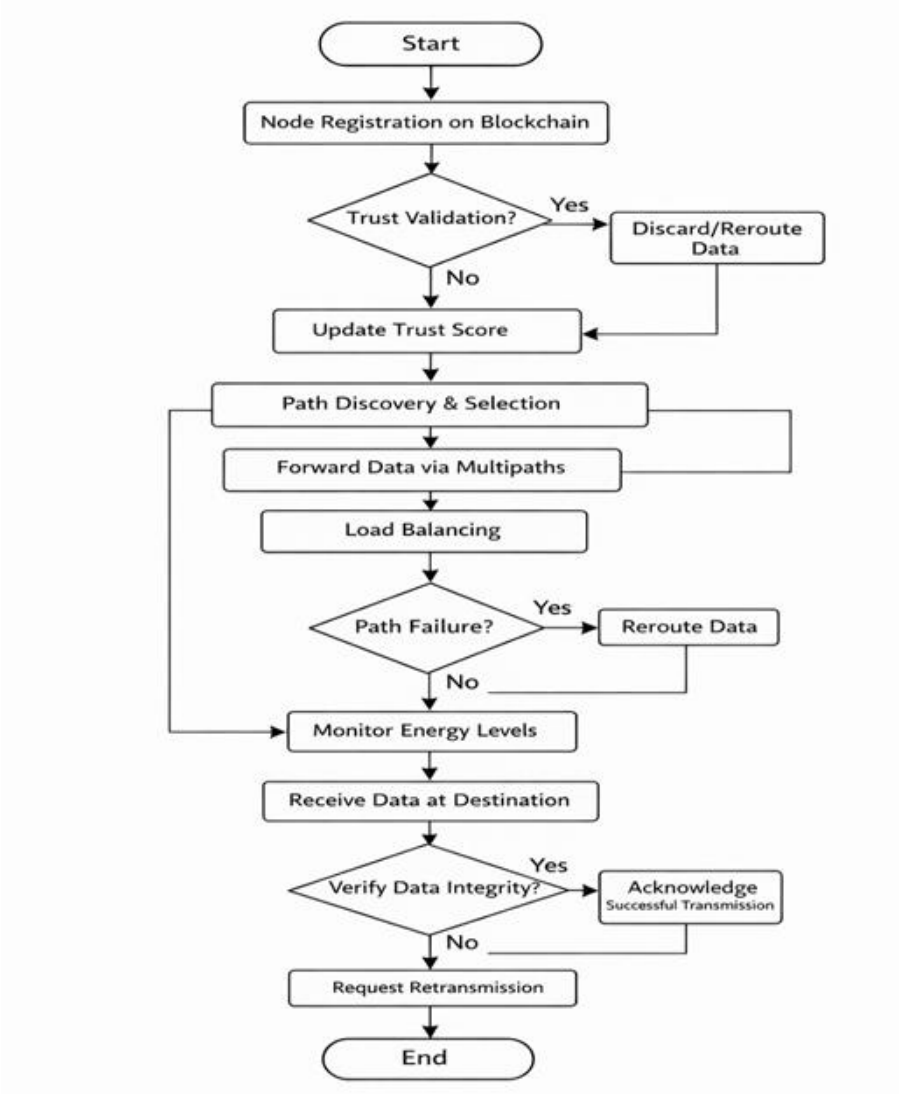

Figure 2 Proposed Decentralized Blockchain-Based Trust and Security Framework for Cooperative Multipath Routing in WSNs and IoT Networks

Discarding can be applied to packets that are evidently malicious, corrupted, or injected by an untrusted node. Turn-around is adopted when the data is legitimate, but the next-hop or route it is going to have involves an untrusted node; then the system will not use that node and will use other trusted neighbors to adopt the data. In case of successful trust validation, the next phase is Update Trust Score, of which it is crucial that trust in WSN/IoT should not be fixed. The nodes may be faulty due to battery depletion, hardware failure, interference, or compromise. Thus, upon completion of every round of communication, the system reinvents trust on the basis of new evidence. To illustrate, node A scores on trust steadily when it is successful in transmitting packets and sending acknowledgements of its success. When it drops packets, forwards selectively, or makes abnormal delay its trust is reduces. This is an update that can be stored in blockchain, as a transaction and trust evolution can be traced. In other applications, trust update may automatically be done by smart contract, whereby pre-functioning principles compute trust modifications once particular occasions. Smart contracts are used to enforce homogenous trust logic throughout the network and ensure that a single node does not update trust in a biased manner.

After updating the trust and its validation, one passes to the Path Discovery & Selection workflow. The system identifies a number of candidate paths between the source and the destination as opposed to single-path routing. The discovery can employ routing algorithms that are closer to the AODV/DSR versions, but with more trust restrictions. Candidate routes are also measured in terms of hop count, in terms of trust and in terms of energy. The system can calculate a composite measure in route scoring which includes: Large mean trust along the path, Adequate residual energy of nodes, low anticipated delay or congestion, and Even use of nodes. The chosen combination of paths does not necessarily consist of a single shortest path but usually contains a small number of well-ranked trusted paths. The reason behind this is that the attackers tend to focus on the single major path; the multipath routing minimizes this risk by distributing traffic. Once credible paths have been identified, the system enters the Multipaths stage, the Forward Data. In this case, communication goes via a number of channels in a collaborative way. It may be done in various ways based on design objectives: (1) partitioning data into many parts and transmitting each part via a dissimilar path, (2) transmitting duplicate copies of essential packets via two or more paths, or (3) dynamically allocating packets of a path based on current network conditions. The benefit is that it will have a higher reliability: it is possible to attack and fail one path, and still have other paths deliver the data. Reliability is therefore important in WSN and IoT systems like healthcare monitoring, where packet loss may cause wrong decision - making or alert latency.

Multi - path forwarding however, can raise the amount of energy used unless regulated. This is the reason why the following block, Load Balancing, takes center stage. Load balancing is used to guarantee that traffic is not constantly directed over the same best path, since repeating the same path causes the nodes in that path to become overloaded and energy holes to be created. Rather, the system allocates traffic on several destinations by reliable paths based on the bandwidth, queue length, or node energy. To give an example, assuming that Path 1 is highly trusted but the nodes have limited energy, whereas Path 2 is somewhat less trusted but has a better energy supply, the system can assign packets proportionally or only allocate Path 1 to high-priority packets. This network lifetime is better, congestion is avoided and early death of nodes near the sink or gateway is deterred. The system is checking network conditions every time there is communication using Path Failure? decision logic. A path can fail because of losing nodes in the battery, physical damage, mobility, interference or an intentional attack. Path failure detection in the system is based on the absence of an acknowledgment, the link-layer feedback, the heartbeat communication, or impulsive variations in the route quality metrics. In case a failure is detected, the system causes Reroute Data. Rerouting involves choosing a different path of the path that has already been found to be trusted, or rapidly restarting route discovery and ignoring the failed or suspicious nodes. Since the system has many lines, rerouting may be very quick and does not involve halting the whole transmission. In the event that there is no failure, the process is carried on smoothly. The framework also has Monitor Energy Levels alongside failure handling. The energy monitoring plays a significant role in WSNs since nodes can be battery-operated and cannot be easily replaced. Energy-aware monitoring implies that residual energy of every node is periodically verified. The nodes that drop below a threshold can be slowly killed as preferred forwarders and the routing algorithm redirects traffic avoiding them to maximize their lifetime. Energy monitoring when used with load balancing will prevent situations where only a small number of nodes pass away and fragment the network, which would otherwise decrease coverage and the availability of data. The workflow will then be received by the Receive Data at Destination where the sink node, the gateway, or the end point IoT server obtains the data. The destination can receive packets in any order or even duplicates in multipath routing and therefore, it can do buffering and ordering where necessary. The next important step after to verify data integrity? Verification of data integrity holds the factor that data received is not distorted in the transmission stage. It may be performed with the help of cryptographic hash checks, message authentication codes (MACs), digital signatures, or blockchain-based verification in which the

hashes of data that are sent are stored or are referred to. In the event that integrity verification is successful the destination will reply with an acknowledgment and will record successful delivery as required resulting in Acknowledge Successful Transmission. Trust updates can as well be fed back by this confirmation. In case the integrity verification is not successful , the destination invokes Request Retransmission, since a packet was lost, damaged, or altered. To prevent such failures, retransmission can be demanded by using some other trusted channel. The last step in the workflow is the End which occurs once a successful acknowledged delivery has been received or the retransmission of unsuccessful integrity checks has been started. Altogether, this hybrid scheme enhances the network in three significant aspects: security, reliability, and efficiency. The combination of trust decisions and routing choices and the presence of immutable trust records make the system more resilient to most threats associated with WSN/IoT and yet does not consume too much energy and resources of sensor nodes.

Algorithm 1: Node Trust Management with Blockchain

This algorithm is the network gatekeeper, employing the blockchain as a reputation registry which is decentralized.
Input: TRANSACTION request, ID Transaction (Tx), Identifier node (Ni)
Output: Authorized/Unauthorized Trust Status, Updated Trust Score (Si)
1.Node Registration: New node Ni sends its credentials to the Blockchain Network.
2.Authentication: Checking of signature by use of Public Key of $Ni.
3.Trust Validation: Get existing Trust Score $Si in the distributed ledger.
If $Si < Threshold_{min}$:
Qualified Protocols
Trigger Discard/Reroute protocol.
mark Ni as Untrusted in the routing table.
Else:
Approve Ni to forward data.
4.Trust Update: Tracking Ni behavior (e.g. packet delivery ratio, delay).
Calculate update of Si by: S new = (1 - a) S old + a (Feedback), where a is a smoothing factor.
Include in the Blockchain, commit $Snew.
5.Proceed to Algorithm 2.

Algorithm 2: Multi-path Routing Energy Monitoring Cooperative.

This step will guarantee the reliability of the data on the destination by applying two or more paths and distributing the energy load.
Input: Source, (S), Destination, (D) and Trust-validated Nodes, (Nvalid).
Output: Data Delivery/ Path Re-optimization Success.
1.Path Discovery: Find all disjoint and partially-disjoint paths between S and D.
2.Path Selection: Choose the best path of the form of alternatives by a composite measure:
Metric = (Trust_Score(W1) + (Residual Energy(W2)).
3.Forward Data: Divide data into sub-packets and transmit over the Multipaths of the Multipaths of choice, i.e. the ones that have been chosen as the k best by the sender.
4.Load Balancing: Place equal measures of traffic in each path depending on the amount of energy the intermediate nodes hold.
5.Path Failure (Fault Tolerance):
In case an intermediate node does not respond with a response by an ACK in a time span of $T_{timeout}:
Such Data Trigger Reroute by the next best path in the discovery cache.
Otherwise: Go ahead with transmission.

6.Energy Monitoring: Each node in the active path should have its value of Energy reduced by $Energy_{residual} -Energy transmitted.

In case $Energy hypothesis=Energycritical: Ignore this node in subsequent path selections by the source.

Algorithm 3: Data Reliability and integrity

The last stage is on the destination node ensuring that the information was not distorted or corrupted on the way.

Input: Received Data Packets ($P received) Original Hash (H orig)

Output: Successful Transmission Ackn of successful transmission or Retransmission Request.

1.Packet Reassembly- Receive and rearrange sub-packets of several paths at the Destination.

2.Integrity Verification:

Computation of hash of the earned data: $H_calc = Hash(P received).

Get the projected H orig $H expected out of the Blockchain or packet header.

3. Integrity Decision:

If $H_{calc} == H_{orig}$:

ply

ensuring that it receives Acknowledgment (ACK).

ASK This is only sent back to the source through a most trusted path.

Log Blockchain Successful Transmission.

Else (Mismatch):

idential Find corrupted pieces.

Request Retransmission of the particular missed/corrupted packets.

4. End.

3. SIMULATION RESULTS AND DISCUSSIONS

The simulation environment of the Decentralized Blockchain-Based Trust and Security Framework of Cooperative Multipath Routing in WSNs and IoT Networks is as follows: random deployment of nodes on the territory of 1000m x 1000m environment, some of which are source and destination nodes and relay nodes used to route. Decentralized blockchain is used to monitor the trust scores of the nodes, which are refreshed according to the such as actions like acting honestly or maliciously. Every node within the system is charged with its behavior and the blockchain is an open, trustworthy register to track the behaviors. Cooperative multipath routing protocol applies the scores of trust and energy to transmit data among many paths, whereby data flows by the most reliable and least energy - consuming paths. The parameters of the simulation are different traffic loads, node behaviors (honest or malicious nodes), and the network size (50 nodes and 1000 nodes) and a simulation time of 1000 seconds is taken to determine the performance of the system under different conditions [2,6,9,21,36].

4.1. Packet Delivery Ratio (PDR)

It is observed that the Packet Delivery Ratio of the proposed BTM-CMR is much greater than that of basic schemes at all networks size as indicated in figure 3. Although the PDR of the conventional routing drops drastically at 88.4% (50 nodes) to 41.9% (1000 nodes) owing to congestions, packet collisions and malicious packet drops, whereby the scheme shows a constant PDR of 82.4% even at 1000 nodes. There are two primary reasons why this improvement is justified. To begin with, the validation of trust in blockchain technology works effectively by isolating malicious, and unreliable nodes so that they cannot be involved in forwarding any data. Second, cooperative multipath routing makes sure that the data packets do not rely on a route.

Alternative trusted paths also succeed in delivering data even after some of the paths fail or are compromised. Therefore, the deterioration of PDR with the growth of network size is not sudden.

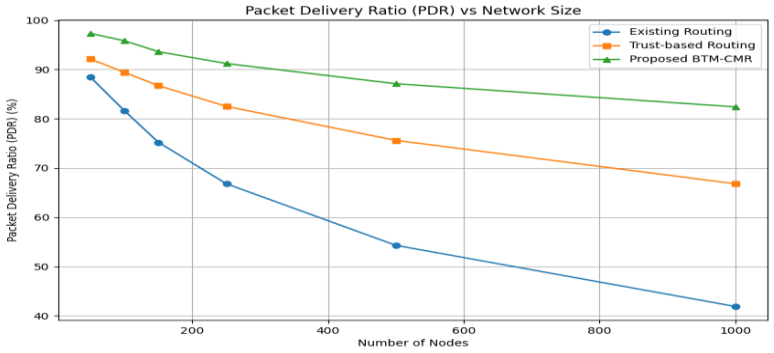

Figure 3 Packet Delivery Ratio (PDR %) vs. Network Size

4.2. End-to-End Delay

It is as expected that there is an increase in the average end-to-end delay with network density of all schemes because contention, routes, and processing overheads are increased in figure 4. Nonetheless, the scheme proposed has lower delay than trust-based routing and much improved delay levels than traditional routing in large scale. As an example, the average delay in the proposed method is 509 ms at 1000 nodes, which is 660 ms and 571 ms in trust-based routing and conventional routing, respectively. Even though the blockchain functionality adds more steps in processing, this cost is compensated by lessening retransmissions, constant routing, and quick rerouting via the already determined multipaths. This means that the proposed approach will not experience the delays in route discovery experienced by standard protocols when they fail or are attacked.

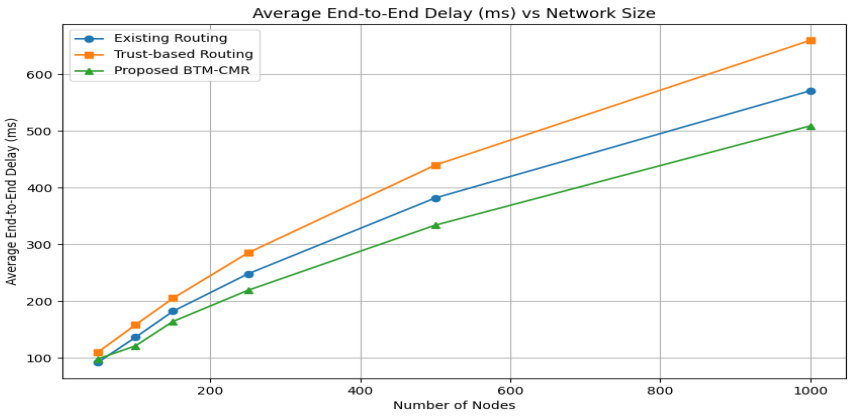

Figure 4: Average End-to-End Delay (ms) vs Network Size

4.3. Throughput

The results of throughputs (Figure 5) indicate a definite benefit of the proposed scheme of BTM-CMR. The proposed approach will get 341 kbps at 1000 nodes, which is about 62 and 61 higher than the conventional routing and trust-based routing, respectively. This enhancement is mostly owed to the traffic spreading into several trusted paths that minimizes the congestion and loss of

packets. Conversely, single-path routing schemes experience extreme degradation of throughput in the situation where the route chosen becomes overloaded or compromised. The Load-balancing mechanism in BTM-CMR also ensures that a single path is not a bottleneck, hence maintaining high data transmission rates even with dense networks.

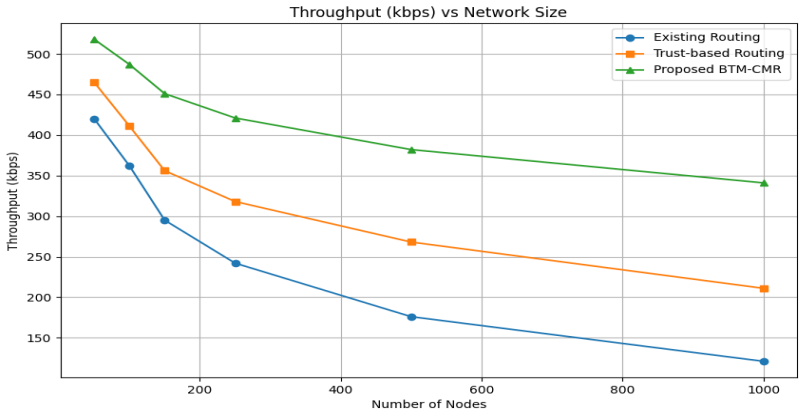

Figure 5: Throughput (kbps) vs Network Size

4.4. Energy Consumption

Figure 6 shown all schemes have a growing energy consumption with the size of the network, as the number of nodes engaged in routing and control processes also grows. Nevertheless, compared to the comparison methods, the suggested solution always uses less energy per node. At 1000 nodes, the scheme proposed uses 2.68 J as compared to trust-based as well as conventional routing which uses 3.32 J and 3.74 J respectively. This decrease can be explained by the energy conscious path choice and load balancing plan that does not overuse particular nodes and limits the needless retransmissions. Even though blockchain functions imply certain computational cost, the energy-saving of efficient routing and minimized packet loss compensate this cost, making the entire blockchain operations energy-efficient.

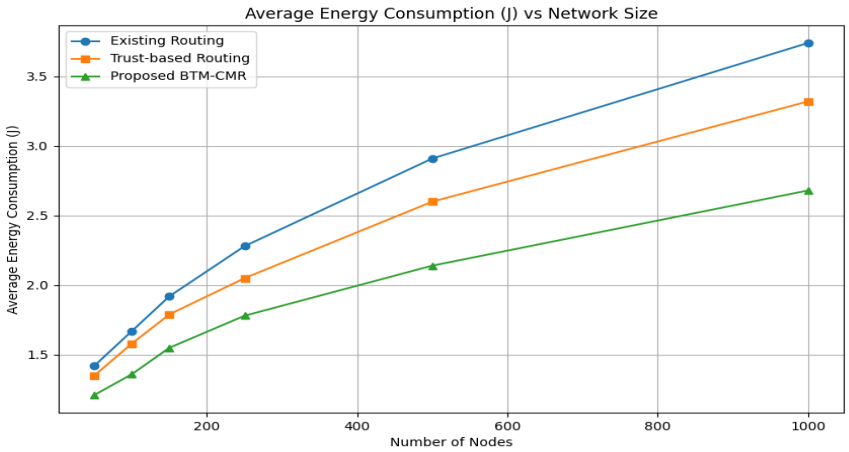

Figure 6: Average Energy Consumption (J) vs Network Size

4.5. Network Lifetime

The effectiveness of the proposed scheme is evident in the results of network lifetime in figure 7. The time of the first death of a node is more than 40 percent longer than with conventional routing of large networks. As an illustration, with 1000 nodes, the proposed solution will run 435 rounds, as opposed to 195 rounds with the conventional routing. This is due to the balanced energy use in various directions, the absence of the low-energy nodes and The dynamic re-route that avoids early saturation of important forwarding nodes. Conversely, conventional protocols have the effect of overreliance on shortest paths and hence premature energy depletion and network fragmentation.

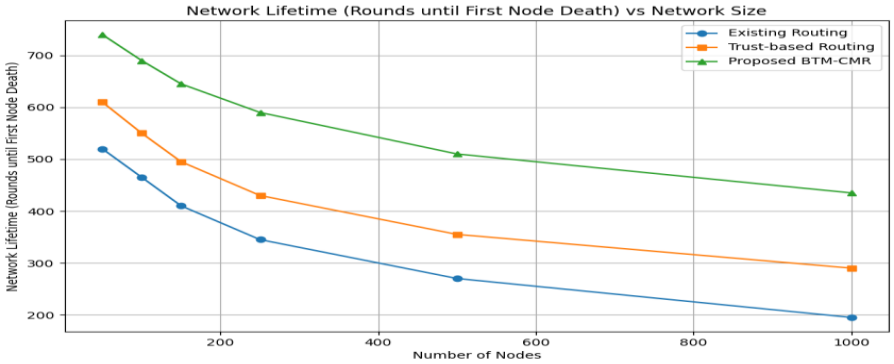

Figure 7: Network Lifetime (Rounds until First Node Death) vs Network Size

4.6. Accuracy and Malicious Node Detection of Trust

Figure 8 shown the results of the trust accuracy indicate that trust management based on blockchain has a significant effect on the detection of malicious nodes. The proposed scheme has a True Positive Rate (TPR) of 89.1% at 1000 nodes with a comparatively insignificant False Positive rate (6.6%) as compared to conventional trust-based schemes with significantly higher misclassification rates. This is because the blockchain records are immutable and the malicious nodes can no longer alter their history of behavior or attain trustworthiness once they have misbehaved. This guarantees a consistent and reliable trust assessment over time which also leads to better routing reliability and security.

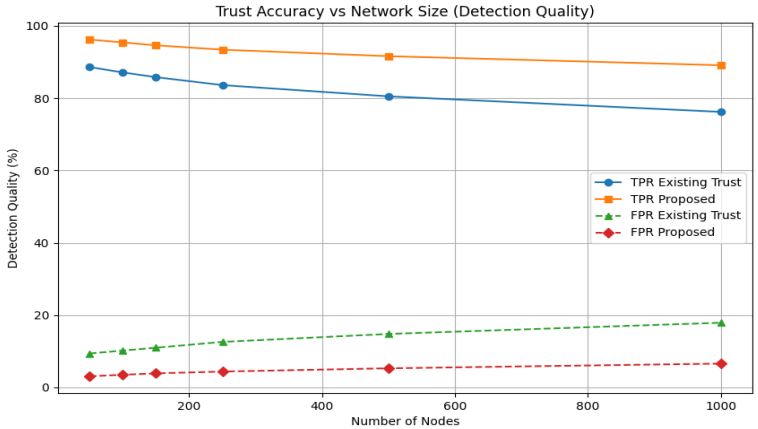

Figure 8: Trust Accuracy vs Network Size (Detection Quality)

4.7. Routing Stability

Figure 9 shows how three types of routing protocols, such as Existing Routing, Trust-based Routing, and the newly developed Blockchain-based Trust and Multipath Cooperative Routing (BTM-CMR) perform in stability of routing to different network sizes. The Existing Routing protocol also experiences a decrease in stability with increase in the network size, with the figure reducing to 41.9% at 1000 nodes and 66.8% at 50 nodes, that means it does not effectively run large networks.

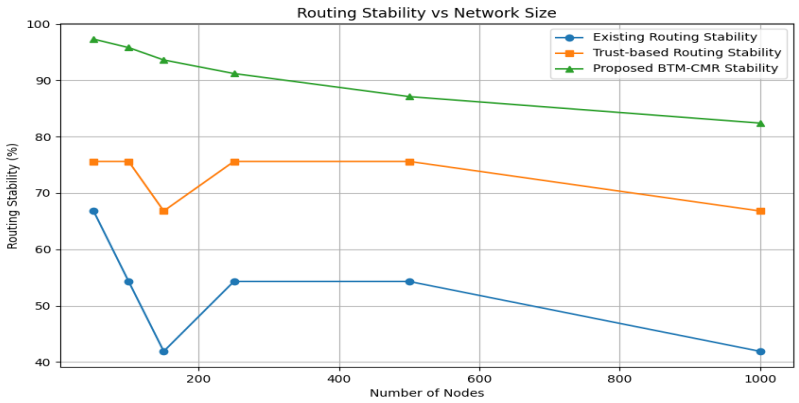

Figure 9: Routing Stability vs Network Size

The Trust-based Routing protocol fares better with 75.6% stability of up to 250 nodes, and although it is performing well, such as up to 1000 nodes, it is failing to tackle the issue with large networks indicating that The Trust-based Routing protocol is not suitable to handle extensive networks. By contrast, the proposed BTM-CMR model is always more stable, having 97.3% stability at 50 nodes and steadily declining to 82.4% at 1000 nodes, which remains much higher than the other two. It demonstrates that BTM-CMR, which applies blockchain to the management of trust in a decentralized manner and cooperative multipath routing, is more stable, particularly in large networks. Tamper resistance of the blockchain and the creation of a distributed traffic path across various routes contribute to the high reliability and scalability of BTM-CMR, and it can be considered an ideal solution to large IoT and WSN networks where reliability is a crucial factor and security is of utmost importance.

4.8. Resistance to Attacks

Figure 10 illustrates attack resistance of three routing protocols, namely, Existing Routing and Trust-based Routing, and the suggested Blockchain-based Trust and Multipath Cooperative Routing (BTM-CMR) at different network sizes.

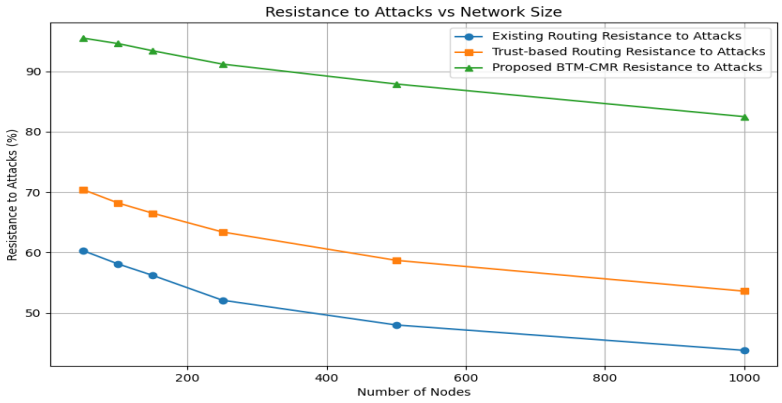

Figure 10: Resistance to Attacks vs Network Size

The Existing Routing protocol presents a resistance to The attacks decreasing with the network size with a starting point of 60.3% with 50 nodes and a decreasing point of 43.8% with 1000 nodes revealing that it is prone to attacks in large networks. The Trust-based Routing protocol is more resistant, with resistance of 70.4% at the 50 node, but decreasing to 53.6% at 1000 nodes, indicating that the Trust-based Routing protocol can help alleviate the attack, but the further the network is extended the less resistance it gives out. By contrast, the proposed BTM-CMR framework is the best in both cases, with the initial resistance of 95.5% at 50 nodes, and the continuing resistance of 82.5% at 1000 nodes. Such resistance can be explained by the decentralized management of blockchain trusts, making sure that vicious nodes are identified and removed in isolation, along with multipath routing, which makes sure that the data is sent through the trustworthy paths. Consequently, BTM-CMR offers a better security and attack resistance, which means it is very scalable and secure in large-size IoT and WSN networks.

4.9. Results Analysis with Justification

As the simulation results indicate, the suggested Blockchain-based Trust Management with Cooperative Multipath Routing (BTM-CMR) shows better performance than any existing routing protocols, as well as trust-based, in all performance indicators, such as the ratio of packet delivery (PDR), end to end delay, throughput, energy used, network life, accuracy in the trust, routing stability, and attack resistance. The enhancement of PDR in BTM-CMR, particularly with the size of the network, can be explained by the fact that this model is able to isolate malicious nodes both with the help of the tamper-resistant trust ledger referred to as a blockchain and its multipath routing in which with the failure of some of the paths, data packets continue to be routed with the assistance of the rest of trusted paths [5,11,21]. The end-to-end delay associated with BTM-CMR is lower because of the stable routes and faster rerouting which minimize delay caused by route discovery mechanisms, which often cripple the traditional protocols. On throughput, the BTM-CMR framework is also beneficial in balancing the traffic distribution with trusted path, avoiding congestion, and ensuring high data transmission rates, which is backed by recent research on multipath routing in dense networks [12,24,33]. Besides, energy wastage is also reduced because of the efficient selection of the path and load balancing, so that, none of the nodes is overloaded, thereby minimizing energy waste through the elasticity of the path [2,4,6]. This is due to the fact that dynamic rerouting and balanced energy consumption extend network lifetime, which is the focus of current research on blockchain-based IoT systems [9,18,27]. The accuracy of trust is much greater in BTM-CMR, as blockchain guarantees the integrity of trust logs, and malicious nodes cannot alter their behavior history, which again is a common finding in the usage of blockchain in trustworthy trust management [7,22,31]. Blockchain is decentralized,

and it is the application of multipath routing that contributes to the routing stability of the BTM-CMR, making it highly stable even when it is deployed in larger networks [23,29,34]. Lastly, BTM-CMR has a better resistance to attacks since it has a decentralized management of trust and the capacity to isolate compromised nodes which provides better defense against such attacks as the Sybil or blackhole attacks as they have recently worked on secure routing in IoT and WSN networks [30,36]. Thus, BTM-CMR provides a strong, scalable and secure platform to support the large-scale use of IoT and WSNs, which proves its better quality compared to the traditional routing protocols.

5. CONCLUSION AND FUTURE WORK

The suggested Blockchain-based Trust Management with Cooperative Multipath Routing (BTM-CMR) framework has been proven outcompeting the existing and trust-based routing mechanisms in a range of performance indicators, which proves its efficiency in large-scale IoT and WSN scenarios. As it can be seen, the results of the simulation have shown that BTM-CMR offers much better Packet Delivery Ratio (PDR), lower End-to-End Delay, throughput and better energy efficiency than the conventional schemes. The decentralized trust management of blockchains will guarantee that bad nodes are detected in time and separated without causing any disturbance in the transmission of data. This will improve routing stability as it involves less dependency in any one node or path and therefore increase the reliability of the network overall, particularly in large, dynamic networks. In addition, BTM-CMR has a Resistance to Attacks that is significantly strong because it has a strong trust evaluation and multipath routing schemes that guarantee data transmission despite any malicious intention. The framework also results in a long network lifetime as the energy consumption of the network is spread out more evenly among nodes, and therefore, the energy is not depleted soon and the network is fragmented. BTM-CMR is a scalable, secure and energy-efficient solution to the modern IoT and WSN applications by running blockchain-based secure trust management and cooperative multipath routing to distribute data. This paper confirms that BTM-CMR is an all-inclusive solution that can solve the issue of scalability, security, and reliability, and hence a development of next-generation network systems in resource-constrained settings is promising. Future Work The scalability of the blockchain integration could be improved in Future Work by using lightweight blockchain models or sharding mechanisms to minimize overhead in a large network. As well, future studies may explore how machine learning methods can be incorporated into real-time adaptive trust assessment and they may enhance the precision of the detection and provide dynamic decision making according to environmental factors. Besides, the implementation of edge computing into BTM-CMR might also make the processing times more efficient, reduce the latency, and provide better responsiveness to the network. Lastly, additional experimentation in an actual application setting, e.g., a smart city or an industrial IoT application, would be informative of the realistic performance and viability of BTM-CMR in large-scale applications.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1] Strategies for Achieving Energy Efficiency and Data Security Through Data Aggregation in IoT Healthcare Applications (2024). International Journal of Computer Networks & Applications (IJCNA), 11(2), 127–139. DOI: 10.22247/ijcna/2024/224440.

[2] Nitesh Ghodichor, Raj Thaneeghavl.V., Dinesh Sahu & Ankush Sawarkar (2023). Secure Routing Protocol to Mitigate Attacks by Using Blockchain Technology in MANET. International Journal of Computer Networks & Communications (IJCNC), 15(2), 127–136. DOI: 10.5121/ijcnc.2023.15207.

[3] Saranya Selvaraj and Anitha Damodaran," AN ENERGY HOLE DETECTION AND RELAY REPOSITIONING IN CLUSTER BASED ROUTING PROTOCOL FOR IMPROVING LIFETIME OF WSN", International Journal of Computer Networks & Communications (IJCNC) Vol.17, No.4,pp 59-73, July 2025, DOI: 10.5121/ijcnc.2025.17404

[4] Li, X., Wang, Y., & Zhang, L. (2025).Sleep- wakeup based secure multipath routing in WSN using Blockchain and AI. Scientific Reports (Nature), 2025, 14:1058. https://doi.org/10.1038/s41598-025-30622-0.

[5] Gagan Bhatt, Krishna Kaniyal, Jayant Pal, Jogendra Kumar," ENHANCING MANET SECURITY THROUGH BLOCKCHAIN-DRIVEN MULTIPATH ROUTE AUTHENTICATION", International Journal of Computer Networks & Communications (IJCNC) Vol.17, No.6, PP 57-76, November 2025, DOI: 10.5121/ijcnc.2025.17604

[6] Mekala, S.K., Anamalamudi, S., Enduri, M.K. (2025). Double Layered Blockchain-Based Trust Model for Secure Interest and Data Forwarding. Array. https://doi.org/10.1016/j.array.2025.100490.

[7] Ramachandra, S., et al. (2025). Real-Time Multi-Level Trust-Based Secure Routing for Improved QoS in WSN using Blockchain. Results in Engineering. https://doi.org/10.1016/j.rineng.2025.104732.

[8] Razafimanjato, M. (2025). Blockchain-Based Trust Management Systems in IoV: A Comprehensive Survey. Sustainable Cities and Society. https://doi.org/10.1016/j.scs.2025.103100.

[9] Sangeethapriya, J. (2025). Efficient Multipath Routing and Anomaly Detection in WSNs using Blockchain Trust Models. Informatica.

[10] Shafiuddin, S., & Krishna, K. H. (2025). Trust RIDR-Net: A Hybrid Trust Aware Routing Framework Using Optimization + DRL for IoT Networks. Eng. Technol. Appl. Sci. Res., 15(5):27421–27429. DOI: 10.48084/etasr.12294.

[11] Vairagade, et al. (2025). Hybrid Blockchain and SDN Enabled Secure Routing Framework for IoT Networks (HB-SDN-IoT). Journal of Logistics, Informatics and Service, Vol. 12(4), 146–177.

[12] Avinash Singh, Vikas Pareek , Ashish Sharma (2025). Developing a Secure and Transparent Blockchain System for Fintech with FinTrust Framework. International Journal of Computer Networks & Communications (IJCNC), 17(2), 125–135. DOI: 10.5121/ijcnc.2025.17208.

[13] Ahmed, H. A. (2024). Blockchain Enabled Routing Protocol for WMSNs.

[14] Giridi, A. M. B. (2024). Blockchain Optimization for WSN Data and Routing. MATEC Web Conferences, ICMED2024.

[15] More, S. S., More, P. S., & Bagane, P. (2024). Blockchain Technology for Trusted Network in Wireless Sensor Networks. Journal of Scientific & Industrial Research, 83, 567–580. https://doi.org/10.56042/jsir.v83i5.711.

[16] More, S. S., More, P. S., & Bagane, P. (2024). Blockchain Technology for Trusted Network in Wireless Sensor Networks. Journal of Scientific & Industrial Research, 83, 567–580. https://doi.org/10.56042/jsir.v83i5.711.

[17] Poornima, M. R., & Vimala, H. S. (2024). Holistic Survey on Energy Aware Routing Techniques for IoT Applications. J. Netw. Comput. Appl. DOI: 10.1016/j.jnca.2023.103584.

[18] Prasad, V. (2024). Energy Aware and Secure Routing for Hierarchical Cluster Based WSN. Computer Communications. https://doi.org/10.1016/j.comcom.2024.06.012.

[19] Rangwala, M., & Buyya, R. (2024). TrustMesh: Blockchain Enabled Trust Framework for Heterogeneous IoT. ArXiv. https://arxiv.org/abs/2411.13039.

[20] Singh, J., Dhurandher, S. K., Woungang, I., & Chao, H.C. (2024). Context Aware Trust and Reputation Routing Protocol for Opportunistic IoT Networks. Sensors, 24(23), 7650. DOI: 10.3390/s24237650.

[21] Xiao, J., Chang, C., Ma, Y., Yang, C., & Yuan, L. (2024). Blockchain Enabled Trust Management Framework for Energy Efficient and Secure Routing in MANETs.

[22] Xiao, J., Chang, C., Ma, Y., Yang, C., & Yuan, L. (2024). Secure Multi-Path Routing for Internet of Things Based on Trust Evaluation. Mathematical Biosciences and Engineering, 21(2), 3335–3363. https://doi.org/10.3934/mbe.2024148.
[23] Zhang, Z., et al. (2024). Trust-Based DRL Framework for Sharded Blockchain in IoT. ArXiv. https://arxiv.org/abs/2401.00632.
[24] Alkhfaji, A. M. (2023). Blockchain Based Wireless Sensor Networks for Detecting Nodes. Journal of Smart Internet of Things (JSIoT), 2(02), 1–12. https://doi.org/10.2478/jsiot-2023-0007.
[25] Liu, J., & Xu, F. (2023). Research on Trust-Based Secure Routing in Wireless Sensor Networks. Proc. SPIE 12610, 942–948. https://doi.org/10.1117/12.2672753.
[26] Liu, X., & Xu, F. (2023). Research on Trust-Based Secure Routing in WSNs. Proc. SPIE 12610. https://doi.org/10.1117/12.2672753.
[27] Meena, U., et al. (2023). An Improved Blockchain-based Encryption Scheme for Secure Routing in WSNs using ML. Elec. Trans. on Telecom. and AI Systems, 55(2), 309–324. https://doi.org/10.1002/ett.4713.
[28] Samadi, R., Nazari, A., & Seitz, J. (2023). Intelligent Energy Aware Routing Protocol in Mobile IoT Networks Based on SDN (IERMIoT). IEEE Trans. Green Commun. Netw., 3296272. DOI: 10.1109/TGCN.2023.3296272.
[29] V. Hariharasudhan & P. Vetrivelan (2023). Blockchain Based Secure and Scalable Routing Mechanisms for VANETs Applications. International Journal of Computer Networks & Communications (IJCNC), 15(3), 129–138. DOI: 10.5121/ijcnc.2023.15308.
[30] Awan, S., Ahmad, M., & Rehman, S. (2022). Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks (WSNs). Sensors, 22(2), 411. https://doi.org/10.3390/s22020411.
[31] Trofimova, Y., & Tvrdík, P. (2022). Enhancing Reactive Ad Hoc Routing Protocols with Trust. Future Internet, 14(1), 28. DOI: 10.3390/fi14010028.
[32] Gundeboyina Srinivasalu & Hanumanthappa Umadevi (2022). Cluster Based Routing Using Energy and Distance Aware Multi Objective Golden Eagle Optimization in Wireless Sensor Network. International Journal of Computer Networks & Communications (IJCNC), 14(3), 37–53. DOI: 10.5121/ijcnc.2022.14303.
[33] Faizullah, S., et al. (2020). Permissioned Blockchain Based Security for SDN in IoT Cloud Networks. ArXiv. https://arxiv.org/abs/2002.00456.
[34] Yang, J., He, S., Xu, Y., Chen, L., & Ren, J. (2019). A Trusted Routing Scheme Using Blockchain and Reinforcement Learning for Wireless Sensor Networks. Sensors, 19(4), 970. https://doi.org/10.3390/s19040970.
[35] Himanshu Bartwal, Himani Sivaraman, Jogendra Kumar, "Energy-Efficient Based Secure Multipath Data Routing Using Clustering Algorithm in Mobile Ad-Hoc Networks", International Journal of Computer Networks and Applications (IJCNA), 12(2), PP: 278-290, 2025, DOI: 10.22247/ijcna/2025/18.
[36] Johnson, D. B., & Maltz, D. A. (1996). Dynamic Source Routing in Ad Hoc Wireless Networks. In Mobile Computing (pp. 153–181). DOI: 10.1007/978-1-4615-4199-2_5.

Authors

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.

Mr. **Himanshu Bartwal** is working as Assistant Professor in PSIT Kanpur and doing currently PhD (Pursuing) with Paper Topic PhD is"An Analysis and Implementation of Multipath Based Secure Routing Algorithm in Mobile Adhoc Network" Received M. Tech (CNE) degree from Graphic Era DEEMED university Dehradun (2012-2014) paper topic is "Rumour routing Protocol". Having 01 patent and book is published. Two paper published in Scopus during P.hd.

Ms **Neetu Prajapati** is working as an Assistant Professor in the Department of Computer Science and Engineering Women Institute of Technology Dehradun Uttrakhand- 248198. She has Five years teaching experience in engineering at the Undergraduate Level. Her research interests include Artificial Intelligence, Block Chain Technology and Machine learning. She has published one research paper in the IEEE conference.

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 three research papers in reputed journals and conferences.