International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209698 Volume 8, Issue 4, July – August (2021)

RESEARCH ARTICLE

Real Time Two Hop Neighbour Strategic Secure Routing with Attribute Specific Blockchain Encryption Scheme for Improved Security in Wireless Sensor Networks

M. Hema Kumar
Department of Biomedical Engineering, Mahendra Institute of Technology, Namakkal, Tamil Nadu, India.
hemakumarmohan@gmail.com

V. Mohanraj
Department of Information Technology, Sona College of Technology, Salem, Tamil Nadu, India
vmohanraj06@gmail.com

Y. Suresh
Department of Information Technology, Sona College of Technology, Salem, Tamil Nadu, India
ysuresh33@gmail.com

J. Senthilkumar
Department of Information Technology, Sona College of Technology, Salem, Tamil Nadu, India
Jsenthil10@gmail.com

G. Nagalalli
Department of Electronics and Communication Engineering, Sona College of Technology, Salem, Tamil Nadu, India
nagalalli87@gmail.com

Received: 04 June 2021 / Revised: 11 July 2021 / Accepted: 22 July 2021 / Published: 28 August 2021

Abstract – Wireless Sensor Network (WSN) is most vulnerable to routing attacks which affects the confidentiality and integrity services of the data transmitted between any nodes. Many research efforts have been taken to propose secure routing schemes for improving the data security against routing attacks in WSN. The existing secure routing schemes are not able to dynamically discover the trust path between nodes for ensuring secure transmission without compromising confidentiality and integrity service. To address this issue, a real-time, two-hop neighbour, strategically secure routing scheme is proposed in this paper. According to the strategy of two-hop neighbours, the method selects the forwarding node according to the trust measures computed based on trust energy support and trust forwarding support of the two hop nodes. Further, the data security is enforced at the attribute level. The Blockchain mechanism is enforced where a single block contains information of specific attribute of data which restrict the user who have access to the attribute only can read the data present in the block. The data encryption is performed according to different encryption standards maintained by the system, unique for different attributes. According to the Hash code present in the Blockchain, the user can decode the key and scheme to obtain the original data. The proposed approach improves the performance in secure routing and increases the data security performance.

Index Terms – WSN, Data Security, Secure Routing, Two Hop Neighbour Strategy, Blockchain, QoS.

1. INTRODUCTION

The growth of information technology has supported the communication between any two devices or persons or systems in a sophisticated manner. However, the data transmission between any two entities is only feasible through the support of networks. The availability of sensor nodes is helpful in collecting the real time data or occurrence of event around of it. Further, sensor nodes are grouped to form a WSN by following a different form of clustering strategy [1]. All these clustering method improves the life time of network and ensure reliable data delivery. WSN is the keen network being used in various locations and situations. In the modern informatics world, wireless sensor nodes are playing a major role in collecting the data or occurrence of event around it. With advancement in WSN, sensor nodes that are located in different geographical region can still transmit the data to base station for the purpose of monitoring or making a decision. The data communications between different nodes are performed using a wireless protocol where each sensor node comes to the limited energy, supporting the limited number of data transmissions.

The restriction on transmission range due to the limited transmission range of sensor nodes encourages the cooperative transmission to deliver the data packets to the destination. Like any other network, the WSN also faces security challenges [2]. The presence of a malicious node in the network introduces several threats to the data communication. Such malicious nodes can read the incoming data and be involved in eavesdrop attacks, modification attacks, and DDoS attacks. So it is necessary to identify the presence of such malicious nodes. There are several ways available to identify such malicious nodes. However, it is much better to perform data transmission through trusted nodes and secure routes.

Secure routing is the process of routing the data packets through a trusted or secure route. Any route can be named a trusted route only if the data transmission performed through the route has been delivered without delay, modification and drop. Even if the malicious node reads the data and forwards it without modification, the malicious node would learn the entire data and perform a DDoS attack or some other one. There are many approaches available to identify the genuine nodes of any route. Some of the methods use energy parameters; some use the frequency of transmission, and so on. However, they do not provide higher results in secure routing to support the QoS [3] of WSN.

Some methods measure the trust of the node according to their energy and transmission. But considering the energy and transmission itself is not enough in deciding the trust of any intermediate nodes. Instead, the trust of a node is locally measured by collecting two-hop neighbour data that would support malicious node detection in two hops. Once there is a second hop that is malicious, then the entire route through the hop is avoided. Otherwise, the second level transmission would suffer from poor security. This article plays over this result and selects a route and measures the route's trust according to the two-hop neighbour strategy. On the other side, data security is enforced by adapting the Attribute-Based Blockchain (ABC) data encryption approach. By encrypting the data with different schemes and keys and applying the Blockchain [4] technique, the security of data in WSN is improved.

According to the problems identified, the objective of research is to design an efficient, secure routing scheme that must consider different parameters like the number of transmissions, frequency of retransmission, successful transmission. Route selection should be done partially to improve safety performance. The trust value of any node must be measured based on any number of parameters. The selection of routes should be performed by considering at least two-hop neighbour information to estimate the trusted value to avoid the insecure route selection. The data encryption schemes and techniques should be performed by the class of information. The data should be classified under different sensitive level. The method should use different schemes and keys for various data attributes, which improves the security performance. The selection of scheme and key in each case should be performed dynamically. The method should improve the security performance and throughput performance. The time complexity of data encryption and decryption should be reduced.

The paper is organized as follows: Section 1 presents a detailed introduction on WSN and data security in WSN with secure routing. Section 2 details the review on various methods of secure routing and data security. Section 3 presents detailed information on proposed real-time two-step neighbour strategic secure routing with ABC. Section 4 presents the evaluation results and discussion. Section 5 presents the conclusion of the proposed scheme in detail.

2. RELATED WORKS

Different approaches on secure routing in WSN are available, and data security is enforced with different approaches. This section reviews the methods of data security and routing in detail in follows.

(Sung-Jin Choi et al., 2013), the key-based pre-distribution method can read the data exchange in the group and does not compromise the other party's existence. This method produces Eigen values based on a square matrix of eigenvectors. The square matrix values are used to select the key, and the encryption is performed accordingly. This method challenged the opponent due to significant time complexity but was affected [6]. (Pu Gong et al., 2015) consideration for the development of gift security Energy types and the name ETARP trust-based routing algorithm. The design of this method requires data security and utility theory in the field of professional warfare used in routing [7]. The main limitation of the work is the computation sensitive key generation algorithm.

(Dan Li and Xian bin Wen, et al., 2015) presented 2 Phase Particle Swarm Optimization (PSO) to the decentralization of the issue of ambiguity on the flip. This algorithm uses a bounding box to find the initial solution used to improve the PSO algorithm [8]. The drawback of the work is that it chooses a local optimum as a best solution in high dimensional space.

(Ziwen Sun et al., 2015) working with a multi-target approach towards secure routing to discussed a PSO-based localization approach. MOPSOLA employs multi-purpose features constrained by spatial distance and geometric topology. The PSO algorithm is used to select the best solution [9]. The drawback is the computational complexity involved in it when applied to solve high dimensional space.

(Yong jun Ren et al., 2018) to adopting Blockchain technology to secure the execution of data stored in wireless sensor networks. Data rewards and magnitudes of rewards are stored, and digitized coins are stored in nodes of WSN that based on volume of saved information. Two different Blockchain have been created and maintained for storage and access control. Proof of Data Certificate (PDS) is the alternative method to proof of work (POW) [10]. The main limitation of the work is computation complexity involved in generating proof of Data certificate.

(Gholamreza Ramezan et al., 2018) Discusses routing issues in wireless sensor networks applies to Blockchain technology. The author recommends routing assurance, contract routing and Blockchain when dealing with IoT devices with a focus on efficient networks. This method centralizes the authority to manage the identities of different sensors and allows communication through a variety of devices [11].

(Ana Reyna et al., 2018) presented different issues related to Internet of Things (IOT) terminals and summarized the survey of WSN integrated Blockchain algorithm [12]. (Jiangdian Yang et al., 2018) Learn techniques to improve security and route the use of enhanced Blockchain technology to discuss its WSN. This method can track routing data, which cannot be tampered with by the other party [13].

(B. Christian et al. 2017) discuss the nature of using Bit coin with Bit coin to control user control protocols for accessing secure communications from adversaries [14]. (R. Hashi et al., 2018) There is a detailed review of P2P network communication methods and destinations for IoT devices available to use the pestle Blockchain. The strengths and weaknesses of the Internet of Things integration are well discussed.

(Yongjun Ren et al. , 2018) support to reduce the computing power of the troops PDS in Bitcoin to exchange prisoners for data storage [16]. (Francisco Prieto-Castrio, 2017) Perform numerical simulations and theoretical analysis of areas that interfere with the network, monitor Blockchain based on threat events and discuss probabilistic models [17].

(Wei She et al., 2019) presented Blockchain trust model, the support is called WSN or BTM for malicious node detection. At first, the trust model is disseminated to every node and configured for detecting Blockchain. To perform the inspection, the 3D spatial model uses a voting mechanism [18].

(Komal Shinde et al. , 2019) presents data security based on inconsistent encryption techniques using signatures or checksums in data packets without redundant encoding [19].

(Jawaid Iqba et al., 2019) the signature encryption discussion is introduced to support secure sensor node connection. [20]. It is suitable for offline and online modes. There is no knowledge of any of the patient data in offline mode, not in online mode, and at least the operation works best with existing patient data.

(Qi Liu et al., 2019) discuss the impact and challenges of research departments from different organizations and industries to take a Blockchain [21]. (Casado - Vara R et al., 2019) discussion is based on Blockchain, and control malicious access methods. This model employs a non-linear control scheme suitable for collaborative properties to maintain safety [22].

(Abdul Mateen et al., 2019) which helps detect malicious nodes, is based on an immutable trust model which is built based on version of Proof of Stack. Nodes are added to the chain are done by POA (Proof of Authority) [23]. (Chen Y et al. , 2018) proposed for data collected using the Blockchain distributed network at WSN [24].

(Moinet, Axel et al. 2017) discussed a Blockchain based data security protocol that limits malicious access until the end of data integrity is preserved [25]. (Volker Skwarek et al., 2017) discussed a Blockchain based framework for achieving reliable data transmission in the IoT and wireless sensor networks [26].

(F. Zawaideh et al., 2017) presented the Fair Trust Mechanism for Detecting Malicious nodes detection method (FTMNDI). Nodes can be isolated based on the weight of their neighbours and detect malicious nodes [27]. (L. G. Zeng et al., 2018) measured user trust based on node behaviour based on previous communication content and discussed data security and WSN trust models [28].

(Y. X. Su et al., 2018) it is recommended to maintain the structure of the trust model based on the method of trust data fusion. The calculation of the confidence value is based created rules set. The work computes the confidence in their methods, data and historical differences. The computed value is used to measure the total trust of any node [29].

(V. R. Prabha et al. , 2017) has introduced attribute's success rate based model, and we argued that the exact needs for applying fuzzy technique is to measure the behavioural trust value in fuzzy logic[30].

(W. Zhang et al. 2018) discussed the proposed methods based on Dempster–Shafer evidence theory is to find the existence of malicious nodes. This technique correlates with measuring confidence values representing data collected from any node in an adjacent spatiotemporal region. Based on this, to measure the behaviour, a trust model is created. [31].

(K. Christidis, M. Devetsikiotis, et al. , 2016) discuss of digital content distribution system based on Blockchain. Decentralization and the pear-to-pear authentication mechanism can be regarded as an ideal authority management mechanism [32]. Blockchain has the potential to realize this ideal content distribution system. (J. Ellul et al. 2018) described the virtual machine Alkyl VM that facilitates the interaction of IoT devices with the Blockchain system [33].

(E. S. Kang et al. 2018) proposed a trading platform to renew energy according to the contract obtained from the use of energy [34]. (J. Kishigami et al. 2015) based on Blockchain, we examined the content distribution method of the work. Research has identified a variety of problems, and these methods do not provide the required performance [35].

From the literature survey, it is observed that the existing methods are still vulnerable to routing attack due to non-establishment of trusted routing path between nodes. Many of the existing methods are statically discovering the trusted routing path and use it for transmission. Over the time, nodes in statically discovered trusted path might act as a malicious node and facilitates the routing attack. Hence, there is a need for secure routing scheme which discovers the trusted path dynamically and ignores the participation of malicious node in the data transmission. Also, the proposed method should ensure fair time complexity involved in finding the trusted path and ensure tamper proof system. In this paper, Two Hop Neighbour Strategic Secure Routing with Attribute Specific Blockchain Encryption Scheme is proposed to address the problem.

3. TWO HOP NEIGHBOUR STRATEGIC SECURE ROUTING WITH ATTRIBUTE SPECIFIC BLOCKCHAIN ENCRYPTION SCHEME

The proposed two-hop neighbour strategic secure routing algorithm works based on the network statistics being maintained by various sensor nodes. Each sensor node maintains a set of information regarding the neighbours of the sensor and their neighbours. The details are maintained in the two-hop level, where for each sensor node, there is much information maintained. According to route discovery, the method collects such information, and the Two Hop Data Forwarding Support (THDFS) measure is computed. Similarly, the data security is enforced according to the Blockchain approach, where the method is enforced at the attribute level. The detailed approach is presented in detail in this section.

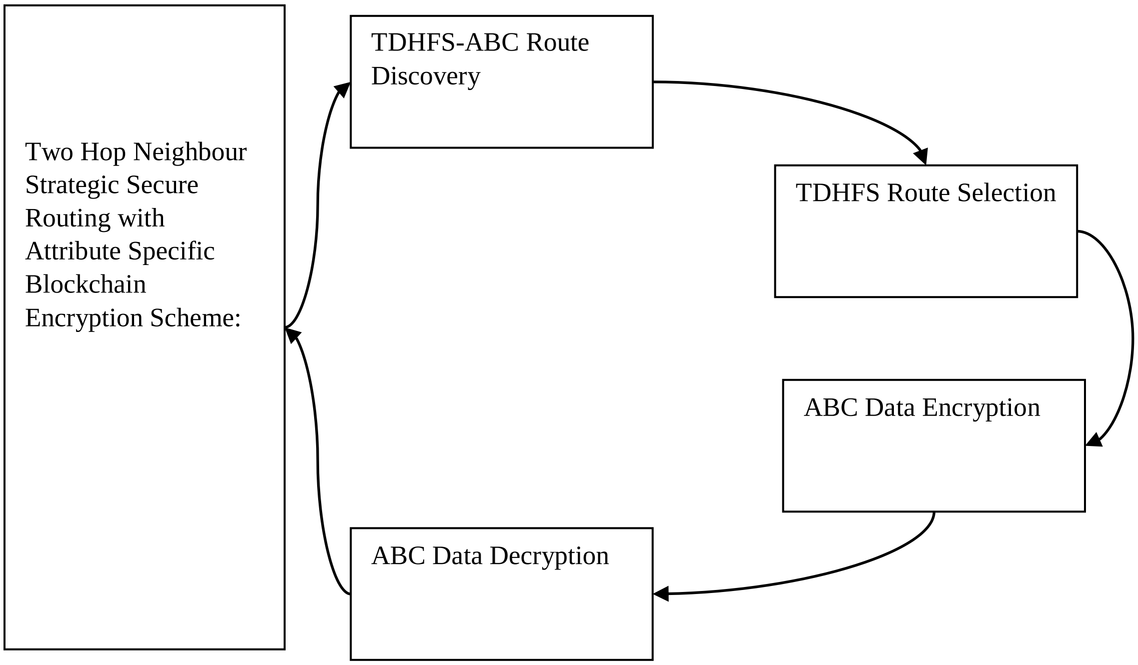
Two Hop Neighbour Strategic Secure Routing with Attribute Specific Blockchain Encryption Scheme:
TDHFS-ABC Route Discovery
TDHFS Route Selection
ABC Data Encryption
ABC Data Decryption

Figure 1 Architecture of Proposed Two Hop Neighbour Strategic Secure Routing with ABC

Feature Proposal Real-time two-hop neighbour strategy structure of security attributes and block-chain cryptography is described in this section. Routing based on the detailed description of the functional components shown in Figure 1.

3.1. TDHFS-ABC Route Discovery

It is necessary to discover the routes between the source and destination to perform routing. It is performed by using the TDHFS-ABC route discovery procedure. As the sensor nodes have abounded transmission range, it has been initiated by generating a broadcast message TDHFS-RREQ that is broadcast to the neighbours, which broadcast to their neighbours when it has no route to reach the destination. When a node identifies a route to reach the destination, then it generates a route reply message TDHFS-RREP towards the source node from where the request has been generated. While generating TDHFS-RREP, the node appends different information related to its neighbours and its own.

The process of appending is performed at the two-hop level. Consider the node X has a route to reach D through a node Y, then it generates the TDHFS-RREP, which has information related to X and Y. It attaches the information like, number of transmissions performed by X and Y. Also, the energy constraints of X and Y are added to the reply. Similarly, numbers of information are added to the reply packet towards the source node. Identified routes are updated to the routing table, used to perform route selection in data forwarding.

3.2. TDHFS Route Selection

The route selection plays an important role in the proposed model, which considers various parameters in identifying a secure route. The TDHFS route discovery procedure generates the routing table. For each route, R_i identified, the method collects two-hop details from the routing table. It estimates Trustable Energy Support (TES) according to the energy of node, current energy, number of transmissions performed. Similarly, Trustable Forwarding Support (TFS) according to the number of transmission and number of transmission among them. This method computes the TDHFS measure. According to the value of TDHFS, using which the route selection is performed.

Consider the route R, which has a K number of intermediate nodes. Then the method estimates the TDHFS value according to the properties and strategies of the K intermediate nodes. More than that, the trust measures are computed according to the strategies of the first two hops. First, the energy support should be considered, as each sensor has only limited energy, the sensor node can perform only a limited number of transmissions.

Only the adversary or malicious nodes comes with higher energy, and by analyzing the energy and the number of transmissions involved, the trustworthiness of the sensor is measured. So, the method first estimates the TES measure for both first and second hop nodes using the Equation in1,2,3, and 4.

Number of transmission of first-hop NTF = $\sum \mathrm{Transmissions} \in \mathrm{R.FirstHop}$ (1)

Number of transmissions of second hop NTS = $\sum \mathrm{Transmissions} \in \mathrm{R.SecondHop}$ (2)

Number of transmissions of entire route NTR = $\sum \mathrm{Transmissions} \in \mathrm{R}$ (3)

Consider, each sensor has J joules of energy which support N number of transmission. According to this, the method computes the TES measure as follows:

$$\mathrm{TES} = \frac{J}{NTF} \times \frac{J}{NTS} \times \frac{\sum_{i=1}^{size(R)} R(i).InitialEnergy}{NTR} \quad (4)$$

Similarly, the Trustable Forwarding Support (TFS) is measured using the Equation 5

$$\mathrm{TFS}= \frac{\sum ReTransmissionwithFirstHOp}{TotalTransmissionwithFirstHOp} \times \frac{\sum ReTransmissionwithSecondHop}{TotalTransmissionwithSecondHop} \times \frac{\sum RetransmissionwithR}{TotalTransmissionwithR} \quad (5)$$

Using these two measures, the method computes TDHFS measures using the Equation 6

$$\mathrm{TDHFS = TES{\times}TFS\text{-}} \quad (6)$$

Depending on the value of TDHFS, a single route is chosen to perform the data transfer.

```
Input: Route Table RT
Output: Route R
Start
   Read RT
   For each route R
       Compute the number of transmission by first-hop using equation (1)
       Compute the number of transmission by second hop using equation (2)
       Compute the number of transmission through the route R using equation (3)
       Compute Trustable Energy Support TES using equation (4)
       Compute Trustable Forwarding support TFS using equation (5)
       Compute TDHFS using equation (6)
End
```

Algorithm 1 TDHFS Route Selection

The Algorithm 1 explains how to perform routing. The method computes the number of transmissions performed by first, second hop and the route considered. This method computes the Trustable energy support (TES), Trustable Forwarding Support (TFS) to compute the value of TDHFS for the route using these features. According to the value of TDHFS, a single route has been selected to perform data forwarding.

3.3. Attribute-Based Blockchain Encryption

The data security in WSN is enforced by adapting attribute-based Blockchain encryption. The method generates a number of blocks with the chain according to the number of attributes the data point contains. For Every block, the scheme generates a Hash code used to detect the decryption key at the receiver side. First, the method generates a random number for each attribute within the bound of the size of the key set. Similarly, the method generates another random number to indicate the scheme from the scheme set. This method performs data encryption using these two methods. The method estimates the difference between the indexes of both of them to generate the Hash code. Generated Hash Code has been added to the block, and there is a reference to the next block generated for each block. Generated Blockchain has been given to the destination, which has been used to perform data decryption.

Consider a scheme set Scs, which contains K number of schemes and key set Ks, which contains P number of keys. A random number R1 is generated for the scheme according to the size of Scs, and a random number R2 is generated to select a key according to the size of Ks for different attributes. According to this, the data has been encrypted using the key and scheme selected. The hash code is generated as follows:

Consider the size of the keyset is P and size of scheme set is K, and the index of scheme selected is S and key selected is R, then the hash code is generated using the Equation 7

Hash Code HC = Ks(S)+Diff((R,P),S) (7)

If the value of P is 10, K is 7, S is 3, and R is 4, then the hash code generated is as follows:

Consider the key set Ks is {x, w, u, r, a, k, p, y, m, c}

Hash Code HC = r+ ((4, 10), 3) =r3

Generated Hash code has been added to the block generated and transmitted to the destination where the data has been decrypted by identifying the scheme and key set.

```
Input: Keyset Ks, Scheme set Scs, Data
Output: Blockchain Bc
Start
        Read data, ks, scs.
        Initialize Blockchain with the size of data BC = $\sum_{i=1}^{size(Data)}$ Initialize Block -- (8)
        For each block B
                        $size(Data)$
            Key k = $Random(1, size(Ks))$        (9)
                        $i = 1$
                        $size(Data)$
            Scheme s = $Random(1, size(Scs))$        (10)
                        $i = 1$
            Block data = Encryption (S,k)
            Hash Code Hc = Generate hash code using equation (7)
            Add data, hash code to the block B.
            Add B to BC.
        End
Stop
```

Algorithm 2 ABC Encryption

The Algorithm 2 explains how the data is encrypted and appended to the chain of blocks. The method generates a scheme and key for each attribute, and according to that, the method performs data encryption.

3.4. Attribute - Based Blockchain Decryption

The data received by the destination node performs attribute-based Blockchain decryption. The data present in each block of the chain has been read and decrypted according to the details of the Hash code present in each block. Each of the blocks, the scheme extracts the hash code, and from the hash code, the method identifies the index of scheme and key to perform data decryption. Let, hash code from block b is r3, then the method split the characters as key k to produce key=r, and the index of the scheme as 3, which denotes the index of the scheme. Using these two, the method performs data decryption to get the original data.

```
Input: Blockchain Bc, key set Ks, scheme set Scs
Output: Data D
Start
        Read Bc, ks, scs.
        For each block b
            Hash code Hc = HashCode$\in b$
            Key k = Split (Hc, characters)
            Scheme index Si = Numeric values in Hc.
            Scheme s = Diff (Ks (index (k)), size (ks))
            Data D = Perform data decryption using key and scheme.
End
```

Algorithm 3 ABC Data Decryption

The Algorithm 3 explains how the data decryption is performed. The hash code is extracted to identify the scheme and key from the block. This method performs data decryption to produce the result using the key and schemes identified.

4. RESULTS AND DISCUSSION

The proposed real-time two-hop neighbouring strategic secure routing with ABC data encryption has been implemented using advanced java. This method has evaluated the performance of using different numbers of users in different situations. In consideration of each test case, the method has been evaluated for its performance under different parameters and compared with BTM, POW, POA and TLRCBC. The results obtained are presented in this section.

Parameter	Value
Number of Nodes	200
Number of Attributes	100
Tool Used	Advanced Java
Running time	10 minutes
Data transmission	100 meters
Energy	50 Joules

Table 1 Details of Simulation

The parameter considered is the performance evaluation of the proposed method. The methods listed in Table 1 have been measured and introduced in this section as their performance at various parameters and proposed.

The performance in security introduced by different methods has been measured for various algorithms such as BTM, PoW, PoA, and TLRCBC. In Blockchain Trust Model (BTM), each node will be given a trust score by its neighbouring nodes. In Proof of WORK (PoW), each node compete with each other by performing mathematical operations in order to generate a random number and get the accounting right. To seize control of the blockchain, malicious need more than 51% of the network's computational power in network. The resource usage of the consensus mechanism is lower than that of other consensus mechanisms. The cost of a PoW blockchain is expensive, and the supervision is ineffective. All of these things are happening at the same moment. In Proof of Authority, an approved node (called a validator) validates the transaction and the block in a PoA Blockchain. A mining process's massive computational overhead Validation must be done on the validator's behalf. Because the Blockchain and qualification are difficult to obtain, the malicious validator will not be able to participate in pursuing their own goals.

Trust Aware Localized Routing and Class-Based Dynamic Block Chain Encryption Scheme (TLRCBC) is a trusted-aware localized routing scheme based on class-based dynamic blockchain encryption scheme that supports data security in wireless sensor networks. Towards routing security, a set of routes are identified where at each route, the hops are measured for their trust value. The approach classifies the data under different data security classes, where each has a dedicated signature with different encryption schemes.

The result produced by the methods is measured and plotted in Table 2. The performance evaluation is performed at different conditions by varying the number of nodes in the simulation. The proposed TDHFS-ABC scheme has produced higher security performance than other methods are BTM, POW and POA.

	50 Nodes	100 Nodes	200 Nodes
BTM	72	61	52
PoW	79	71	62
PoA	84	73	68
TLRCBC	95	91	87
TDHFS-ABC	99	96	92

Table 2 Comparison of security Performance

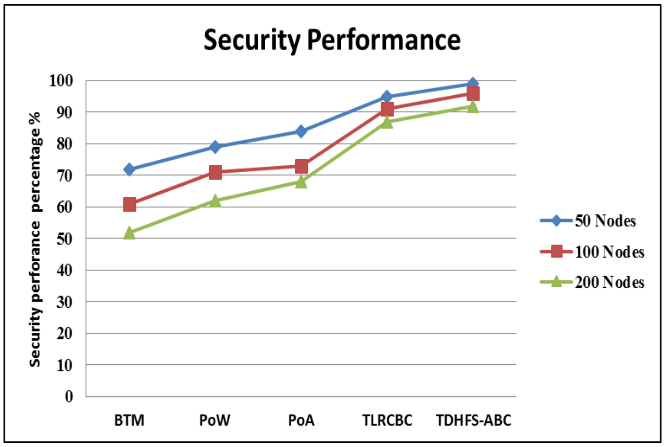

Figure 2 Security Performance Analysis of Various Consensus Mechanisms with TDHFS-ABC

The proposed model outperforms other methods by eliminating the participation of malicious node in the data transmission. The proposed model dynamically discovers the trusted path based on the trust value which is computed based Trust Energy Support and Trust Forwarding Support. The existing methods are discovering the trusted path statically where some of the nodes in the path might become a malicious node over the time. Since the proposed method periodically updates the trust path, the participation of malicious node is completely eliminated. Due to the dynamic discovery of trusted path by the proposed work, the network is least vulnerable to routing attacks and outperforms other methods in security performance, throughput, computational complexity, and packet delivery ratio.

Performance methods with different security performance are measured by changing the number of nodes in the network. Under each condition, the results produced by various methods were measured and compared. The TDHFS-ABC method proposed in Figure 2 produces higher safety performance than other methods.

Throughput Performance Analysis			
	50 Nodes	100 Nodes	200 Nodes
BTM	76	71	64
PoW	79	74	69
PoA	83	78	74
TLRCBC	95	91	87
TDHFS-ABC	98	94	92

Table 3 Comparison of Throughput Analysis

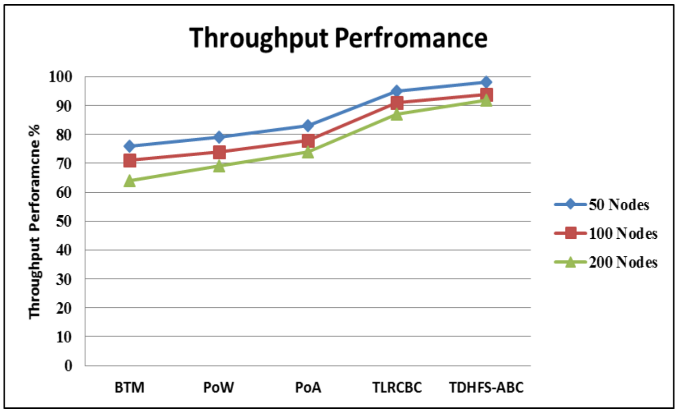

Figure 3 Performance Analysis of Throughput

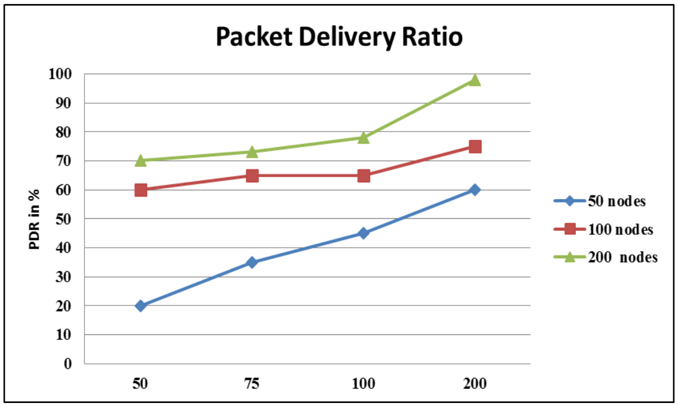

Figure 4 Performance Analysis of Packet Delivery Ratio

The throughput performance introduced by different methods has been measured and presented in Table 3. At each condition considered, the proposed TDHFS-ABC algorithm has produced higher throughput performance than other methods. The comparison of throughput performance is shown in Figure 3.

In this throughput analysis is taken different number of 50, 100 and 200 nodes in the network. In each of the states considered, the proposed TDHFS-ABC algorithm produces higher performance throughput than the other methods.

Packet delivery Ratio Analysis			
	50 Nodes	100 Nodes	200 Nodes
BTM	20	35	60
PoW	60	65	75
PoA	70	73	78
TLRCBC	95	91	87
TDHFS-ABC	98	94	92

Table 4 Comparison of Packet Delivery Ratio Analysis

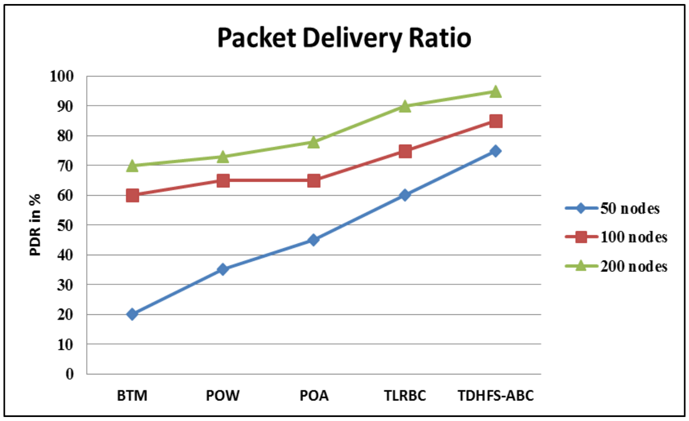

Figure 4 Performance Analysis of Packet Delivery Ratio

The performance analysis of packet delivery ration is taken by different methods which have been presented in Table 4.Packet delivery ration analysis is measured by changing the number of nodes in the network. Under each condition, the results produced by various methods were measured and compared. As shown in Figure 4, the proposed TDHFS-ABC produces higher performance than other methods.

Data encryption and decryption performance is measured in Table 5 and the analysis is taken different number of nodes. The proposed TDHFS-ABC algorithm produced better data encryption and decryption performance than the other methods.

	50 Nodes	100 Nodes	200 Nodes
BTM	65	61	58
PoW	69	65	61
PoA	73	69	65
TLRCBC	95	92	89
TDHFS-ABC	98	96	93

Table 5 Performance Analysis of Data Encryption/Decryption

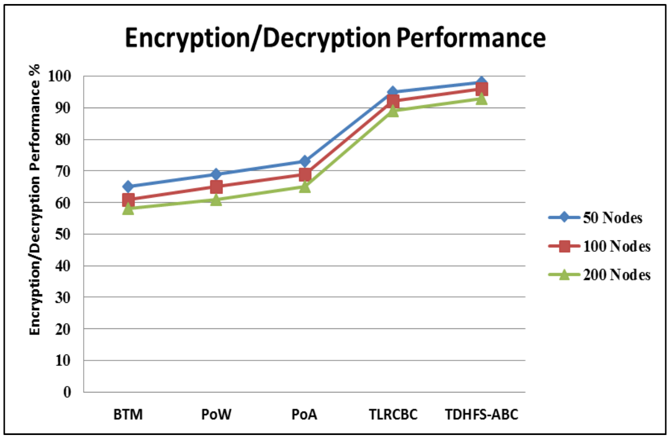

Figure 5 Performance Analysis of Encryption and Decryption

The percentage of crypto security efficiency is measured by many methods, and Figure 5 shows the effectiveness of TLRCBC and notifications that high performance can be achieved under all conditions. The performance estimate different number of nodes in the network. This performance analysis of the proposed TDHFS-ABC algorithm produced better data encryption and decryption performance than the other methods.

Time Complexity			
	50 Nodes	100 Nodes	200 Nodes
BTM	87	92	97
PoW	75	84	91
PoA	71	78	85
TLRCBC	31	36	43
TDHFS-ABC	19	26	32

Table 6 Performance on Time Complexity

The result analysis time complexity is taken by different methods in data encryption decryption has been measured and presented in Table 6. The proposed method performance taken different number of nodes and the TDHFS-ABC algorithm provide less time complexity compared to other existing method.

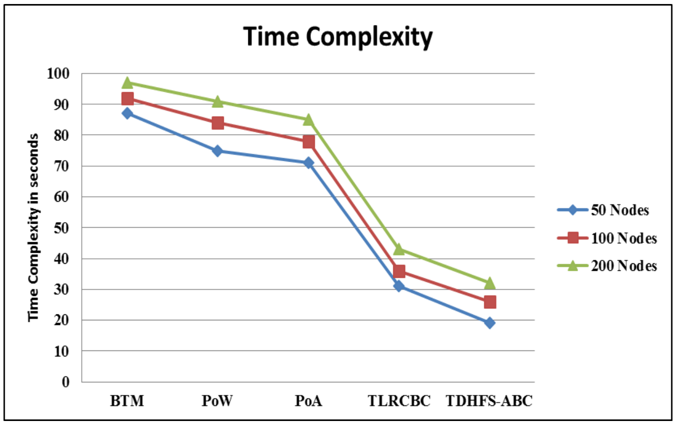

Figure 6 Comparison of Time Complexity

The time complexity shown in Figure 6 is obtained by monitoring different scenarios under different conditions. It has been found that TDHFS-ABC can do business faster than others.

5. CONCLUSION

This paper presented a novel real time two-hop neighbour strategic secure routing with an attribute-based Blockchain encryption scheme towards QoS development in WSN. The method first discovers the routes available by broadcasting the route request message. By collecting the route, the information like energy, several data transmission performed is collected. Using that information, the method computes the Trustable Energy support (TES), Trustable forwarding support (TFS) to measure the value of TDHFS for each route. According to the value of TDHFS, a single route has been selected to perform data transmission.

Similarly, the method generates a Blockchain where the data is added. Each attribute of data has been added to a block in the chain where the data has been encrypted by choosing a random key and scheme according to the ABC algorithm. The hash codes are generated and updated with each block used to find the scheme and key to perform data decryption. The method introduces higher performance in all the parameters considered than other methods.

REFERENCES

[1] Kalla N., Parwekar P. (2018) “A Study of Clustering Techniques for Wireless Sensor Networks”. In: Satapathy S., Bhateja V. , Das S. (eds) Smart Computing and Informatics. Smart Innovation, Systems and Technologies, vol 77. Springer, Singapore. https://doi. org/10. 1007/978-981-10-5544-7_46

[2] J. Grover and S. Sharma, "Security issues in Wireless Sensor Network — A review," 2016 5th International Conference on Reliability,

Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2016, pp. 397-404,

[3] S. B. Takale and S. D. Lokhande, "Quality of Service Requirement in Wireless Sensor Networks: A Survey," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2018, pp. 34-38,

[4] Xu, M., Chen, X. & Kou, G. “A systematic review of blockchain”. FinancInnov 5, 27 (2019).

[5] Pournaghi, S. M. , et al. Med SBA: “A novel and secure scheme to share medical data based on Blockchain technology and attribute-based encryption”. J Ambient Intell Human Computing (2020).

[6] Sung-Jin Choi, et al. "An energy-efficient key pre-distribution scheme for wireless sensor networks using eigenvector”, College of Information and Communication Engineering, Sungkyunk wan University, Vol 1, pp. 440-746, 2013

[7] Pu Gong, et al. ETARP: “An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks”, Journal of Sensors, Vol 2015, pp. 1-5.

[8] Dan Li and Xian bin Wen, "An Improved PSO Algorithm for Distributed Localization in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Vol, pp. 1-8, 2015.

[9] Ziwen Sun, et al. "Localization Algorithm in Wireless Sensor Networks Based on Multi objective Particle Swarm Optimization", Vol. 2015, pp. 1-9.

[10] Yongjun Ren. , Yepeng Liu. , Sai Ji. , Arun Kumar Sangaiah. , &Jin Wang “Incentive mechanism of data storage based on blockchain for wireless sensor networks”. Mobile Information Systems, PP. 1–11, 2018.

[11] Gholam reza Ramezan & Cyril Leung “A Blockchain-based contractual routing protocol for the Internet of things using smart contracts”. Wireless Communications and Mobile Computing, 1–15, 2018.

[12] Reyna, A., Martin, C. , Chen, J. , Soler, E. , &Díaz, M. (2018). “On blockchain and its integration with IoT. Challenges and opportunities”. Future Generation Computer Systems, 88, 173–190, 2018.

[13] Jidian Yang. , Shiwen He. , Yang Xu. , Linweiya Chen. , &Ju Ren. , “A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. Sensors”, 19, 1–19, 2019.

[14] Christian, B., Ueli Maurer. , Daniel Ts chudi. , & Vassilis Zikas. , (August 2017). “Bitcoin as a transaction ledger: A composable treatment”. In Proceedings of the 36th Annual International Cryptology Conference—Advances in Cryptology (CRYPTO 2017) (pp. 324–356). Santa Barbara, CA, 2017.

[15] Qiao, R. “Blockchain-based secure storage scheme of dynamic data”. Computer Science, 45, 57–62, 2018.

[16] Yongjun Ren. “Incentive mechanism of data storage based on blockchain for wireless sensor networks”, HINDAWI (MIS), 2018.

[17] Prieto - Castrillo, F. “Distributed sequential consensus in networks: Analysis of partially connected blockchains with uncertainty”, HINDAWI (COMPLXITY), 2017.

[18] She, W. “Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks”, Research Gate (In ieee access), 2019.

[19] Komal Shinde, “Securing Wireless Sensor Network against Pollution attack with BlockChain”. (IJMTST), 05(06), 2019.

[20] JawaidIqba, “Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on Blockchain”, (IJDSN). Volume, 15(9),2019.

[21] Liu, Q. “Research on trust mechanism of cooperation innovation with big data processing based on Blockchain”. Springer Link (WCN),2019.

[22] Casado - Vara, R. “Blockchain-based distributed cooperative control algorithm for WSN monitoring”, (AISC), 2019.

[23] Mateen, A. “One step Forward: Towards A Blockchain-based Trust Model for WSNs”, Research gate (3PGCIC),2019.

[24] Chen, Y. “Blockchain-based collocation storage architecture for data security process platform of WSN”, IEEE (CSCWD), 2018.

[25] Moinet, A. Benoit Darties. , & Jean-Luc Baril. , “Blockchain-based trust and authentication for decentralized sensor networks”, (Ar. Xiv), (2017).

[26] Skwarek, V. “Blockchains as security-enabler for industrial IoT applications”. Asia Pacific Journal of Innovation and Entrepreneurship, 11(3), 301–311. Doi: 10. 1108/APJIE-12-2017-035, 2017.

[27] Zawaideh, F. Muhammed Salamah. , & Hussein Al-Bahadili. , (December 2017). “A fair trust-based malicious node detection and isolation scheme for WSNs”. Proceedings of the 2nd IT-DREPS (pp. 1–6), 2017.

[28] Zeng, L. G. , (2018). “Detecting WSN node misbehaviour based on the trust mechanism”. Journal of Zhejiang Normal University (Natural Sciences), 41(1), 39–43, 2018.

[29] Su, Y. X., “Credibility based WSN trust model. Electronics Optics and Control”, 25(3), 32–36, 2018.

[30] Ram Prabha, V. R. , &Latha, P. (2017). “Fuzzy trust protocol for malicious node detection in wireless sensor networks”. Wireless Personal Communications, 94(4), 2549–2559., 2017.

[31] Zhang, W., Zhu, S. , Tang, J. , &Xiong, N. (2018). “A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks”. Journal of Supercomputing, 74(4), 1779–1801.

[32] Christidis, K., & Devet sikiotis, M. (2016). “Blockchains and smart contracts for the Internet of Things”. IEEE Access, 4, 2292–2303.

[33] Ellul, J., & Pace, G. J. (February 2018). Alky IVM: “A virtual machine for smart contract blockchain connected Internet of Things”. Proceedings of the 9th NTMS (pp. 1–4), 2018.

[34] Kang, E. S., Seung Jae Pe. , Jae Geun Song. , & Ju Wook Jang. , (April 2018). “A blockchain-based energy trading platform for smart homes in a micro grid”. Proceedings of the 3rd ICCCS (pp. 472–476), 2018

[35] Kishigami, J., Shigeru Fujimura. , Hiroki Watanabe. , & Atsushi Nakadaira (August 2015). “The blockchain-based digital content distribution system”. Proceedings of the IEEE 5th International Conference Big Data Cloud Computability (pp. 187–190), 2015.

Authors

M. Hema Kumar obtained his BE in Electronics and Communication Engineering from Anna University in 2006, ME in Communication Systems from Anna University in 2012 and Currently he is pursuing Ph. D. degree in Information and Communication Engineering from Anna University, Chennai. At present he is working as an Assistant Professor in the department of Biomedical Engineering at Mahendra Institute of Technology, Namakkal, affiliated to Anna University, Chennai. His teaching and research areas include Wireless sensor networks, Mobile computing, Cloud Computing and Security. He has published more than 5 publications in various national, International conferences and journals. He has acted as reviewer for International Conference on Transformations in Engineering Education by IUCEE-Indo Universal Collaboration for Engineering Education. He received Best Project Award in District level Category for the contribution of project in International Society for Scientific Research and Development.

V. Mohan Raj obtained his BE in Computer Science and Engineering from Madras University in 1999, ME in Computer Science and Engineering from Anna University, Chennai in 2004 and PhD in Information and Communication Engineering from the Anna University, Chennai in 2013. He has 20 years of teaching experience. Currently, he is working as Professor in the Department of Information Technology at Sona College of Technology, Salem, India. He had published more than 25 research papers in international journals. Currently, he is guiding 12 PhD scholars under Anna University, Chennai. His teaching and research areas include web mining, wireless sensor networks, analytics, security and cloud computing. He has acted as reviewer for Inderscience -International Journal Computational

Science and Engineering, International, Journal of Big Data Intelligence, Elsevier – Swarm and Evolutionary Computation and many of the international conferences sponsored by IEEE.

Y. Suresh obtained his BE in Electrical and Electronics Engineering from Madras University in 1998, ME in Applied Electronics with distinction from Anna University, Chennai in 2004and PhD in the Faculty of Information and Communication Engineering from Anna University, Chennai in 2012. He has 22 years of teaching experience. Currently he is working as a Professor in the Department of Information Technology at Sona College of Technology, Salem. He had published more than 30 research papers in international journals and IEEE international conferences. He has been appointed as doctoral committee member for many PhD scholars. He has received the NPTEL topper award for the online certification course introduction to cryptology and elite category in internetwork Security. His research interest includes computer networks, wireless sensor networks, Image processing, and neural networks.

J. Senthilkumar obtained his BE in Computer Science and Engineering from Bharathiyar University in 2000, ME in Computer Science and Engineering from Anna University, Chennai in 2004 and PhD in Information and Communication Engineering from the Anna University, Chennai in 2013. He has 19 years of teaching experience. Currently, he is working as Professor in the Department of Information Technology at Sona College of Technology, Salem, India. He had published more than 30 research papers in international journals. Currently, he is guiding 12 PhD scholars under Anna University, Chennai. His teaching and research areas include wireless technology, wireless sensor networks, analytics, security and cloud computing. He has acted as reviewer for Elsevier – Applied Soft computing, Swarm and Evolutionary Computation and many of the international conferences sponsored by IEEE.

G Nagalalli obtained his BE in Electronics and Communication Engineering from Anna University in 2008, ME in Communication Systems from Anna University in 2012 and Currently she is pursuing Ph. D. degree in Information and Communication Engineering from Anna University, Chennai. Her research areas are Wireless Networks, Wireless Sensor Networks, Machine Learning, IOT and Computer Networks. He has published more than 5 publications in various national, International conferences and Journals.

How to cite this article:

M. Hema Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, G. Nagalalli, "Real Time Two Hop Neighbour Strategic Secure Routing with Attribute Specific Blockchain Encryption Scheme for Improved Security in Wireless Sensor Networks", International Journal of Computer Networks and Applications (IJCNA), 8(4), PP: 300-310, 2021, DOI: 10.22247/ijcna/2021/209698.