Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7281872, 15 pages
https://doi.org/10.1155/2022/7281872

Research Article

Exploiting Blockchain and RMCV-Based Malicious Node Detection in ETD-LEACH for Wireless Sensor Networks

Asad Ullah Khan,[1,2] Maimoona Bint E. Sajid,[1] Abdul Rauf,[3] Malik Najmus Saqib,[4] Fawad Zaman,[5] and Nadeem Javaid[1,6]

[1]*Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan*
[2]*Department of Computer Science, Federal Urdu University, Islamabad 44000, Pakistan*
[3]*Hamdard University, Islamabad 44000, Pakistan*
[4]*Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia*
[5]*Department of Electrical and Computer Engineering, COMSATS University Islamabad, Islamabad 44000, Pakistan*
[6]*School of Computer Science, University of Technology Sydney, Ultimo, NSW 2007, Australia*

Correspondence should be addressed to Nadeem Javaid; nadeemjavaidqau@gmail.com

Received 5 March 2022; Revised 1 July 2022; Accepted 8 July 2022; Published 2 August 2022

Academic Editor: A.H. Alamoodi

In this paper, a routing protocol based on energy temperature degree-low energy-adaptive clustering hierarchy (ETD-LEACH) is proposed. In the protocol, nodes consume less energy when transmitting data, which improves the network lifetime. The proposed protocol selects the cluster heads (CHs) on the bases of degree, temperature, and energy to perform routing. Moreover, for solving the issue of a single point of failure, the blockchain is utilized. The data transactions are also housed in the blockchain, which is deployed on the CHs and BSs, as, in blockchain, multiple nodes take part. Therefore, to perform a consensus between them, a proof-of-authority (PoA) consensus mechanism is used in the underlying work. In the blockchain, the secure hashing algorithm-256 (SHA-256) is used for secure hashing of data transactions. Furthermore, malicious nodes are detected during the routing using the real-time message content validation (RMCV) scheme in the ETD-LEACH protocol. The proposed model is evaluated under the denial-of-service (DoS) attack, the man-in-the-middle (MITM) attack, and the smart contract analysis performed by the Oyente tool. The performance of the proposed model is evaluated through simulations. The ETD-LEACH and energy threshold-low energy-adaptive clustering hierarchy (ETH-LEACH) protocols are compared using different parameters like number of alive nodes, energy consumption, throughput, and delay. ETD-LEACH consumes less energy and has a better network lifetime as compared to ETH-LEACH. In addition, the RMCV-ETD-LEACH network performance is better than that of both DoS-ETD-LEACH and MITM-ETD-LEACH. Moreover, PoA transaction cost is less than that of proof of work. Also, the execution time of SHA-256 is less than the execution time of SHA-512. Moreover, the value of the packet delivery ratio (PDR) is found to be 89.9% and 99.9% with and without the malicious nodes, respectively.

1. Introduction

In the past few years, the wireless sensor networks (WSNs) have been globally used in different fields of life like the military, transportation, health applications, etc. [1, 2]. The WSN consists of compact-sized sensors that are deployed in the targeted environment. The sensors are used for tracking and monitoring purposes. In tracking purposes, sensors track enemies, animals, road traffic, etc., while in the monitoring process, sensors monitor the environment, patients' health, malicious activities, etc. [3, 4].

Unfortunately, WSNs have high security threats. The attackers attack the network and affect the network performance. Malicious nodes take part and tamper or misroute the data packets [5, 6]. Moreover, sensors are resource-constrained devices and have limited storage for storing the sensed data, while the base station (BS) is a centralized entity that causes a high chance of a single point of failure.

Therefore, blockchain is used in the WSNs to store data and provide security.

The blockchain is a decentralized, distributed, transparent, and tamper-proof ledger. In the blockchain, data transactions of the networks are stored in blocks. All blocks are chronologically connected with each other using hashes. The block structure consists of a block header and body. In the block header, there is a nonce, hash, timestamp, and Merkle tree, as shown in Figure 1, while all transactional informational is stored in the body. The nonce contains a 32-bit value that shows that the block is generated correctly. It is used in the block-mining process. Proof of work (PoW), proof of authority (PoA), and proof of stake are some of the prominent consensus mechanisms that are used to perform mining in blockchain networks. Besides, the hash is of two types: block hash and Merkle root hash. The hash is generated by the secure hashing algorithm-256 (SHA-256). Moreover, the timestamp shows the time when a new block is generated. In the Merkle tree, the hashes of all the transactions are stored in the root, and it provides security to the transactions. Therefore, it is difficult for a third party to tamper with the transactions.

Moreover, once the data transaction is added to the block, it is difficult to tamper. Therefore, blockchain is used to avoid a single point of failure. Furthermore, in the WSNs, the blockchain uses double SHA-256 for security that consumes high computational power. Furthermore, the PoW consensus mechanism is used, which incurs high transaction costs. Moreover, in WSNs, CHs are resource constrained, and their energy is drained at an early stage. Therefore, all nodes die early, which affects the network lifetime [3, 5, 7]. Moreover, in the WSNs, malicious nodes attack the network while performing routing to tamper with the data packets [8–10].

In this paper, we focus on the efficient selection of cluster heads (CHs), malicious nodes' detection, and secure routing data. The CHs are efficiently selected using the energy threshold-low energy-adaptive clustering hierarchy (ETD-LEACH), while the malicious nodes are detected using real-time message content validation (RMCV). Furthermore, the PoA consensus mechanism is used to perform consensus between the network nodes while SHA-256 is used for secure hashing the routing data. Moving ahead, the robustness and resilience of the proposed model is checked by evaluating it against denial-of-service (DoS) and man-in-the-middle (MITM) attacks. The smart contract is also assessed against different vulnerabilities using Oyente.

The major contributions made in the proposed work are as follows.

(1) ETD-LEACH and RMCV are used for efficient clustering and malicious nodes' detection, respectively

(2) PoA consensus mechanism is used for consensus while SHA-256 is used for secure hashing of the routing data

(3) The proposed model is evaluated against DoS and MITM attacks, while Oyente tool is employed to check the smart contract's resilience against different vulnerabilities

The organization of the remaining manuscript is as follows. The related work is provided in Section 2 while Section 3 comprises the explanation of the proposed system model. The validation of the proposed work is performed through simulations, the results of which are discussed in Section 4. Furthermore, the resilience of the smart contract against different vulnerabilities is discussed in Section 5, while Section 6 presents the conclusion. Table 1 presents the list of acronyms.

2. Related Work

The Internet of Things (IoTs) is a subdomain of WSN. In IoTs, multiple nodes communicated with each other via wireless connectivity. To disturb the communication, the nodes are attacked both internally and externally. When attacked internally (referred to as internal attack), malicious nodes tamper the data, while when attacked externally (referred to as external attack), malicious nodes attack the whole network, which is more damaging than the damage caused by an internal attack. Therefore, malicious nodes' detection is the main issue nowadays [11]. In [12], the authors work on localization issues in WSN. However, malicious nodes tamper the location of unknown nodes; therefore, nodes' energy is consumed. The high energy consumption affects the network lifetime [13].

In the WSN [1], authentication of the nodes is not efficient. However, a third party performs authentication, which has a high chance of performing maliciously. In [14], while performing routing, detection of the data-tampering nodes is performed. Furthermore, in [7], IoTs generate a large amount of data; therefore, security risks in terms of tampering data and unauthorized devices accessing the data are increased. However, malicious nodes' presence affects the customer's trust.

The sensors sense the data and forward it to the destination [9]. A WSN is mostly used in military wars, education, healthcare, etc. The security issue arises in the WSN while sending a data packet from source to destination. The security issues involve the malicious nodes attacking the data packet or a legitimate node acting selfishly. Moreover, a malicious node creates a black hole attack in the network. The data packets are not being forwarded to the destination and are dropped on their way to the destination due to the malicious nodes. Therefore, to resolve the above-mentioned security issues, the authors propose a central management routing protocol in which the intermediary node acts as a gateway and third party [9]. However, central authority or third party does not provide a fair secure model. Malicious nodes attack the central authority. Furthermore, in routing, a loop routing issue also arises. Malicious nodes broadcast false routing information; therefore, the data packet does not reach the destination and continuously moves in the loop [15, 16].

IoTs are used worldwide for every field of life [17]. However, IoTs have less memory and computational power and a

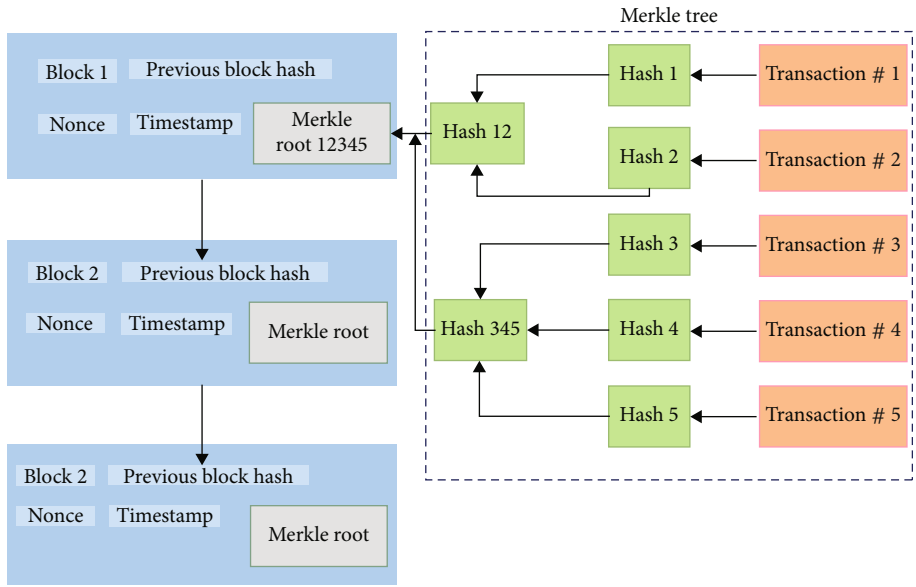

Figure 1: Block's structure.

high rate of security threats. Furthermore, the blockchain is widely used in WSN [18]; however, the consensus used in blockchain takes much time in mining data and is not suitable for smart health.

In [19], it is mentioned that WSNs are used in each field of life. However, sensors are not secured, and customers are not satisfied because of the lack of trust in terms of packet drop, delay, and energy consumption [20, 21]. In [22], the blockchain is widely used in each application for data storage and security. However, the number of users increases with the increase in applications; therefore, the PoW consensus mechanism incurs a large computational cost. Moreover, no consensus mechanism is scalable; therefore, a scalability issue also arises.

In [23], the authors highlight the issue of the centralized database. IoTs are used everywhere like smart cities, healthcare, e-commerce, etc. Large data is accessed and stored on the fog layer, which is centralized and not secure. In [24], the authors highlight the issue of security, in which a third party is involved in the communication of two parties. However, the third party is not trustworthy. In the past, authors resolve this issue by using a central authority (CA) that communicates with both parties. However, in CA, there is an issue of a single point of failure. Therefore, in the communication of IoTs, the main challenges are the single point of failure and connectivity between the increasing number of devices in IoT networks.

In [25], the authors discuss the issue of localization in WSNs. In the past, authors propose localization algorithms [26]; however, the algorithms are not secure, consume high computational resources of BS, and do not provide an accurate location of sensors. Therefore, securing sensor nodes' localization remains a challenge. The authors face the issue of security in smart cities, fog, and cloud in [27]. There is another issue of trustworthiness among nodes and privacy of data. The data is not secure against unauthorized users. Moreover, smart cities are scalable; however, there is an issue of data traceability.

In [28], authors highlight the issues related to a centralized entity and nodes' malicious behavior. In traditional models, authors use centralized servers that process and store the data in a centralized manner. Therefore, there is a high chance that unauthorized nodes access the data and tamper or misuse the data. Furthermore, in the centralized system, there is a chance of a single point of failure. In [29, 30], IoTs share the data both intranetwork and internetwork. The data is shared on a large scale; however, data is not secured because users are not authorized. Traditional models use CA, digital signature, etc. However, these all are centralized and not secure.

3. System Model

3.1. Network Deployment. In the proposed system model, we deploy ordinary nodes (ONs) in the network, select the cluster heads (CHs) from ONs, and perform routing. The CHs' selection and routing are performed using the ETD-LEACH protocol. The ETD-LEACH is used for reactive networks. In these networks, sudden changes occur in the environment like change in temperature, humidity, etc., and nodes sense the data immediately. The ONs sense data from the surroundings and forward it to the CHs, which have more energy than ONs. Afterwards, CHs forward energy to the BSs. The ETD-LEACH protocol is divided into two phases that are mentioned as follows.

(1) Cluster formation

(2) Data transmission

3.1.1. Cluster Formation. At the initial stage, nodes are deployed with energy $E_O = 1.5$. When the sensors sense the same type of data, they are grouped in one cluster. After

Table 1: List of acronyms.

Acronyms	Description
BS	Base station
CA	Central authority
CHs	Cluster heads
CV	Current value
DoS	Denial of service
ETD-LEACH	Energy temperature degree-low energy-adaptive clustering hierarchy
ETH-LEACH	Energy threshold-low energy-adaptive clustering hierarchy
HT	Hard threshold
IoTs	Internet of things
MITM	Man-in-the-middle
ONs	Ordinary nodes
PDR	Packet delivery ratio
PoA	Proof of authority
PoW	Proof of work
RMCV	Real-time message content validation
SHA-256	Secure hashing algorithm-256
ST	Soft threshold
WSNs	Wireless sensor networks
Con	Conflict
e	Exponential function
etype	Type of message
G	Group of ONs
info	Information
loc_i	Location of sender
loc_q	Location of receiver
P	Probability of ONs
n	Nodes
CV	Current sensed value

clusters' formation, CHs are created from ONs based on energy, temperature, and degree, in which those ONs are selected as CHs, which have high energy and degree. These CHs sense the temperature value within the given range that gives the current sensing value (CV), as provided in Equation (1).

3.1.2. Data Transmission. In the ETD-LEACH protocol, data is transmitted hierarchically [31]. The ONs sense the data and forward it to the CHs, which further transmit the data to the BS. In this protocol, data is transmitted to the BS when sensed data values meet the given thresholds. The following two types of thresholds are used in the proposed work.

(a) *Hard threshold (HT)*: in the HT, when ONs sense the data and data values are found to be greater than or equal to HT, then ONs transmit the sensed data towards the CHs. The sensed data is calculated in the following equation.

$$\text{CV} = \text{temp}i \sum (\text{temp}f - \text{temp}i) * \text{rand}\,(1, 1), \quad (1)$$

where CV is the current sensed value and temp$i$ and temp$f$ are the minimum and maximum ranges of temperature, respectively. The rand is a random function.

(b) *Soft threshold (ST)*: in the ST, ONs transmit data only in the condition when the difference of CV and the previously sensed value is greater than or equal to the given ST

Therefore, the ETD-LEACH network lifetime is better because less energy is consumed when data is transmitted in the low range. Moreover, only that data is transmitted to BS that meets the thresholds.

3.2. Blockchain Deployment. After the deployment of the WSN, the blockchain is deployed on CHs and BS. Blockchain is the decentralized ledger in which data hashes are stored on CHs and data is transmitted to BS. The private blockchain is utilized, and the PoA consensus mechanism is used for mining new blocks. In the blockchain, the SHA-256 hashing algorithm is used to secure data. In SHA-256 [32, 33], data is converted into ciphertext, and a hash of 256 bits is generated, which is difficult to tamper. The size of the generated hash is the same for one letter, one paragraph, and one word. The block size is 512 bits, and the padding length is 10 bits. Moreover, extra data can be added at the end of the message, as shown in Figure 2.

3.3. Malicious Nodes' Detection. Malicious nodes are present in the network, which act as legitimate nodes and send the data packets during routing. Malicious nodes are detected using the real-time message content validation (RMCV) scheme. In this scheme [34], malicious nodes are detected by validating the message content. Data packets are divided into clusters; same types of data packets are gathered in one cluster while different types of data packets are grouped in different clusters. Then, data packet validation is performed in intraclustering to find false and true data packets. In this manner, malicious nodes are detected. Figure 3 put forwards the overview of malicious nodes' detection process. The format of the data packet is given in the following equation.

$$\text{DataPacket} = \text{Msg}\left(\text{loc}_q, \text{loc}_{\text{int}}, \text{etype}, \text{info}, \text{te}, \text{mpath}\right), \quad (2)$$

where loc_q is the location of the receiver, loc_{int} is the location of the sender, and etype is the message type like temperature conditions, e.g., rainy and sunny. The info is the information that the message contains like temperature is an event and its info is sunny, rainy, and cloudy. te is the time in which a message is received by the receiver. The mpath shows the path from where the data packet

```
1: Deployment of nodes and BS
2: Degree of nodes
3: For i = 1 : nodes do
4:   For j = 1 : nodes do
5:     If i ≠ j then
6:       Find distance of the nodes
7:       If distance < = 20 then
8:         Add index of the nodes
9:       End if
10:    End if
11:  End for
12: End for
13: For i = 1 : nodes do
14:   For j = 1 : nodes do
15:     Check the nodes, neighbors
16:     If neighbor == 0 then
17:       A(i, j) = 0
18:     Else
19:       A(i, j) = 1
20:     End if
21:   End for
22: End for
23: For r = 1 : rounds do
24:   For i = 1 : n do
25:     If energy < = 0 then
26:       Then all nodes will die
27:     End if
28:     If dead == 1 then
29:       First node dies
30:     End if
31:     If dead==0.5∗nodes then
32:       Half nodes die
33:     End if
34:     If dead == nodes then
35:       Full nodes die
36:     End if
37:   End for
38:   For i = 1 : nodes do
39:     On the basis of degree, CHs are selected
40:     If current sensed value = temperature initial +
    (temperature initial + temperature final) ∗ rand (1, 1) then
41:       If sensed value > = hard threshold then
42:         Test = current value − sensed value
43:         If test > = soft threshold then
44:           Perform CHs' selection
45:           Send data packets
46:         End if
47:       End if
48:     End if
49:   End for
50: End for
```

Algorithm 1: ETD-LEACH protocol.

is transmitted. After sending data packets to the destination, trustworthiness of data packets is calculated using Equation (3).

$$\text{Trust}(c) = \frac{\left(e^{\xi} - e^{\xi}.\text{Con}_c\right)\text{Support}'(c)}{e^{\xi} - 1}. \tag{3}$$

In Equation (3), e is the exponential function with ξ, which is a positive number. The e^{ξ} increases with the increase in Con_c conflicts in data packets' content. Conflict is either true or false. The $\text{Support}'(c)$ is the function that shows the path from where the data packet is sent. When the same paths are used for data packet transmission, then there is a high chance of a false data packet being

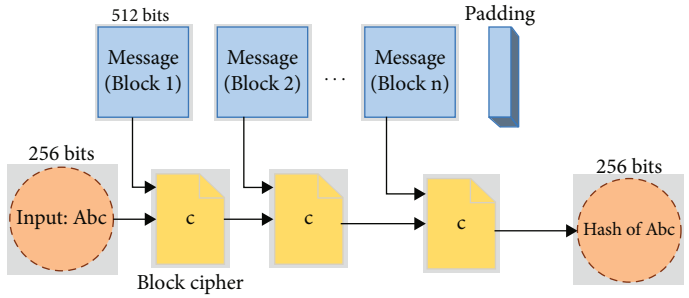

Figure 2: SHA-256.

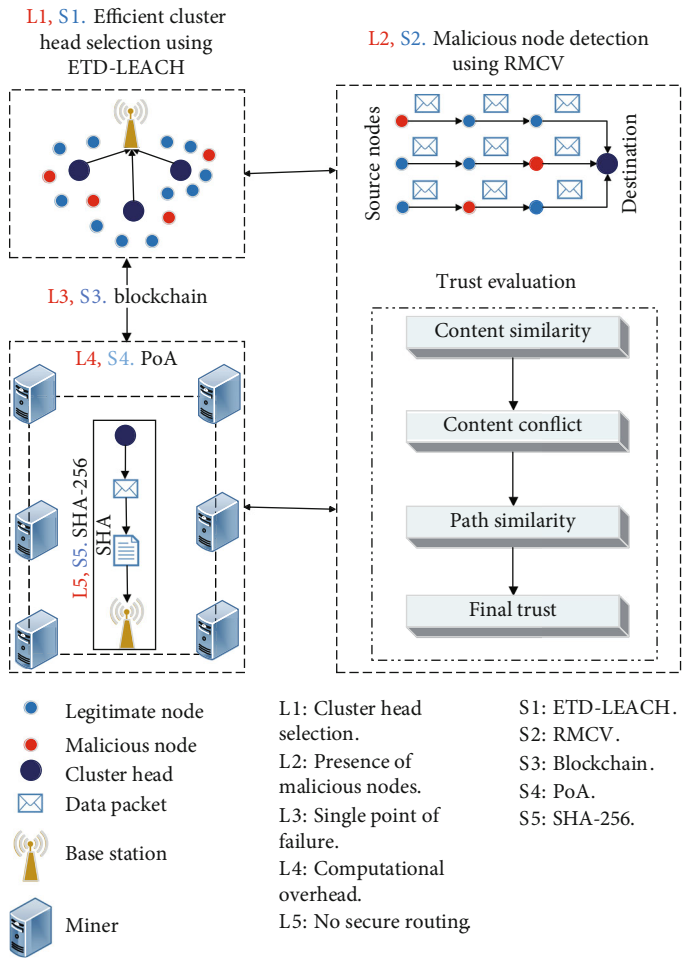

Figure 3: RMCV-based malicious nodes' detection in ETD-LEACH with blockchain in WSN.

transmitted. Therefore, Support$'(c)$ finds independent paths. The message tampering rate is low when the data packet is sent over independent paths. After calculation of trust of each message, we come to know that these nodes send less trustworthy data packets and are considered as malicious. For performing secure routing and successfully sending all the packets to the destination, malicious nodes are detected and revoked from the network [35].

The identified limitations are mapped with their proposed solutions and validations in Table 2. The first limitation (L1) is inefficient CHs' selection because CHs consume high energy and have minimum network lifetime. The limitation is solved through ETD-LEACH in which CHs are selected on the bases of energy, degree, and temperature. The selected CHs have less energy and high network lifetime. The second limitation (L2) is the presence of malicious nodes that is solved through the RMCV technique. Through this technique, 35% of malicious nodes are detected. Furthermore, in limitation three (L3), a single point of failure issue arises that is solved through decentralized blockchain. Limitation four (L4) is consuming high computational power while mining using the PoW

```
1: Deployment of nodes and BS
2: Degree of nodes
3: For i = 1 : nodes do
4:   For j = 1 : nodes do
5:     If i ≠ j then
6:       Find distance of the nodes
7:       If distance < = 20 then
8:         Add index of the nodes
9:       End if
10:    End if
11:  End for
12: End for
13: For i = 1 : nodes do
14:   For j = 1 : nodes do
15:     Check the nodes' neighbors
16:     If neighbor == 0 then
17:       A(i, j) = 0
18:     Else
19:       A(i, j) = 1
20:     End if
21:   End for
22: End for
23: For r = 1 : rounds do
24:   For i = 1 : n do
25:     If energy < = 0 then
26:       All nodes will die
27:     End if
28:     If dead == 1 then
29:       First node dies
30:     End if
31:     If dead == 0.5 ∗ nodes then
32:       Half nodes die
33:     End if
34:     If dead == nodes then
35:       Full nodes die
36:     End if
37:   End for
38:   For i = 1 : nodes do
39:     On the basis of nodes' degree, CHs are selected
40:     If current sensed value = temperature initial +
    (temperature initial + temperature final) ∗ rand (1, 1) then
41:       If sensed value > = hard threshold then
42:         Test = current value − sensed value
43:         If test > = soft threshold then
44:           Perform CHs' selection
45:           Send data packets
46:         End if
47:       End if
48:     End if
49:   End for
50:   Calculate content similarity of data packets using Equation (2)
51:   Calculate content conflict using Equation (3)
52:   Calculate path similarity using Equation (3)
53:   Calculate final trust using Equation (3)
54: End for
```

Algorithm 2: RMCV-ETD-LEACH protocol.

consensus mechanism. This issue is solved through the PoA consensus mechanism that consumes less computational power. Limitation five (L5) is that the XOR hashing function is not secure for hashing of routing data. In the proposed model, SHA-256 is used for securely hashing the routing data while storing it in the blockchain.

Table 2: Identified limitations' mapping with proposed solutions and validations.

Identified limitations	Proposed solutions	Performed validations
L1: inefficient CHs' selection	S1: ETD-LEACH	V1: dead nodes, delay, energy consumption, and throughput, as shown in Figures 4, 5, 6, and 7, respectively
L2: presence of malicious nodes	S2: RMCV	V2: PDR, number of alive nodes, and energy consumption, as shown in Figures 8, 9, and 10, respectively
L3: single point of failure	S3: blockchain	V3, V4: transaction cost shown in Figure 11
L4: PoW utilizes high computational power	S4: PoA	
L5: no secure routing using XOR	S5: SHA-256	V5: execution time shown in Figure 12

4. Simulation Results and Discussions

4.1. Simulation Parameters. In this section, we evaluated the performance of the proposed system model by implementing and comparing the routing protocols and schemes. The WSN consists of 100 nodes that are randomly deployed in an area of 100 m × 100 m, and each node has 1.5 J energy. The data packets are delivered to the destination through the source node. Here, it is to be noted that the data packet size is 4000 bits. The simulation parameters are provided in Table 3.

The routing protocols use 10,000 rounds. The ETD-LEACH is used for routing, and RMCV is used for the malicious nodes' detection during routing. The blockchain is deployed on BS and CHs. The SHA-256 is used in the blockchain for data hashing.

4.2. Comparison of ETD-LEACH and ETH-LEACH. The ETD-LEACH protocol is used for clustering and routing. The ETD-LEACH performance is better than that of ETH-LEACH because ETD-LEACH has high energy as compared to ETH-LEACH. In ETH-LEACH, CHs are selected on the basis of energy threshold, which is equal to 0.85 J, whereas, in ETD-LEACH, CHs are selected on the bases of high degree, energy, and temperature-sensing value. Moreover, in ETH-LEACH, the energy threshold is fixed. In ETD-LEACH, the node that has high energy is selected as a CH. This is the reason that in ETH-LEACH, nodes' energy dissipates early as compared to ETD-LEACH.

In Figure 4 and Table 4, it is seen that in ETD-LEACH, the first node dies at the 4000th round while all nodes die at the 9500th round, whereas, in ETH-LEACH, the first node dies at the 3000th round while all nodes die at the 7500th round. Therefore, network lifetime of ETD-LEACH is better than that of ETH-LEACH.

In Figure 5, it is seen that ETH-LEACH has less delay as compared to ETD-LEACH. The ETD-LEACH has high delay because of HT and ST. In ETD-LEACH, data is transmitted after meeting the thresholds due to which the delay occurs while sending data to the BS. In ETH-LEACH, data is frequently sent to the BS without meeting any thresholds; therefore, delay does not occur.

In the routing protocols, high energy is consumed when data is sensed and transmitted from nodes to CHs and CHs to BS. As shown in Figure 6 and Table 5, the ETD-LEACH consumes less energy as compared to ETH-LEACH because ETD-LEACH uses thresholds while transmitting the data.

Table 3: Simulation parameters.

Parameters	Value of parameters
Network interface	Wireless
Sensing area	100 × 100 m^2
Deployment	Random
Total nodes	100
Initial energy of nodes	1.5 J
Data packet size	4000 bps
Protocol	ETD-LEACH
Rounds	10,000
Malicious node detection	RMCV
Consensus	PoA
Hashing algorithm	SHA-256

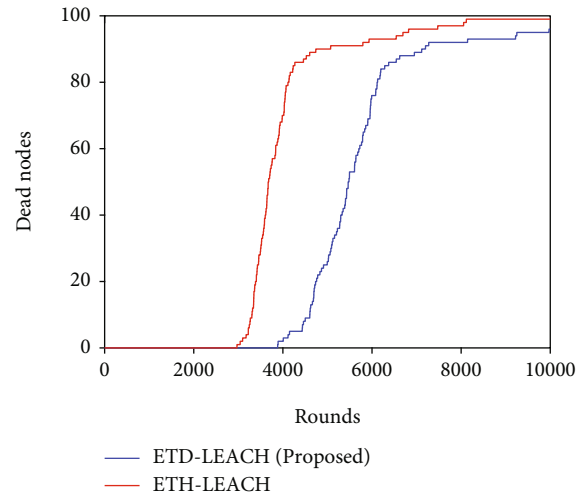

Figure 4: Comparison of dead nodes between ETD-LEACH and ETH-LEACH.

Table 4: Performance analysis of ETD-LEACH and ETH-LEACH.

Protocols	First node dies	Last node dies
ETD-LEACH	4000th round	9500th round
ETH-LEACH	3000th round	7500th round

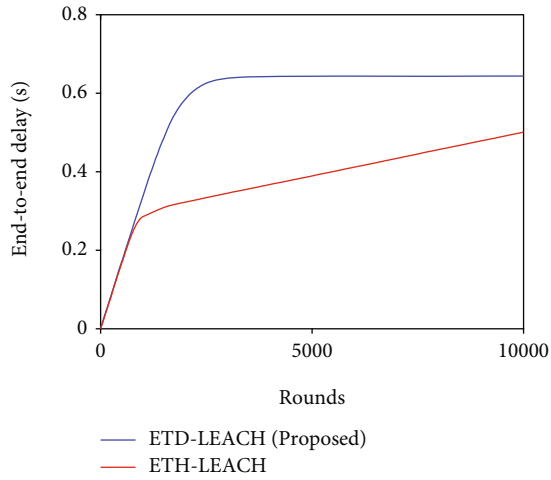

Figure 5: Comparison of delay between ETD-LEACH and ETH-LEACH.

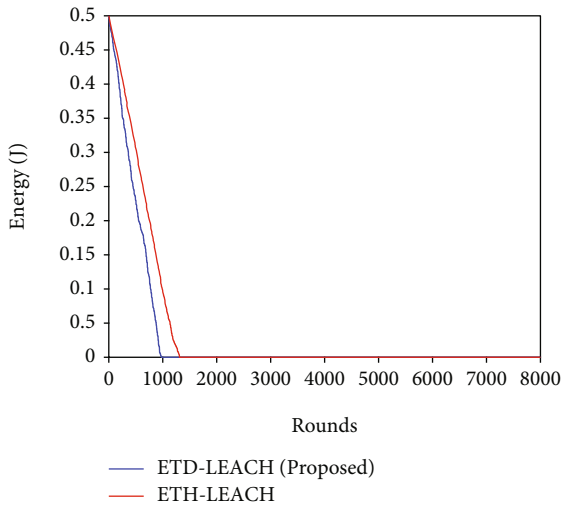

Figure 6: Comparison of energy between ETD-LEACH and ETH-LEACH.

Table 5: Performance analysis of energy consumption in ETD-LEACH and ETH-LEACH.

Protocols	Energy consumption
ETD-LEACH	0.1 J
ETH-LEACH	1.3 J

When sensed data meets the HT, then data is transmitted towards the CHs. In the next iteration, when new data is sensed, which is different from the saved sensed data and equal to or greater than ST, then it is transmitted, whereas, in ETH-LEACH, data packets are transmitted repeatedly. Therefore, nodes' energy dissipates early, and they die rapidly.

In Figure 7, it is shown that the data packets are sent from CHs to BS. In ETD-LEACH, fewer data packets are

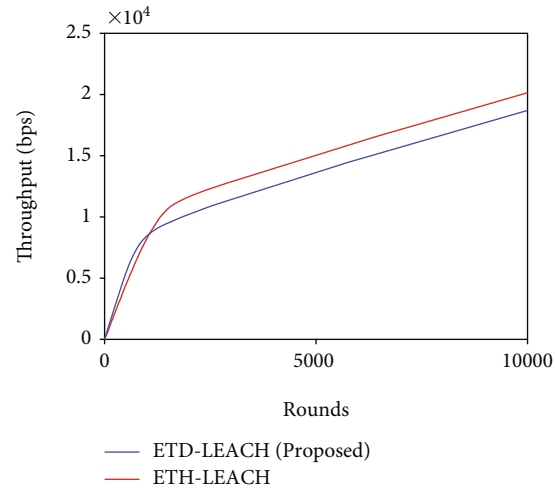

Figure 7: Comparison of throughput between ETD-LEACH and ETH-LEACH.

sent to the BS as compared to ETH-LEACH. The data packet sending rate is less in ETD-LEACH because only that data is sent to the BS, which meets the thresholds. In ETH-LEACH, there is no threshold to send the sensed data towards the BS; therefore, the throughput rate is high.

4.3. Malicious Nodes' Detection Using RMCV. Routing is performed by the ETD-LEACH protocol. We performed routing in which 89.9% of data packets are received at the destination while the remaining 10.1% of data packets are dropped that shows the presence of malicious nodes. These nodes are detected by the RMCV scheme. In this scheme, malicious nodes are detected by data packets' content. Moreover, the scheme checks the trust of each data packet and marks the packet as either honest or fake. Afterwards, nodes that send the fake data packets are detected. Based on the nature of data packets, 35% of malicious nodes are detected. After detection, routing is performed again. 99.9% of data packets are received while 0.1% of data packets are dropped, as shown in Figure 8 and Table 6.

The RMCV-ETD-LEACH performs better than ETD-LEACH because nodes remain alive for a long period in the absence of malicious nodes. As given in Figure 9 and Table 7, in RMCV-ETD-LEACH, the last node is alive till the 4800th round while in ETD-LEACH, the last node is alive till the 3900th round. In ETD-LEACH, nodes die early as compared to RMCV-ETD-LEACH because in ETD-LEACH, nodes act maliciously by sending wrong data packets. As a result, correct data packets are to be resent. Moreover, high energy is consumed while sending accurate data packets again.

In Figure 10 and Table 8, ETD-LEACH consumes high energy as compared to RMCV-ETD-LEACH because of corrupted data packets' delivery in ETD-LEACH. 31% of malicious nodes are present in the ETD-LEACH. These nodes are revoked from the network using RMCV-ETD-LEACH. It means that the number of nodes in RMCV-ETD-LEACH is less as compared to ETD-LEACH and that is why less energy is consumed.

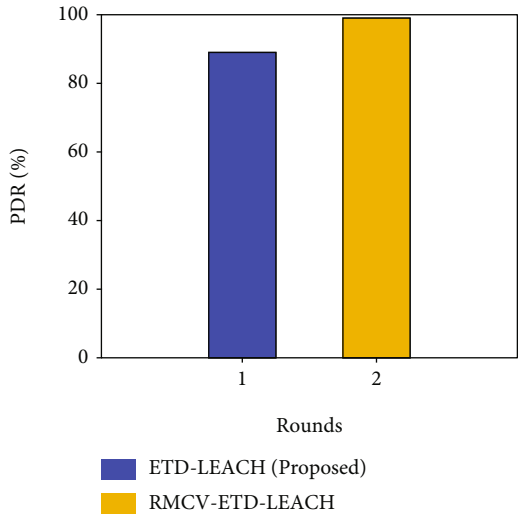

Figure 8: Comparison of PDR in ETD-LEACH and RMCV-ETD-LEACH.

Table 6: Performance analysis of PDR in ETD-LEACH and RMCV-ETD-LEACH.

Protocols	PDR
ETD-LEACH	89.9%
RMCV-ETD-LEACH	99.9%

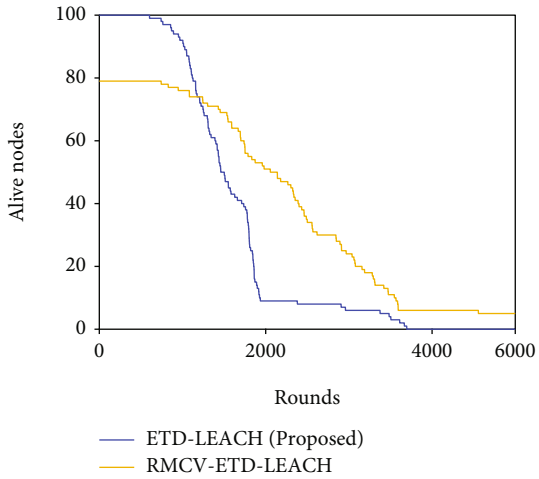

Figure 9: Comparison of number of alive nodes in ETD-LEACH and RMCV-ETD-LEACH.

Table 7: Performance analysis of alive nodes in ETD-LEACH and RMCV-ETD-LEACH.

Protocols	First node alive	Last node alive
ETD-LEACH	1000th round	3900th round
RMCV-ETD-LEACH	1100th round	4800th round

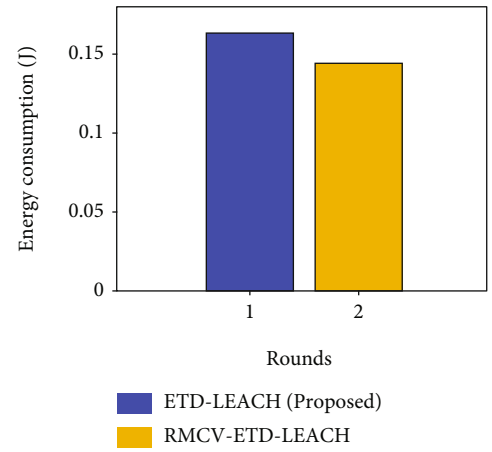

Figure 10: Comparison of energy consumption between ETD-LEACH and RMCV-ETD-LEACH.

Table 8: Performance analysis of energy consumption in ETD-LEACH and RMCV-ETD-LEACH.

Protocols	Energy consumption
ETD-LEACH	0.16 J
RMCV-ETD-LEACH	0.14 J

4.4. SHA-256 in Blockchain. The blockchain is implemented on CHs and BS. In the blockchain, the PoA consensus mechanism is used because its transaction cost is less than that of PoW. In the PoW, miners first solve a complex mathematical puzzle and then add a new block to the blockchain, which incurs a high transaction cost. In the PoA, preselected miners have the authority to add new blocks without solving a complex mathematical puzzle. Therefore, PoA outperforms PoW in terms of transaction cost, as shown in Figure 11.

The routing data is stored on BS and is encrypted by SHA-256. The data hashes are stored in the blockchain. The SHA-256 is used because it is more secure than SHA-1 and has less execution time than SHA-512. In the SHA-1, 164 bits are used for hashing the data. Therefore, it is less secure because 164 bits can be tampered easily and quickly. In the SHA-512, 512 bits are used for hashing, which makes it more secure than SHA-1 and SHA-256. However, execution time is maximum in it because of 512-bit hashing. Therefore, SHA-256 is used for hashing because it is more secure than SHA-1, and its execution time is less than that of SHA-512, as shown in Figure 12.

4.5. Formal Security Analysis. The security analysis is performed on the proposed ETD-LEACH protocol. The attacks discussed below are induced in our proposed model. Attacks are evaluated using different performance metrics: PDR, dead nodes, energy consumption, and delay.

The DoS and MITM attacks are induced in ETD-LEACH. In the DoS, malicious nodes send extensive unnecessary data packets towards the destination and create heavy

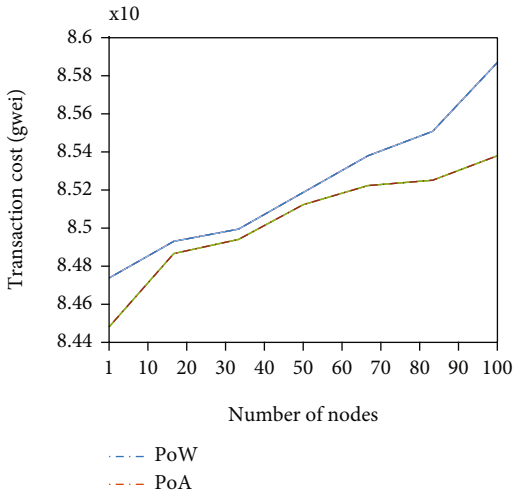

Figure 11: Comparison of transaction cost between PoA and PoW.

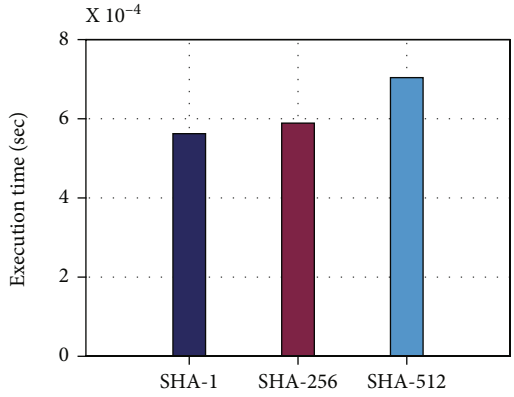

Figure 12: Comparison of execution time of SHA-1, SHA-256, and SHA-512.

traffic. Therefore, due to heavy traffic during routing, large bandwidth is occupied that minimizes the network performance. The fake data packets are received at the destination that are not required. Therefore, under DoS, 82% of legitimate data packets are received at destination, and the remaining 18% of data packets are considered malicious. In the MITM attack, malicious nodes become part of the network that eavesdrop and tamper the data packets. In this attack, tampered data packets are sent towards destinations. In the MITM attack, PDR is 79% because in this attack, tampered data packets are received at the destination. This attack has lower PDR as compared to DoS because this attack steals the victim node's IP address and also gateway IP address. Therefore, malicious nodes in the MITM attack easily get routing information and tamper the data packets without any limit. It is because malicious nodes get access to the data packets without the knowledge of the legitimate source and destination nodes. Furthermore, both attacks are prevented by the RMCV scheme that detects the malicious nodes present in the network. The scheme evaluates the trust of each data packet once the data packets are successfully received at the destination. Afterwards, malicious and legitimate data packets are detected and checked. Based on malicious and legitimate data packets, 35% of malicious nodes are detected. The RMCV scheme detects the malicious nodes because clusters are formed and the trust is calculated on the basis of trust of the malicious node. In the same way, malicious nodes are detected. The data required at destination is sent by maximum nodes; however, a minimum number of nodes send tampered data and they have low trust. Therefore, malicious nodes are detected through RMCV. After the malicious nodes' detection, PDR is increased to 99%, which shows that all legitimate data packets are received by the destination, as shown in Figure 13 and Table 9.

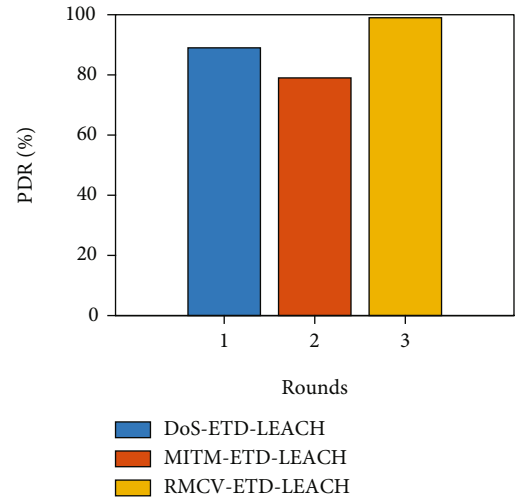

Figure 13: Comparison of PDR in DoS-ETD-LEACH, MITM-ETD-LEACH, and RMCV-ETD-LEACH.

Table 9: Performance analysis of ETD-LEACH under DoS and MITM attacks and RMCV scheme.

Protocols	PDR
DoS-ETD-LEACH	89.9%
MITM-ETD-LEACH	79.9%
RMCV-ETD-LEACH	99.9%

Figure 14 and Table 10 show that RMCV-ETD-LEACH has high network lifetime because all nodes are dead after 3900 rounds, and all such nodes that behave maliciously are removed from the network. Therefore, only legitimate nodes perform routing, and the network consumes low energy, whereas, in the presence of DoS and MITM attacks, all nodes are dead at the 2300th and 1400th rounds, respectively. In the DoS attack, malicious nodes send a large number of data packets towards the destination node that consume a large amount of resources. As a result, the energy is drained, and the nodes die early. Moreover, in the MITM attack, all nodes die early as compared to the DoS attack. In this attack, malicious nodes act as legitimate nodes, and legal nodes perform routing using malicious nodes as intermediary nodes. Upon receiving the data packets, the malicious

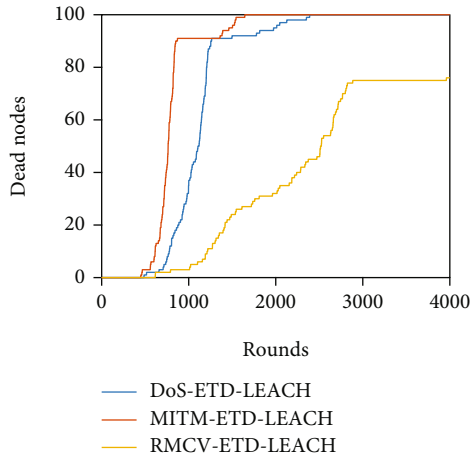

Figure 14: Comparison of dead nodes in DoS-ETD-LEACH, MITM-ETD-LEACH, and RMCV-ETD-LEACH.

Table 10: Performance analysis of ETD-LEACH under DoS and MITM attacks and RMCV scheme.

Protocols	First node dead	Last node dead
DoS-ETD-LEACH	500th round	2300th round
MITM-ETD-LEACH	400th round	1400th round
RMCV-ETD-LEACH	700th round	3900th round

nodes behave maliciously and corrupt the data packets before forwarding them to the destination. All the received data packets are tampered; therefore, destination nodes again send the request for the legitimate data packets. Consequently, nodes' energy depletes, and they die at the 1400th round.

The ETD-LEACH performance depends on the energy consumed by the nodes. As shown in Figure 15, the MITM attack consumes high energy as compared to the DoS attack and the proposed scheme RMCV-ETD-LEACH. The legitimate nodes perform routing for the sake of sending legitimate data packets. Furthermore, in the DoS attack, malicious nodes target a legitimate node and send heavy traffic that makes the legitimate node busy, and it does not receive legitimate data packets. After receiving a large number of malicious data packets, its energy is depleted. Moreover, in RMCV-ETD-LEACH, malicious nodes are not part of the network, and only the legitimate nodes are part of the network. They do not perform any malicious activity and consume less energy. Consequently, the RMCV-ETD-LEACH network performance is better than that of both DoS-ETD-LEACH and MITM-ETD-LEACH.

DoS-ETD-LEACH has high delay as compared to both MITM-ETD-LEACH and RMCV-ETD-LEACH, as shown in Figure 16. In the DoS attack, the destination node receives a large number of data packets resulting in high congestion. The legitimate data packets have to wait for routing that increases the delay. The MITM attack has less delay because the delay occurs only when the data packets are being tampered by the malicious nodes. These corrupted data packets are then sent to the destination node. Furthermore, in RMCV-ETD-LEACH, delay is the least, and it occurs only when checking the presence of malicious nodes in the routing path.

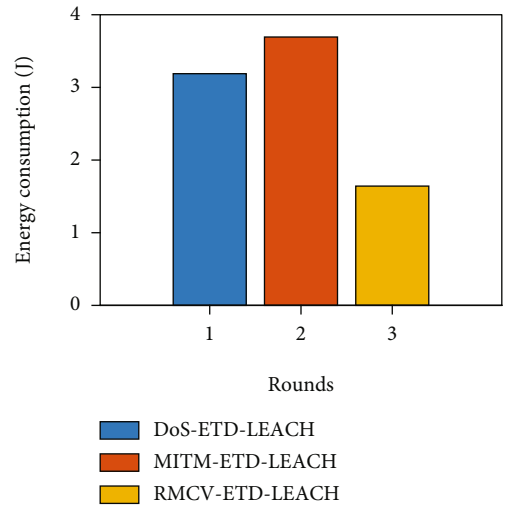

Figure 15: Comparison of energy consumption in DoS-ETD-LEACH, MITM-ETD-LEACH, and RMCV-ETD-LEACH.

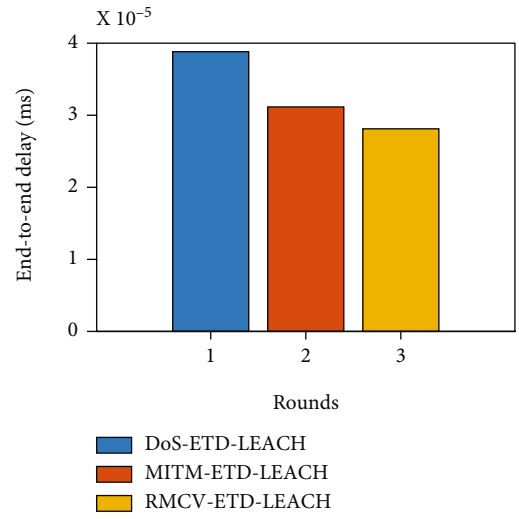

Figure 16: Comparison of end-to-end delay in DoS-ETD-LEACH, MITM-ETD-LEACH, and RMCV-ETD-LEACH.

(1) *Impersonation attack*: the registration of nodes at the blockchain secures the network against this attack. Moreover, it is ensured that malicious node cannot make a duplicate ID of a legitimate node

(2) *Spoofing attack*: the malicious node acts as a legitimate node using its ID. This attack is not possible because it is difficult to steal a legitimate ID from the blockchain

```
root@68c239632c96:/oyente/oyente# python oyente.py -s reg-storage.sol
WARNING:root:You are using evm version 1.8.2. The supported version is 1.7.3
WARNING:root:You are using solc version 0.4.21. The latest supported version
0.4.19
INFO:root:contract reg-storage.sol:reg-storage:
INFO:symExec:          ========== Results ==========
INFO:symExec:             EVM Code Coverage:                      99.5%
INFO:symExec:             Integer Underflow:                      False
INFO:symExec:             Integer Overflow:                       False
INFO:symExec:             Parity Multisig Bug 2:                  False
INFO:symExec:             Callstack Depth Attack Vulnerability:   False
INFO:symExec:             Transaction Ordering Dependence (TOD):  False
INFO:symExec:             Timestamp Dependency:                   False
INFO:symExec:             Re-Entrancy Vulnerability:              False
INFO:symExec:          ===== Analysis Completed =====
root@68c239632c96:/oyente/oyente# python
```

Figure 17: Security analysis using Oyente tool.

5. Smart Contract Analysis

The blockchain is used around the globe for data security. However, malicious entities perform attacks on the smart contract to make it vulnerable and to tamper the data. Therefore, the security analysis of the proposed smart contract through which CHs are registered and authorized, and routing data is stored, is performed. Furthermore, the registration of those CHs is canceled from the smart contracts that are detected as malicious by the RMCV scheme. The security analysis is performed through the Oyente tool that detects the attacks, which is possible on the smart contract, as shown in Figure 17. The attacks are discussed as follows [35].

5.1. Integer Underflow and Overflow. In the smart contract, the maximum size of the integer is 256 bits. The error arises when an attacker changes the integer value by subceeding and exceeding the lower and upper boundaries of the smart contract.

5.2. Parity Multisig Bug 2. Multiple fake accounts are created, and transactions are performed by an attacker in this attack. The smart contract stops working when multiple fake accounts are detected. From Figure 17, it is inferred that the proposed smart contract is not affected by this attack.

5.3. Callstack Depth Attack Vulnerability. The call function depth limit is taken to be 1023 frames. If the limit exceeds 1024 frames, the execution of new instructions fails. The attacker intentionally makes the frames to exceed, so the execution of new information fails. In the proposed smart contract, this attack is not possible because only authorized nodes call the functions.

5.4. Transaction Ordering Dependence. The functions involved in the smart contract consumes gas during execution. Malicious nodes manipulate the gas price to execute transactions maliciously. In this smart contract, this attack is not possible because there is no transaction-ordering function.

5.5. Timestamp Dependency. In this attack, the attacker changes the timestamp. When the mining time of the transaction is changed from a block, then the mining time of all transactions is changed. In our smart contract, this attack is not possible because there is no timestamp dependency function.

5.6. Reentrancy Vulnerability. The attacker calls the same function again and again that interrupts its execution. In the proposed smart contract, this attack is not possible because only authorized nodes are allowed to call the functions.

6. Conclusion

In this paper, we focus on efficient clustering using ETD-LEACH that consumes less energy and has better network lifetime. Moreover, blockchain is deployed on the WSNs for achieving security and SHA-256 is used for secure hashing. Furthermore, RMCV is used to find the trustworthiness of data packets. Based on the trustworthiness, malicious nodes are detected during routing. The efficiency of the proposed model is evaluated through simulations. The ETD-LEACH network lifetime is found to be better than that of ETH-LEACH. Moreover, in ETD-LEACH, energy consumption is less than ETH-LEACH. Moreover, the PoA transaction cost is less than that of PoW, and the SHA-256 execution time is less than that of SHA-512. The PDR is calculated to be 89.9% and 99.9% with and without the malicious nodes, respectively. Furthermore, the proposed model's resilience is tested by inducing DoS and MITM attacks and performing security analysis. Smart contract analysis is also performed using the Oyente tool, which shows the robustness of the proposed smart contract.

Data Availability

No dataset is used in this article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Z. Cui, X. U. E. Fei, S. Zhang et al., "A hybrid blockchain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[2] K. Latif, N. Javaid, I. Ullah, Z. Kaleem, Z. A. Malik, and L. D. Nguyen, "DIEER: delay-intolerant energy-efficient routing with sink mobility in underwater wireless sensor networks," *Sensors*, vol. 20, no. 12, p. 3467, 2020.

[3] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[4] Z. A. Khan, G. Latif, A. Sher et al., "Efficient routing for corona based underwater wireless sensor networks," *Computing*, vol. 101, no. 7, pp. 831–856, 2019.

[5] K. Haseeb, N. Islam, A. Almogren, and I. U. Din, "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things," *IEEE Access*, vol. 7, pp. 185496–185505, 2019.

[6] Z. Noshad, N. Javaid, T. Saba et al., "Fault detection in wireless sensor networks through the random forest classifier," *Sensors*, vol. 19, no. 7, p. 1568, 2019.

[7] M. P. Barua and M. S. Indora, "Overview of security threats in WSN," *International Journal of Computer Science and Mobile Computing*, vol. 2, pp. 422–426, 2013.

[8] N. Javaid, U. Shakeel, A. Ahmad et al., "DRADS: depth and reliability aware delay sensitive cooperative routing for underwater wireless sensor networks," *Wireless Networks*, vol. 25, no. 2, pp. 777–789, 2019.

[9] P. K. Chithaluru, M. S. Khan, M. Kumar, and T. Stephan, "ETH-LEACH: an energy enhanced threshold routing protocol for WSNs," *International Journal of Communication Systems*, vol. 34, no. 12, article e4881, 2021.

[10] A. Javaid, N. Javaid, Z. Wadud et al., "Machine learning algorithms and fault detection for improved belief function based decision fusion in wireless sensor networks," *Sensors*, vol. 19, no. 6, p. 1334, 2019.

[11] B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," *Sensors*, vol. 18, no. 11, p. 3894, 2018.

[12] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650–655, 2018.

[13] S. Tabatabaei, "A novel fault tolerance energy-aware clustering method via social spider optimization (SSO) and fuzzy logic and mobile sink in wireless sensor networks (WSNs)," *Computer Systems Science and Engineering*, vol. 35, no. 6, pp. 477–494, 2020.

[14] J. Yang, S. He, X. Yang, L. Chen, and J. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," *Sensors*, vol. 19, no. 4, p. 970, 2019.

[15] J. Wang, Y. Gao, C. Zhou, S. Sherratt, and L. Wang, "Optimal coverage multi-path scheduling scheme with multiple mobile sinks for WSNs," *Computers, Materials & Continua*, vol. 62, no. 2, pp. 695–711, 2020.

[16] J. Wang, H. Han, H. Li, S. He, P. K. Sharma, and L. Chen, "Multiple strategies differential privacy on sparse tensor factorization for network traffic analysis in 5G," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1939–1948, 2022.

[17] W. She, Q. Liu, Z. Tian, J. S. Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019.

[18] T. H. Kim, R. Goyat, M. K. Rai et al., "A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks," *IEEE Access*, vol. 7, pp. 184133–184144, 2019.

[19] 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, 14 pages, 2018.

[20] J. Wang, J. Chunwei, Y. Gao, A. K. Sangaiah, and G.-j. Kim, "A PSO based energy efficient coverage control algorithm for wireless sensor networks," *Computers, Materials & Continua*, vol. 56, no. 3, pp. 433–446, 2018.

[21] J. Wang, Y. Gao, X. Yin, F. Li, and H.-J. Kim, "An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2018, 9 pages, 2018.

[22] S. Hong, "P2P networking based internet of things (IoT) sensor node authentication by Blockchain," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 579–589, 2020.

[23] A. Rovira-Sugranes and A. Razi, "Optimizing the age of information for blockchain technology with applications to IoT sensors," *IEEE Communications Letters*, vol. 24, no. 1, pp. 183–187, 2020.

[24] M. Revanesh and V. Sridhar, "A trusted distributed routing scheme for wireless sensor networks using blockchain and meta-heuristics-based deep learning technique," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, pp. 42–59, 2021.

[25] L.-E. Wang, Y. Bai, Q. Jiang, V. C. M. Leung, W. Cai, and X. Li, "Beh-Raft-Chain: a behavior-based fast blockchain protocol for complex networks," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1154–1166, 2020.

[26] J. Wang, X. Qiu, and T. Yuanfei, "An improved MDS-MAP localization algorithm based on weighted clustering and heuristic merging for anisotropic wireless networks with energy holes," *Computers, Materials & Continua*, vol. 60, no. 1, pp. 227–244, 2019.

[27] N. Shi, L. Tan, C. Yang et al., "BacS: a blockchain-based access control scheme in distributed internet of things," *Peer-to-peer networking and applications*, vol. 14, no. 5, pp. 2585–2599, 2021.

[28] S. Hameed, S. A. Shah, Q. S. Saeed et al., "A scalable key and trust management solution for IoT sensors using SDN and blockchain technology," *IEEE Sensors Journal*, vol. 21, no. 6, pp. 8716–8733, 2021.

[29] R. Goyat, G. Kumar, M. Alazab et al., "A secure localization scheme based on trust assessment for WSNs using blockchain technology," *Future Generation Computer Systems*, vol. 125, pp. 221–231, 2021.

[30] P. Kumar, G. P. Gupta, and R. Tripathi, "TP2SF: a trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning," *Journal of Systems Architecture*, vol. 115, pp. 101954–101954, 2021.

[31] D. Liao, H. Li, W. Wang, X. Wang, M. Zhang, and X. Chen, "Achieving IoT data security based blockchain," *Peer-to-Peer Networking and Applications*, vol. 14, no. 5, pp. 2694–2707, 2021.

[32] A. Mubarakali, "An efficient authentication scheme using blockchain technology for wireless sensor networks," *Wireless Personal Communications*, pp. 1–15, 2021.

[33] T. Samant, P. Mukherjee, A. Mukherjee, and A. Datta, "TEEN–V: a solution for intra-cluster cooperative communication in wireless sensor network," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 209–213, IEEE, 2017.

[34] A. Almasri and K. A. Darabkh, "A comparative analysis for WSNs clustering algorithms," in *2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 263–269, IEEE, 2020.

[35] M. B. E. Sajid, S. Ullah, N. Javaid, I. Ullah, A. M. Qamar, and F. Zaman, "Exploiting machine learning to detect malicious nodes in intelligent sensor-based systems using blockchain," *Wireless Communications and Mobile Computing*, vol. 2022, 16 pages, 2022.