Computers, Materials & Continua
DOI:10.32604/cmc.2022.021305
Article

Tech Science Press

Wireless Sensor Networks Routing Attacks Prevention with Blockchain and Deep Neural Network

Mohamed Ali[1], Ibrahim A. Abd El-Moghith[2], Mohamed N. El-Derini[3] and Saad M. Darwish[2,*]

[1]Higher Institute for Tourism, Hotels and Computer, Al-Seyouf, Alexandria, 21533, Egypt
[2]Department of Information Technology, Institute of Graduate Studies and Research, Alexandria University, 21526, Egypt
[3]Department of Computer and Systems Engineering, Faculty of Engineering, Alexandria University, Alexandria, 21544, Egypt
*Corresponding Author: Saad M. Darwish. Email: saad.darwish@alexu.edu.e.g
Received: 29 June 2021; Accepted: 23 August 2021

Abstract: Routing is a key function in Wireless Sensor Networks (WSNs) since it facilitates data transfer to base stations. Routing attacks have the potential to destroy and degrade the functionality of WSNs. A trustworthy routing system is essential for routing security and WSN efficiency. Numerous methods have been implemented to build trust between routing nodes, including the use of cryptographic methods and centralized routing. Nonetheless, the majority of routing techniques are unworkable in reality due to the difficulty of properly identifying untrusted routing node activities. At the moment, there is no effective way to avoid malicious node attacks. As a consequence of these concerns, this paper proposes a trusted routing technique that combines blockchain infrastructure, deep neural networks, and Markov Decision Processes (MDPs) to improve the security and efficiency of WSN routing. To authenticate the transmission process, the suggested methodology makes use of a Proof of Authority (PoA) mechanism inside the blockchain network. The validation group required for proofing is chosen using a deep learning approach that prioritizes each node's characteristics. MDPs are then utilized to determine the suitable next-hop as a forwarding node capable of securely transmitting messages. According to testing data, our routing system outperforms current routing algorithms in a 50% malicious node routing scenario.

Keywords: Wireless sensor networks; trusted routing; deep neural network; blockchain; markov decision

1 Introduction

The multi-hop routing mechanism is a fundamental component of WSN technology. Nonetheless, the dispersed and dynamic characteristics of WSN render multi-hop routing susceptible to a variety of attack patterns, compromising security [1]. A malicious node may emit erroneous queue length information in order to increase the likelihood of receiving packets, hence altering the routing schedule of other routing nodes. Current routing algorithms have difficulty identifying such malicious nodes

since it is difficult to distinguish between two routing nodes' real-time changes in routing information [2]. When a malicious node receives data packets from a neighbor node, it discards them immediately rather than forwarding them to the next-hop neighbor node. This results in a data "black hole" in the network, which is difficult to detect in WSNs for routing nodes [3]. These malicious nodes might be external attackers or legal internal nodes that have been intercepted by external attackers. Trust management has been a common method of assuring the routing network's security in recent years. This approach enables the routing node to identify reasonably trustworthy routing connections efficiently.

There have been a significant amount of study in recent years on blockchain technology and routing algorithms [4]. The blockchain is a decentralized database that is maintained by several nodes and is essentially concerned with problems of trust and security. The blockchain relies on four critical technological features to deliver reliable and secure services that include distributed ledger, asymmetric encryption and authorization technique, the consensus method, and smart contracts. See [5,6] for different types of consensus methods. Proof of Authority (PoA) is a Byzantine consensus technique that is used for authorization and private blockchain technology [6]. The method is based on a group of reputable entities (i.e., authorities) referred to as validators. Validators gather, construct, and add blocks to the chain in response to consumer transactions. As a result, we must pay special attention to the selection of validators.

Recent advances in reinforcement learning have enabled wireless nodes to watch and acquire information from their effective local operational environment, learn, and make efficient routing choices on the fly [6]. A common decision-making strategy is to determine the optimal next-hop based on the present situation. Numerous academics have identified Markov Decision Systems (MDSs) as one of the most appropriate decision-making techniques for a random dynamic approach to solve this problem. Each hop in the routing process may be thought of as a state in this case, with each hop choosing one of the best hops. Then, by making consecutive judgments, messages may be sent effectively and securely to their destination [7].

We present a novel trustworthy routing system for WSNs based on blockchains and MDS in this study. We use proof of authority inside the blockchain network to validate the node for the transmission phase. To do this, a deep neural network is employed to choose the salient nodes that represent the node-dependent validators' features. Through the attributes associated with each node, a deep-learning model augments the collection of validators. The technique leverages the decentralized, tamper-resistant, and traceable nature of blockchain transactions to increase the integrity of routing information across routing nodes. The MDPs model is used to assist routing nodes in making more informed routing choices and selecting the most dependable and efficient routing links.

The rest of this article is as follows: Section 2 summarizes current strategies for a reliable routing method in WSNs. Section 3 discusses the suggested trustworthy routing model. Section 4 presents many experimental results that demonstrate the suggested model's efficiency. Finally, in Section 5, we will conclude the paper and outline future goals.

2 Related Work

This section will discuss many established trustworthy routing solutions for enhancing route security and dependability. Following that, we discuss some relevant methods to blockchain development routing methods. Finally, we investigate existing systems that use MDP in order to make the appropriate decision about message delivery [8–20]. By and large, all trust models in WSNs fall into two categories: central models and distributed models [21]. The base station or a specialized trustable

interface performs the action of aggregating and integrating the trust values of sensor nodes in central trust models. However, in distributed trust architectures, sensor nodes collect trust values on their own. Different approaches, technologies, and procedures for establishing trust have been suggested in WSNs, including fuzzy logic, probabilistic, and deterministic methodologies. The authors of [19] employed fuzzy logic to create a mechanism for evaluating trust in WSNs. The reputation values of nodes are used to calculate the reputation values of pathways in this manner. Then, for packet transmission, the route with the greatest reputation value is chosen. The fuzzy logic-based trust model is considered to be one of the core models; it should be mentioned that central models use a lot of energy. One advantage of fuzzy reasoning is that it is well-suited for very complicated systems whose actions are difficult to deduce. Additionally, the authors in [22] introduced a lightweight, low-energy adaptive hierarchy clustering technique for detecting suspicious node-to-node interactions.

Numerous proposals have been made recently to create a robust spatial routing algorithm for a wireless sensor network that can identify and communicate data about an incident to the base station [23]. The authors in [24] designed a safe routing protocol using hierarchical routing algorithms based on numerous criteria such as the distance between nodes and the base station, the distribution density of nodes, and the residual energy of nodes. In [25], the author proposed a secure communication and routing architecture based on the routing protocol's security architecture.

Several academics have recently combined the tamper-proof and traceable characteristics of blockchain technology with routing algorithms in order to improve the stability of routing nodes. The authors in [26] presented the trustworthy public key management framework. The method eliminated the need for central authentication and provide a decentralized inter-domain routing network by substituting a blockchain protocol for traditional public key infrastructures. In [27], a concurrent, multi-link blockchain-based communications network is created. The nodes may be classified as malicious or benign, depending on the methodology used to link the interrelated factors and the behavioral features of the blockchain-based data routing nodes. The authors in [28] developed a blockchain-based contractual routing system for networks with untrusted nodes using smart contracts. The critical principle is that the source node confirms the arrival of each hop routing to the smart contract, and malicious behavior nodes are recorded. The following packets will no longer pass through a malicious node that has been set up. A malicious node equipped with the token's algorithm, on the other hand, may fraudulently report that the packets were received. As a result, there are safety concerns [29,30].

As mentioned in [31], several studies have described a signal-to-noise ratio-based dynamic clustering-based routing system for wireless sensor networks. For the security of routing protocols, the authors used a cluster-based symmetric key cryptography technique. To address the problem in WSN, they created a unique bio-inspired trustworthy routing architecture combining ant colony optimization and Physarumautonomic optimization. The neighbor's conduct was observed with the purpose of assessing trust, and trust-based information was obtained. Another group of academics in [32] published a comprehensive study on the energy-efficient encryption and decoding algorithms for various keys. The introduced mechanism is responsible for encryption and decryption utilizing the DES and RSA algorithms. The quality of channels in wireless sensor networks may be enhanced by encrypting the data using various keys. As described in [33–37], several authors suggested securing ad hoc on-demand distance vector, a secure routing protocol based on initial encryption that can withstand certain routing assaults while ensuring the integrity and acknowledgment of identification.

Other authors introduced an energy-aware secure routing architecture that preserves a trusted environment, isolates misbehaving nodes, and has a minimal control cost. The authors devised an intrusion-tolerant routing system for wireless sensor networks. Although a malicious node may compromise certain nodes in the close area, it cannot cause extensive network disruption.

To protect data from eavesdropping assaults, several researchers have suggested a safe multipath routing protocol in sensor networks that use random network coding in directed diffusion routing. Current works addressed the issue of colluding and coordinated black hole attacks and suggested an approach that can be included in the ad hoc on-demand distance vector and secure ad hoc on-demand distance vector protocols. Numerous up-to-date papers have combined multipath routing with a feedback mechanism to identify nodes that lose packets and choose a different path for data transmission, therefore avoiding misbehaving nodes. The trust and energy-aware routing protocol is a safe routing framework that is based on three distinct frameworks and represents the trust value. The weighted trust and contributed residual energy are two of them, while the hop count is the third. A new trust model is predicted [37] that is built on message trust, data trust, and energy trust. The trustworthiness of data is determined by three factors: trust evaluation, fault tolerance, and data consistency. Energy trust identifies denial-of-service attacks by recognizing the node that spends the most energy in comparison to other nodes.

Recent developments in MDP solvers have enabled the solution of large-scale structures and sparked interest in WSNs in the future. For example, the authors of [29] established a WSN-controlled transmission power-level routing protocol using MDPs. The chosen power source is chosen by determining the best strategy for the MDP setup. The authors in [30] presented past work that examined relay selection in WSNs using an MDP. Additionally, to selecting from the explored relay nodes, a transmitting node may choose to continue searching for other relay choices. The node selects the reward to be dispersed to accessible relays throughout the probing process. The states are the finest historical recompense, as well as the recompense for unproven relays in earlier levels. The MDP formulation is then solved using the Bellman equation. Different indicators, such as transmission latency, energy usage, and anticipated network congestion, might be considered while making a choice. For further information, see [29].

To summarize, although the majority of secure protocols provide protection against replay and routing table poisoning attacks, they lack significant protection against black-hole attacks. Current blockchain-based routing systems rely on the proof of work concept to authenticate transactions (packets) in order to handle additional overhead. In comparison to previous protocols, the proposed approach utilizes proof of authority for authentication, which takes less computing time due to its reliance on a small number of key nodes (validators). The novelty here is the utilization of the deep neural network selecting the validators based on their node's features. These validators are then utilized by MDP for choosing the secure path.

3 The Proposed Framework

The primary objective of this suggested method is to build a reliable, trustworthy routing protocol for wireless sensor networks by integrating deep chain and Markov decision-making to provide secured routing. The suggested scheme's basic architecture is illustrated in Fig. 1, and it is composed of three phases: building a node data structure, selecting a validator through a deep learning model, and optimizing the next hop via MDP. Each of these stages is discussed in depth in the following subsections.

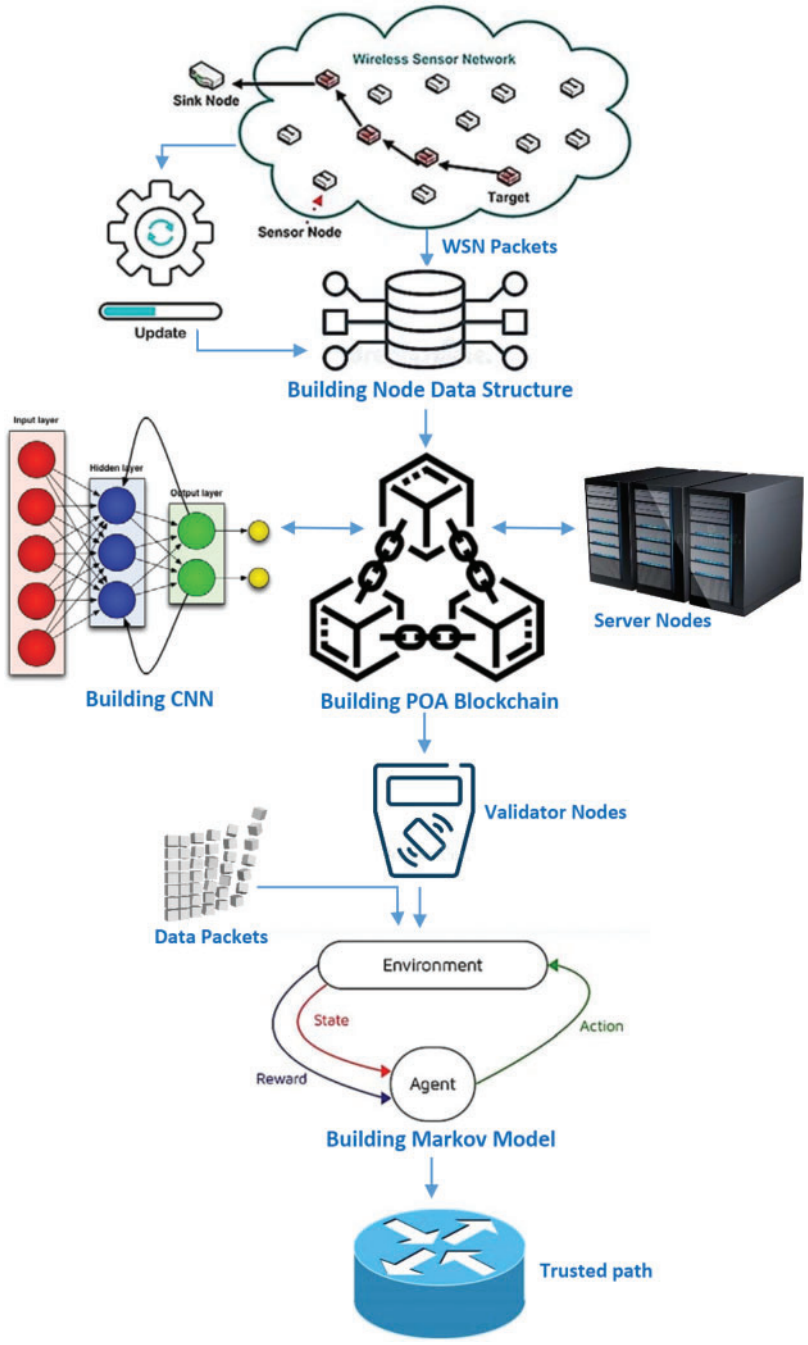

Figure 1: The proposed trusted routing scheme

We assume in this paper that the blockchain network is either a trusted routing node or that it rejects packets delivered by other routing nodes. Malicious routing nodes may publish erroneous routing information to the routing network, such as queue length information, thus interfering with the routing scheduling process. Additionally, they may serve as black hole attack nodes, refusing to forward data. However, we exclude collusion attacks between two routing nodes in order to execute

incorrect blockchain transactions. Additionally, we believe that a routing node may function solely as a normal or malicious node, implying that attacks are far from intermittent. Meanwhile, we disregard the sporadic aberrant behavior produced by the node's performance (e.g., a node does not send a message in time or loses the wireless spectrum). Herein, the server nodes are often static, while the routing nodes may be dynamic. However, the entrance and departure of nodes have no effect on our scheme, since our blockchain-based system's status information is likewise constantly updated.

3.1 Step 1: Build Node Data Structure

At first, all sensors operate in the same manner and serve no use as validators or slave nodes. They are not anonymous sensors; they have unique identification (e.g., anonymous addresses). Each packet in the transmission is the same size. There are two types of data transmission in a wireless sensor network: direct transmission and multi-hop data transfer. Multi-hop data transfer is utilized in this instance. With symmetrical communication, each cell in the WSN starts with the same amount of energy and remains static. During initialization, the function of any node that is originally set to un-state is converted into the validator or minion. Each node in the network maintains a data structure including a variety of information on the node property, such as the chosen action (validator or not), the energy level, the coverage, the connectivity, and the number of its neighbors. For more information, see [38].

3.2 Step 2: Validators Election Using Deep Neural Learning

After establishing the data structure for each node, the characteristics of these nodes are utilized to determine the most significant nodes that will act as validators in the blockchain-proof framework's authentication network. A deep neural network is used to make the selection. Deep learning techniques are used to learn functional hierarchies, in which features are constructed on higher levels using minor levels. The activation potentials supplied by each of the first hidden layer's unique input measurements are utilized to choose the most appropriate functions. The features are selected to provide more accurate classifications than the high-dimensional initial characteristics. The stacked RBMS (Deep Belief Network) is used as a BlackBox with its default settings in this paper. For more information, see [17,39,40]. This optimization problem is also sometimes termed empirical risk minimization. After completing this step, the selected nodes will be determined which will be used in blockchain-based routing networks. These selected nodes will be acted as validators and routing nodes.

3.3 Step 3: Blockchain-Based Routing Networks

To increase the trustworthiness and robustness of routing information, we integrate the blockchain, which is essentially a distributed ledger with tamper-proof, decentralization, and information traceability characteristics, into the wireless sensor network and use blockchain token transactions to record node-related information [41–47]. The primary structure is composed of two components: the routing network itself and the blockchain network. Packets are sent from the source terminal to the destination terminal through a routing node, which then chooses the next-hop routing node based on the routing policy received from MDPs. The MDP requests and gathers pertinent routing network status information from the blockchain network on a continuous basis. The packets will be sent to the target routing node and subsequently to the destination terminal after continuous transmission. Each blockchain system uses a unique consensus method to guarantee the transaction's fairness. We picked the PoA consensus method for our blockchain network because it is more efficient at processing transactions. Two distinct types of entities are specified in our concept for the PoA-based blockchain network.

Validator: validators are pre-authenticated nodes on the blockchain that have advanced authorization and are in charge of the PoA Blockchain's verification job. Their particular responsibilities include the execution of smart contracts, the verification of blockchain transactions, and the release of blockchain blocks. As described in step 2, a new validator may be introduced via the election of verified validators through a deep belief network. Even if a malicious validator exists, it is limited to attacking one of the contiguous blocks, at which time the malicious validator may be thrown out by other validator votes.

Minion: minions are fewer privileged nodes that are unable to conduct verification work in the PoA blockchain as validators. Each routing node in our system is likewise a minion with fewer privileges on the PoA blockchain, and it also has a unique blockchain address. They may start token contracts, activate certain contract functionalities, and access the blockchain for transaction details.

On the blockchain network, we utilize various blockchain tokens to represent the various packets that need to be sent to target nodes, with n unit tokens representing n unit related packets. The essence of a token is that it is a representation of the digitized data included in the smart contract's associated packets. Token contracts may be initiated by routing nodes to create tokens and map the state information of associated packets. They will exchange tokens through the token contract in order to transfer tokens depending on the transmitted and received packets. The consensus method between server nodes prevents malicious nodes from revising the token transactions arbitrarily; to some degree, the token properly reflects the packet transmitted between the routing nodes. After joining the blockchain-based routing network, each routing node is registered on the registration contract. When the routing node gets data from its offspring, it forwards the packets and drops the data. However, in the case of the blockchain next-hop routing node, the system must validate the routing information on the blockchain, which includes the address of the next-hop routing node, the number of packets delivered to the next node, and the timestamp. The routing information is then verified and updated on the blockchain by the server nodes through the blockchain consensus process. The proposed approach is consistent with the idea described in [1] about the implementation of a blockchain-based routing network.

3.4 Step 4: Next Hope Selection Using MDPS

MDP is used to determine the optimum strategy for maximizing a value function, which is defined as the expected sum of rewards at all decision epoch's infinite horizon issues, or as the anticipated total discounted reward or the expected average reward in infinite horizon problems [40]. When using MDP theory to opportunistic routing, the following issues must be considered: how the state is defined and how the choice is made. In general, the process of packet forwarding from one node to another may be thought of as a state change. Due to the fact that the packet must reach the target node in the fewest feasible hops, we examine only the finite horizon scenario; therefore, the set of decision epochs is represented by $T = \{0, 1, 2, \ldots, M\}$. $S = \{ 1, 2, \ldots, N \}$. N is the state space, with system state i defined as the ID of the node to which the packet belongs at a decision epoch t. A packet produced by the source node is sent to the destination node through many hops, which implies that the initial state (any node in the network) passes through several stages to reach the termination state, which in this case an absorption state is matching to the destination node.

Following that, we examine what actions are possible when the system's state at decision epoch t is i. In opportunistic routing, suitable candidate forwarders should be chosen from among neighbors and prioritized from the sender's perspective. However, from the receiver's perspective (the candidate nodes that received the packet), a coordinate mechanism is required to determine whether or not to

transmit the packet in response to other nodes' replies. The article makes the assumption that a flawless coordination mechanism is utilized between the candidate nodes, i.e., that packets are sent in exact accordance with the candidate nodes' priorities. As a result, we examine just the former choice scenario, in which the accessible action space consists of all potential ordered subsets of the sender's neighbor node-set. See [40] for more information regarding the steps of building MDP.

The key question of WSN routing is how best to find the next step in every hop. As mentioned in the literature, the key impacts on next-hop decision-taking involve trust, congestion probability and distance to the target". Readers looking for more information regarding how to compute these factors can refer to [39]. The optimal next step is a standard decision-making mechanism focused on the current circumstances, and we are implementing MDPs to address the issue as it is one of the better choices for a random dynamical system. Any hop on the route can be seen as a state; each hop is determined to pick one of the next best hops. The decision-making in each stage relies on the current scenario, and the entire routing method is efficient in chain decisions. Because hops are not infinite from source to destination, we follow a final Markov decision to solve it. The simple principle is that to find a sequence of better hops by candidates; we must use optimal decision metrics in the routing process as a criterion for the decisions to construct a Finite Markov Decision control system. As the network of the wireless sensor is a global network, central computation does not appeal to accomplish one path. Every node is, therefore, responsible for measuring and making decisions in any hop. Thereby, we find the decision of next-hop as a one-phase decision-making process; the purpose of the decision is to optimize the reward for each move.

4 Experimental Results

We constructed a prototype and compared its performance to that of existing state-of-the-art reinforcement learning-based routing algorithms, the trust-based algorithm, and the blockchain-based algorithm. We compared our system to a standard PoW-based blockchain system to determine our system's performance in terms of latency, consumption, and throughput. We created a PoA consortium blockchain and simulated a single server that would update the chain's transactions. The MDPs may receive all of the routing information they needed from public blockchain transactions. The consortium blockchain was developed using Solidity 0.8.4 to ensure the integrity of Ethereum transactions. We used the blockchain-based routing algorithm as a performance test [1]. To replicate actual packet arrival rates, we use the same setup as in [1], with 32 terminals in a 16×16 matrix randomly broadcasting packets to the destination point using a Poisson distribution with one packet per slot.

Additionally, we simulated 16×16 routing nodes that were capable of receiving and delivering actual packets in a maximum of one packet/slot depending on the routing strategy given by the MDPs model. Finally, the experiment collected data on average packet latency, transaction latency, and energy usage. In the experiments, there were 25% and 50% malicious nodes in the 16×16 routing nodes. The malicious nodes attempted to manufacture fake queue length information and use the BP algorithm weakness to cheat more packets or function as a black hole node and broadcast no packets. The server node equipment is configured as follows: CPU 2.6 GHz, RAM 16 GB, Storage 1 TB, Network 1000 Mb, OS Ubuntu Server 19.04. Whereas the sensor node devices' detailed configurations are as follows: CPU 1.2 GHz, RAM 1 GB, Storage 16 TB, Network 100 Mb, OS TinyOS Alliance 2.1.2.

4.1 Experiment 1: Comparative Analysis- Routing with Malicious Nodes

To understand whether malicious nodes may alter the routing scheduling algorithms, we ran an experiment that compared the Trust-based backpressure algorithm (TB-BP), the Q-Learning backpressure algorithm (QL-BP), and the Reinforcement learning and blockchain-based algorithm (RLBC) to our system. For further information on the comparative methodologies, see [1]. The comparison studies show that our method outperformed TB-BP, QL-BP, RLBC, and RLBC in the malicious routing environment as a function of packet arrival rate and average latency. As seen in Fig. 2, our technique outperforms the TB-BP method in a routing environment with 25% malicious nodes, saving about 74% of the time when compared to the TB-BP method, 58% when compared to the QL-BP methodology, and 21% when compared to the RLBC methodology. Additionally, we conducted comparative experiments in a routing environment with 50% malicious routing nodes (see Fig. 3) and discovered that it reduces delay by approximately 82% when compared to the TB-BP algorithm, 66% when compared to the QL-BP algorithm, and 28% when compared to the RLBC algorithm.

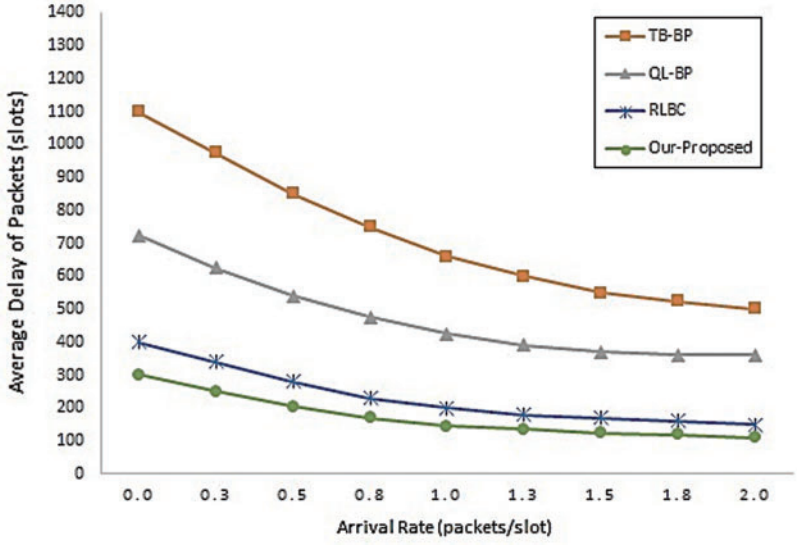

Figure 2: Average delay of packets with 25% malicious nodes

The experimental results demonstrate that our technique is not sensitive to malicious node impact in terms of average packet delay, and its efficacy demonstrates that it is conceivable to utilize it to enhance the routing algorithm's performance. While both the proposed system and the RLBC algorithm rely on the blockchain network to determine trust nodes and are based on the PoA algorithm, the comparative system identifies validators randomly, in contrast to the proposed system, which selects validators using deep learning (PoA-DL), which has the effect of determining the best trust nodes for paths that are not exposed to at least one attack.

4.2 Experiment 2: System Efficiency with PoA-DL

In the second set of experiments, we compared our blockchain system based on the PoA-DL consensus mechanism, which employs deep learning to determine validators, to a traditional PoA-based blockchain system, which employs a random selection of validators, and to a traditional PoW-based blockchain system. Throughout the investigation, we captured experimental data such

as transaction delay and throughput. We used transaction packaging time as a proxy for average token transaction delay. We measured the latency of token transactions on PoA-DL, PoA, and PoW blockchain systems as the arrival rate increased. The results of the experiment are shown in Fig. 4.

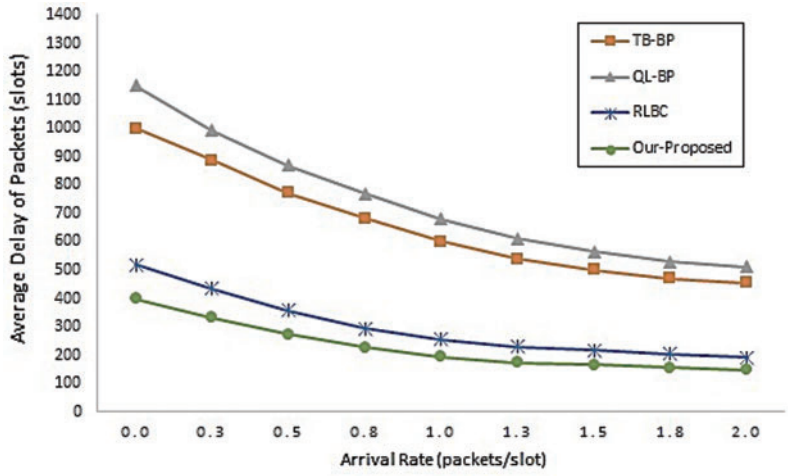

Figure 3: Average delay of packets with 50% malicious nodes

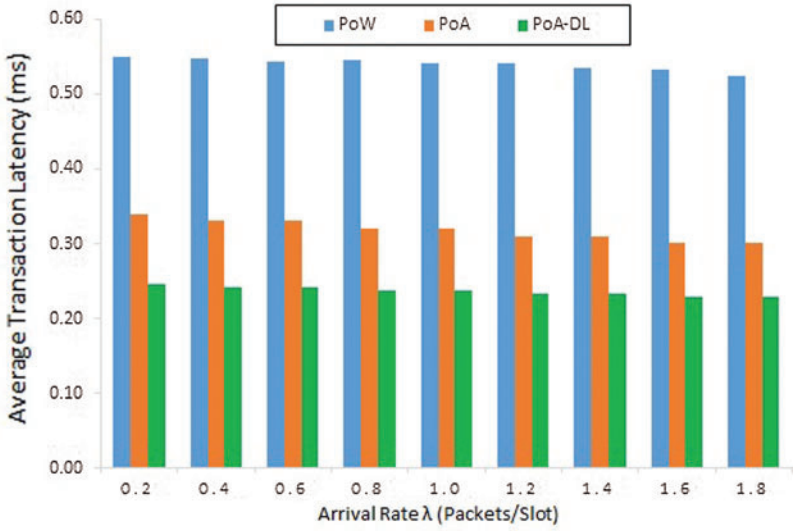

Figure 4: Average transaction latency for both PoA and PoW-based blockchain systems

As can be seen from Fig. 4, the transaction's latency is pretty steady and does not vary much with the arrival rate. Our PoA-DL blockchain system had an average transaction latency of roughly 0.24 milliseconds, whereas the PoA blockchain system had an average transaction delay of roughly 0.32 milliseconds. Whereas the PoW blockchain technology has a latency of roughly 0.55 ms. Results indicate that our blockchain system, which is based on the PoA-DL consensus mechanism, can reduce around 25% and 56% of transaction delay, respectively, when compared to PoA and PoW. Such a delay in token transactions is acceptable since it has a negligible effect on the routing schedule. It is

both feasible and efficient to gather and maintain routing scheduling information using our PoA-DL blockchain solution. The proposed approach is efficient since the most secure nodes are chosen by applying deep learning methods to choose the best validators. Later, these nodes will be utilized by MDP to determine the optimal routing route; since there is no risk of assaulting these nodes, transaction latency will be decreased.

4.3 Experiment 3: Token Transaction Throughput with POA-DL

The final set of experiments validated the proposed trusted routing scheme's efficiency in terms of token transaction throughput. The throughput of token transactions demonstrates the blockchain system's capacity to manage concurrent token transactions. The results in Fig. 5 demonstrate that as the rate of synchronous requests grows, the token transaction throughput climbs steadily, and the curve gradually flattens out as the throughput reaches its peak. The token transaction throughput of our blockchain system using the PoA-DL consensus mechanism is stable at 3630 concurrent requests per second, while the symbolic transaction throughput of the RLBC comparative system using the PoA consensus mechanism is stable at 3,300 concurrent requests per second, and the classic blockchain system using the PoW consensus mechanism is only stable at around 1,500 concurrent requests per second. The experimental results demonstrate that the PoA-DL-based method has a more efficient transaction processing capacity while dealing with concurrent searches due to the restricted number of validators. It is appropriate and legitimate to use the PoA-DL algorithm as the blockchain system's consensus mechanism. This PoA-DL blockchain-based routing scheduling technique is capable of successfully coping with the routing environment's high concurrent request volume.

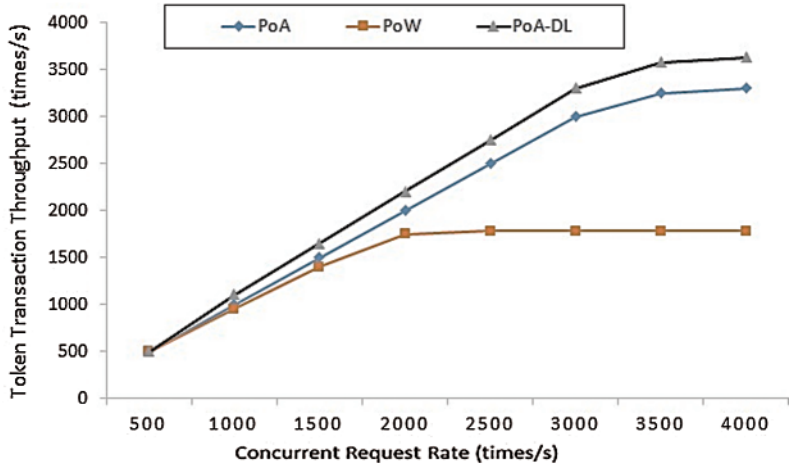

Figure 5: Throughput of transaction token for both PoA-DL, PoA and PoW-based blockchain systems

Due to the fact that the proposed model uses MDP for routing rather than reinforcement learning as in [1], the solution of an MDP model referred to as a policy, may be implemented using a routing lookup table. This table may be easily saved in the sensor node's memory for online operations. As a result, the MDP model can be applied to even the smallest and most resource-constrained nodes without requiring excessive computation. Additionally, near-optimal solutions may be constructed to approach optimum decision policies, allowing for the creation of WSN algorithms that are less computationally intensive [28]. The reinforcement learning-based routing, on the other hand, is based on modifying the weight matrix to attain the required performance. In general, constructing an ideal

weight matrix is a difficult task that is often solved by trial and error. To summarize, using MPD for routing improves the model's transaction throughput [18].

5 Conclusions and Future Work

We proposed a trusted routing technique in this research that enhances the routing network's performance by integrating deep blockchain and Markov decision processes. The routing packets are represented by the blockchain token, and each routing transaction is validated by validator nodes prior to being disseminated to the blockchain network. By ensuring the traceability and immutability of each routing transaction tracker, routing nodes will be able to monitor dynamic and trustworthy routing information on the blockchain network. Additionally, we build the MDP architecture in such a way that routes are discovered quickly and connections to hostile nodes are avoided. Our test results indicate that our schema is capable of rapidly eliminating hostile node attacks, and the device has exceptionally low latency. We want to use our method in the future to evaluate the effectiveness and portability of other route scheduling strategies to the backpressure technique. Additionally, we aim to include blockchain-based data validation tools.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Yang, S. He, Y. Xu, L. Chen and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, pp. 1–19, 2019.

[2] Z. Jiao, B. Zhang, C. Li and H. Mouftah, "Backpressure-based routing and scheduling protocols for wireless multihop networks-a survey," *IEEE Wireless Communications*, vol. 23, no. 1, pp. 102–110, 2016.

[3] F. Ahmed and Y. Ko, "Mitigation of black hole attacks in routing protocol for low power and lossy networks," *Security and Communication Networks*, vol. 9, no. 18, pp. 5143–5154, 2016.

[4] F. Abdel-Fattah, K. Farhan, F. Al-Tarawneh and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," in *Proc. IEEE Jordan Int. Joint Conf. on Electrical Engineering and Information Technology*, Jordan, pp. 28–33, 2019.

[5] A. Angrish, B. Craver, M. Hasan and B. Starly, "A case study for blockchain in manufacturing:"fabRec": A prototype for peer-to-peer network of manufacturing nodes," *Proc. Manufacturing*, vol. 26, no. 1, pp. 1180–1192, 2018.

[6] L. Bach, B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 42nd Int. Convention on Information and Communication Technology, Electronics and Microelectronics*, Croatia, pp. 1545–1550, 2018.

[7] E. Wang, Z. Nie, Z. Du and Y. Ye, "MDPRP: Markov decision process based routing protocol for mobile WSNs," in *Proc. Springer Conf. on Geo-Informatics in Resource Management and Sustainable Ecosystem*, Singapore, pp. 91–99, 2016.

[8] I. Abd El-Moghith and S. Darwish, "A deep blockchain-based trusted routing scheme for wireless sensor networks," in *Proc. Int. Conf. on Advanced Intelligent Systems and Informatics*, Egypt, pp. 282–291, 2020.

[9] Y. Lv, Y. Liu and J. Hua, "A study on the application of WSN positioning technology to unattended areas" *IEEE Access*, vol. 7, pp. 38085–38099, 2019.

[10] A. Ahmed, K. Abu Bakar, M. Channa, K. Haseeb and A. W. Khan, "TERP: A trust and energy aware routing protocol for wireless sensor network," *IEEE Sensors Journal*, vol. 15, no. 12, pp. 6962–6972, 2015.

[11] D. Zhang, G. Li, K. Zheng, X. Ming and Z. H. Pan, "An energy-balanced routing method based on forward-aware factor for wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 766–773, 2014.
[12] L. Tang, Z. Lu and B. Fan, "Energy efficient and reliable routing algorithm for wireless sensors networks," *Applied Sciences*, vol. 10, no. 5, pp. 1–16, 2020.
[13] J. Garay, A. Kiayias and N. Leonardos, "The bitcoin backbone protocol: analysis and applications," in *Proc. Annual Interrelation Conf. on the Theory and Applications of Cryptographic Techniques*, Germany, pp. 281–310, 2015.
[14] W. Cai1, Z. Wang, J. Ernst, Z. Hong, C. Feng *et al.*, "Decentralized applications the blockchain-empowered software system," *IEEE Access*, vol. 6, pp. 53019–53033, 2018.
[15] W. Thin, N. Dong, G. Bai and J. S. Dong "Formal analysis of a proof-of-stake blockchain," in *Proc. IEEE Int. Conf. on Engineering of Complex Computer System*, Australia, pp. 197–200, 2018.
[16] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, Canada, pp. 2567–2572, 2017.
[17] S. Seshia, A. Desai, T. Dreossi, D. Fremont, S. Ghosh *et al.*, "Formal specification for deep neural networks," in *Proc. Int. Symp. on Automated Technology for Verification and Analysis*, USA, pp. 20–34, 2018.
[18] T. Dreossi, A. Donzé and S. Seshia, "Compositional falsification of cyber-physical systems with machine learning components," *Journal of Automated Reasoning*, vol. 63, no. 4, pp. 1031–1053, 2019.
[19] X. Liu, G. Zhao, X. Wang, Y. Lin, Z. Zhou *et al.*, "MDP-Based quantitative analysis framework for proof of authority," in *Proc. Int. Conf. in Cyber-Enabled Distributed Computing and Knowledge Discovery*, China, pp. 227–236, 2019.
[20] L. Kiffer, R. Rajaraman and A. Shelat, "A better method to analyze blockchain consistency," in *Proc. ACM Conf. on Computer and Communications Security*, Canada, pp. 729–744, 2018.
[21] A. Beheshtiasl and A. Ghaffari, "Secure and trust-aware routing scheme in wireless sensor networks," *Wireless Personal Communications*, vol. 107, no. 4, pp. 1799–1814, 2019.
[22] Y. Arfat and R. A. Shaikh, "A survey on secure routing protocols in wireless sensor networks," *International Journal of Wireless and Microwave Technologies*, vol. 6, no. 3, pp. 9–19, 2016.
[23] Y. Wang, Z. Ye, P. Wan and J. Zhao, "A survey of dynamic spectrum allocation based on reinforcement learning algorithms in cognitive radio networks," *Artificial Intelligence Review*, vol. 51, no. 3, pp. 493–506, 2019.
[24] C. Deepa and B. Latha, "HHCS: hybrid hierarchical cluster based secure routing protocol for wireless sensor networks", in *Proc. Int. Conf. on Information Communication and Embedded Systems*, India, pp. 1–6, 2014.
[25] F. Khan, "Secure communication and routing architecture in wireless sensor networks", in *Proc. IEEE Int. Conf. on Consumer Electronics*, Japan, pp. 647–650, 2014.
[26] A. G-Arevalillo and P. Papadimitratos, "Blockchain-based public key infrastructure for inter-domain secure routing." in *Proc. Int. Workshop on Open Problems in Network Security*, Sweden, pp. 20–38, 2017.
[27] J. Li, G. Liang and T. Liu, "A novel multi-link integrated factor algorithm considering node trust degree for blockchain-based communication," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 8, pp. 3766–3788, 2017.
[28] G. Ramezan and C. Leung, "A blockchain-based contractual routing protocol for the internet of things using smart contracts," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–15, 2018.
[29] M. Abu Alsheikh, D. Hoang, D. Niyato, H. Tan and S. Lin, "Markov decision processes with applications in wireless sensor networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1239–1267, 2015.
[30] W. Rehan, S. Fischer, M. Rehan and M. Rehmani, "A comprehensive survey on multichannel routing in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 95, pp. 1–25, 2017.

[31] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi and A. Kannan, "Qos aware trust based routing algorithm for wireless sensor networks," *Wireless Personal Communications*, vol. 110, no. 4, pp. 1637–1658, 2020.
[32] R. Raghav, K. Thirugnansambandam and D. Anguraj, "Beeware routing scheme for detecting network layer attacks in wireless sensor networks," *Wireless Personal Communications*, vol. 112, no. 4, pp. 2439–2459, 2020.
[33] S. Taterh, Y. Meena and G. Paliwal, "Performance analysis of ad hoc on-demand distance vector routing protocol for mobile ad hoc networks," In *Computational Network Application Tools for Performance Management*, Springer, Singapore, pp. 235–245, 2020.
[34] A. Ahmed, K. Abu Bakar, M. I. Channa, A. Khan and K. Haseeb, "Energy-aware and secure routing with trust for disaster response wireless sensor network," *Peer-to-Peer Networking and Applications*, vol. 10, no. 1, pp. 216–237, 2017.
[35] S. Sharma, A. Singh and V. Dattana, "A survey of IoT routing protocols based on security and trust management," in *Proc. IEEE Int. Conf. on Reliability, Infocom Technologies and Optimization*, India, pp. 623–629, 2020.
[36] M. Boulaiche, "Survey of secure routing protocols for wireless ad hoc networks," *Wireless Personal Communications*, vol. 114, no. 1, pp. 483–517, 2020.
[37] S. Prabhu and M. Anita, "Trust based secure routing mechanisms for wireless sensor networks: A survey," in *Proc. IEEE Int. Conf. on Advanced Computing and Communication Systems*, India, pp. 1003–1009, 2020.
[38] S. Darwish, M. El-Dirini and I. Abd El-Moghith, "An adaptive cellular automata scheme for diagnosis of fault tolerance and connectivity preserving in wireless sensor networks," *Alexandria Engineering Journal*, vol. 57, no. 4, pp. 4267–4275, 2018.
[39] N. Sabar, A. Turky, A. Song and A. Sattar, "An evolutionary hyper-heuristic to optimise deep belief networks for image reconstruction," *Applied Soft Computing*, vol. 97, pp. 1–24, 2020.
[40] J. Hao, X. Jia, Z. Han, B. Yang and D. Peng, "Design of opportunistic routing based on markov decision process," in *Proc. IEEE Chinese Control Conf.*, China, pp. 8976–8981, 2017.
[41] K. Yu, Z. Guo, Y. Shen, W. Wang, J. Lin *et al.*, "Secure artificial intelligence of things for implicit group recommendations," *IEEE Internet of Things Journal, (Early Access)*, vol. 9, pp. 1–10, 2021.
[42] K. Yu, L. Tan, M. Aloqaily, H. Yang and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IoT," *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 7669–7678, 2021.
[43] L. Tan, H. Xiao, K. Yu, M. Aloqaily and Y. Jararweh, "A blockchain-empowered crowdsourcing system for 5G-enabled smart cities," *Computer Standards & Interfaces*, vol. 76, pp. 1–21, 2021.
[44] L. Tan, K. Yu, F. Ming, X. Chen and G. Srivastava, "Secure and resilient artificial intelligence of things: A honeynet approach for threat detection and situational awareness", *IEEE consumer electronics magazine*," *(Early Access)*, vol. 10, pp. 1–13, 2021.
[45] L. Tan, N. Shi, K. Yu, M. Aloqaily and Y. Jararweh, "A blockchain-empowered access control framework for smart devices in green internet of things," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–20, 2021.
[46] C. Feng, K. Yu, A. Bashir, Y. Al-Otaibi, Y. Lu *et al.*, "Efficient and secure data sharing for 5G flying drones: A blockchain-enabled approach," *IEEE Network*, vol. 35, no. 1, pp. 130–137, 2021.
[47] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin *et al.*, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," *IEEE Journal of Biomedical and Health Informatics, (Early Access)*, vol. 25, pp. 1–15, 2021.