SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V10I3P107

Volume 10 Issue 3, 59-66, March 2023
© 2023 Seventh Sense Research Group®

Original Article

A HIBE using Blockchain for Hierarchical Key Management Approach in Wireless Sensor Networks

Siddiq Iqbal[1], B. R. Sujatha[2]

[1]*Department of Electronics & Telecommunication, BMS Institute of Technology and Management, Bengaluru.*
[2]*Department of Electronics & Communication, Malnad College of Engineering, Hassan.*

[1]*Corresponding Author : siddiq@bmsit.in*

Received: 18 January 2023 Revised: 03 March 2023 Accepted: 15 March 2023 Published: 29 March 2023

Abstract *- This paper proposes a solution to enhance the key management of Wireless Sensor Networks (WSNs) by integrating blockchain technology with Hierarchical Identity-Based Encryption. The aim is to establish a highly secure WSN structure. The current wireless network is improved by incorporating blockchain technology to increase security and reliability. However, the security of key management in dynamic WSNs is threatened by the vulnerability of untrusted Head Nodes(HN) to attack. The presence of an untrusted HN imposes a heavy burden on the sensors for key management, in addition to the already existing challenges. In order to overcome these issues, blockchain technology has been used to propose a secure key management scheme (BSKM). We offer a secure node movement technique and a safe cluster-building mechanism, with the blockchain acting as a trust machine to replace the major functions of the Head node. We run extensive simulations for security analyses. The findings show that the BSKM scheme is efficient and effective and is more suitable for enhancing the reliability of dynamic WSNs.*

Keywords *- Blockchain, Hierarchical Identity-Based Encryption, Key management.*

1. Introduction

A wireless sensor network (WSN) consists of devices with sensors, processors, and wireless communication capabilities, known as nodes. The nodes work together to collect, process, and transmit data about environmental conditions like temperature, light, or sound. WSNs are used in a wide range of applications, including industrial monitoring and control, environmental monitoring, and health care. The key features of a WSN include low-power operation, scalability, and the ability to operate in harsh or remote environments [1]. Based on the mobility of nodes, there are static and dynamic networks. Static WSN is frequently utilized in applications with fixed and unchanging node locations, such as industrial process control or environmental monitoring. Dynamic WSN is commonly used in applications where the node locations change, such as wildlife monitoring, military operations, or disaster response. In this, the nodes must be able to accommodate alterations in the network structure or network partitions. In a Hierarchical Wireless Sensor Network (WSN), the network is divided into smaller sub-networks with specific tasks, making it easier to manage and scale. The hierarchy can be organized according to geography, network design, or the application's demands [2].

In a Heterogeneous Wireless Sensor Network (WSN), the nodes have varying responsibilities and abilities depending on their function within the network. This kind of network is frequently used in applications where some nodes require more capabilities than others, such as those in which certain nodes must act as gateways or cluster heads. Encryption keys play a crucial role in maintaining the security and reliability of communications within a wireless sensor network (WSN). They protect sensitive data from unauthorized access or interception by encrypting the information being transmitted between nodes. Using strong and valid encryption keys is also vital for maintaining the reliability of network communication. A compromised or poorly managed encryption key can severely impact the security and reliability of the network. Therefore, it is necessary to implement secure key management protocols to ensure that only authorized nodes have access to the encryption keys and are regularly updated to preserve the network's security [3].

Symmetric cryptography is a method of encryption where the same key is utilized for both encrypting and decrypting messages in a wireless sensor network (WSN). In this process, both sender and receiver of the message must have access to a shared secret key, which they use for encryption and decryption. Maintaining the secrecy of the key is crucial, as any attacker who obtains it can use it to decrypt messages and access sensitive information. Symmetric cryptography is favoured in WSNs due to its efficiency and simplicity since the same key is used for encryption and decryption. However, the security of this method depends on the safekeeping of the shared key, hence the need for secure key management techniques to maintain its confidentiality [4, 5].

Public-key cryptography, also known as asymmetric cryptography, uses a pair of public and private keys to encrypt and decrypt data. In wireless sensor networks, asymmetric cryptography is employed for secure communication between nodes, preventing unauthorized access and tampering, and establishing trust among nodes[6, 7]. This makes it suitable for WSNs where nodes need secure communication without a pre-existing secret key [4, 8]. However, asymmetric cryptography demands more computational resources compared to symmetric cryptography and might not be appropriate for WSN nodes with limited resources[9]. A Cluster head network functionality is simulated using blockchain technology [30].

Blockchain is a decentralized and distributed ledger technology that can provide several benefits, including:

1. Security: Security is ensured by using cryptography and consensus algorithms, making it near impossible for data to be tampered with or erased, providing a robust shield for transactions and information stored on the blockchain [11].
2. Transparency: It enables the establishment of a clear and open record of transactions, enabling all participants to see the transaction history, ensuring the information kept in the blockchain is precise and up-to-date
3. Decentralization: It operates on a decentralized network, meaning no central authority controls it. This leads to lower costs, increased efficiency, and greater stability.
4. Immutability: The information recorded cannot be altered or removed, ensuring a secure and unalterable record of all transactions.
5. Traceability: The transparency of transactions makes it well-suited for industries and applications where tracking and accountability are crucial, such as in supply chain management.
6. Improved trust: The implementation enhances participant trust by creating a secure and open record of transactions.
7. Automation: Blockchain-based smart contracts can streamline processes by eliminating the need for intermediaries, increasing efficiency and reducing the potential for fraud.

Hierarchical Identity-Based Encryption (HIBE) has certain drawbacks. The remote head node plays a significant role in key management. The technique does not specifically outline the solution when the cluster key is generated for the case where a simple sensor member node is hacked and fabricates a message indicating that a cluster head is not valid to the Head node. Forward secrecy cannot always be guaranteed by HIBE [12]. It is more difficult to scale, as the hierarchical structure of keys can make it more difficult to add new users or groups[13, 14]. Key revocation is complex, as it may require revoking keys at multiple levels of the hierarchy. Accordingly, we provide a secure key management scheme which is based on the blockchain (BSKM) that satisfies the trustworthiness (i.e., security and dependability) in order to optimise the security level and also to alleviate the vulnerabilities caused by over-dependence on the HN. This paper proposes a Blockchain-based Secure Key management (BSKM) for dynamic Wireless Sensor Networks. The main contributions in the article are; first, we investigate the secure key management problem based on the blockchain using a distributed approach. Second, we put forth the BSKM for WSNs, which makes decisions between nodes using the blockchain and consists of the node registration, cluster creation, node exit and join processes. Finally, we examine the BSKM's security to see how well it defends against different assaults to stop a network crash or data leak. The system's effectiveness is then assessed in terms of energy usage, memory storage occupied and reliability.

The structuring of the paper is as follows; Several similar works are presented in the II sections. In the third section, we suggest attack and network models for the BSKM and discuss choosing a consensus mechanism. The BSKM is the suggestion in the fourth. We examine the BSKM's security in the fifth section. Reports on the BSKM's performance evaluation can be found in the sixth section. The article is concluded in the last seventh section.

2. Related Works

In[28], a key distribution method for wireless sensor networks that utilize the HIBE has been introduced. This approach conserves storage and reduces the computational demands at each node. The HIBE only requires three instances of exponential modular computation, resulting in a significant reduction in storage space. In [12], the authors have presented a key management strategy that uses robust high-end sensor nodes in heterogeneous networks. According to performance evaluation and security analysis, the scheme offers superior security with reduced complexity and a sizable reduction in storage requirements. There is an approach called asymmetric pre-distribution (AP) for heterogeneous sensor networks. Simple, effective, and efficient key setup techniques are provided for M-sensors using powerful C-sensors. It is appropriate to assume that powerful C-sensors are supplied with tamper-proof hardware, even though it is too expensive for M-sensors [16]. In [17], an attack-resistant key establishment process is part of a resource-efficient security approach comprising authentication across devices on different networks and between devices. In [17], The efficient group key management scheme proposed provides a revocation system is proposed that identifies and revokes misbehaving nodes as a powerful security measure. To guard against threats to users' privacy, a safe and simple authentication strategy for heterogeneous sensor networks has been implemented employing smart cards and dynamic identities [18, 19]. In [29], a Tree-based key management scheme has been discussed, where the head of the group serves as the responsible node.

3. Proposed Methodology

3.1. Network Initialization

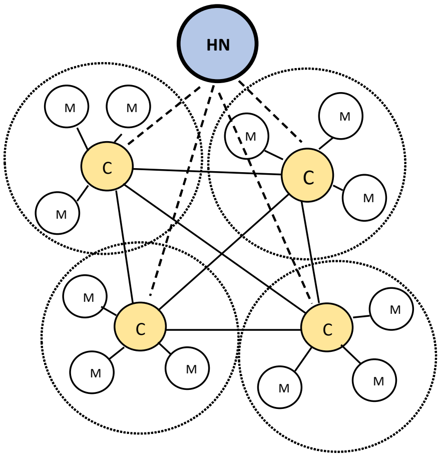

Fig. 1 Node deployment in WSN

The following outlines the steps for initializing the wireless sensor network. The network has a root node with limited capabilities, which necessitates the need for initiation. During initialization, information is distributed among the nodes. During network setup, a Head Node (HN) broadcasts properties, such as the public parameters of HIBE(Hierarchical Identity-Based Encryption), to all nodes. After the properties have been transmitted, the Head node is no longer necessary.

Based on computing power and resources, nodes are classified as Cluster head nodes (C) and mini nodes (M). The network model is shown in figure.1. Cluster head nodes have high computing power, storage space and complex hardware necessary. Mini nodes have low computing power, storage space and basic hardware necessary. Suppose N is the total number of nodes, which includes X cluster heads and Y mini nodes. The network will have fewer cluster head nodes compared to mini nodes, such that X<<Y. In a blockchain network, C-sensors serve as consensus nodes. As a result of their performances, M-sensors are merely regular nodes and will not take part in any aspect of the consensus. It is important to note that the Head node, a centralised machine, will not participate in the consensus, allowing C-sensors to create a decentralised system and removing the need for the HN for key management. The HN's sole responsibility is to provide each node with a distinctive identification. Every node in the WSNs receives a set of certificateless public/private key pairs from the key generation centre (KGC) held by the Head node. In our network architecture, a cluster key is shared by the member nodes in a cluster. The certificateless public-private key creates a pairwise key mutually shared among any two neighbouring nodes.

3.2. Attack Model and the Security Requirements

We assume that the attacks are carried out after the network has been deployed and that the system does not initially include any compromised sensor nodes. By taking control of a node and collecting the private cryptographic settings, an attacker might launch an external assault. The following security requirements have been proposed.

- Forward Secrecy- A node cannot participate in communication if it has logged out or been removed. Furthermore, it is unable to send legitimate encrypted packets and retrieve session information.
- Backward Secrecy- This occurs when a new sensor node that has not yet joined the network cannot decrypt the session communication.
- Resistance to node imitation attacks- The scheme must provide a node mechanism to identify the malicious node.

3.3. Blockchain Functions

Blockchain is a dependable distributed record that safeguards anonymity and is ideal for P2P networks [21]. The consensus technique that may address the issue of excessive resource consumption is extremely important since it is expensive to set up a blockchain among C-sensor nodes with limited resources. Since the agreement processes became the basis of blockchain technology, excellent research on these topics has flourished. DPoS has been adopted here.

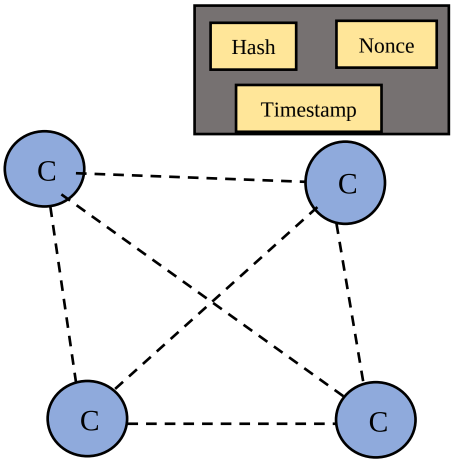

Fig. 2 Blockchain-based decentralized key management

With DPoS [22], there is no domination of the wealthy nodes and little computational power use. It uses fewer resources and produces blocks for the blockchain more quickly. It uses fewer resources and produces blocks for the blockchain more quickly. In other words, WSNs with restricted node resources benefit greatly from low energy usage[23][24]. Because of the rapid block manufacturing pace, c-sensor nodes can quickly agree and decide on a course of action. The DPoS method also makes the blockchain incredibly scalable so that more nodes may be connected [21].

4. Key Management Scheme

This section provides the various steps involved in building a blockchain-based key management system. The system design is shown in fig.2, which comprises node registration, grouping, and mobility.

4.1. Node Registration

The HN creates system parameters and aids C-sensor nodes in registering the node prior to network deployment.

4.1.1. System Parameter Generation

i. A k-bit prime p is selected via Key Generation Centre (KGC) at the Head node, producing the tuple E(Fp) over a finite field Fp. Key Generation Centre selects a group G, with order n over E(Fp) and P as the generator.

ii. KGC chooses a random s ∈ Z^{*}_{n} as the master *mk* and calculates the public key $P_{pub} = sP$. Where s is the master private key.

iii. The Cryptographic hash functions are {H0, H1, H2, H3}.

iv. KGC circulates the system parameter params = { *p, n, $E(F_p)$, G, P, P_{pub}, H_0, H_1, H_2, H_3* and holds the master key s secret.

4.1.2. Public-Private Key Extract

```
function KGC(params, mk, ID):
  nMi = number of M-sensors
  nGj = number of C-sensors
  rID = random number generated using mk and the user ID
  RID = rID * params.P
  hID = H1(ID, RID)
  sID = (rID + hID) mod n
  DID = (sID, RID)
  return DID

function Set-SecretValue(ID, params):
  xID = random number in Z_n^*
  PID = xID * params.P
  return xID

function Set-PublicKey(xID, params):
                    PID = xID * params.P
                    return PID

function Verifier(sID, RID, PID, ID, hIDPpub, params):
  if (sID * params.P) == H(H(PID) + RID + hIDPpub) + RID:
    return 1
  else:
    return 0
```

4.1.3. Genesis Block Generation

i. Following the completion of key creation for each node, the HN sent a message msg containing a registration list comprising the IDs and public keys of each node to all C-sensor nodes.

ii. If the verification is successful, the witness node (C-sensor node), in accordance with the DPoS method, marks the new block referred to as the genesis block. When greater than 50 percent of the consensus nodes validate via the block, the witness sensor node instantly propagates the block, confirming that it has been added to the blockchain.

iii. If verification is unsuccessful, the C-sensor nodes send out alerts concerning HN hacking or a fake HN assault.

4.2. Cluster Formation

The cluster construction starts once nodes have generated their public/private keys without a certificate.

i. Node Discovery- nCj broadcasts a cluster message which contains Cj and pk_{Cj}. When n_{mi} obtains the message, it performs the pairwise key generation process and validates Cj and pk_{Cj} against the blockchain's genesis block. Since n_{Mi} may obtain cluster signals from several cluster heads, n_{Mi} selects one C-sensor based on the signal's distance and intensity. n_{Mi} and n_{Cj} obtain a pairwise master key K_{MiCj} and a pairwise encryption key k_{MiCj}.

ii. Cluster Key Generation- n_{Gj} generates a cluster key C_{Kj} and x_{ID} ∈ $Z^{*}_{n,}$
CKj = HMAC(xj, Cj).

iii. Making entries on the blockchain: message <WARNING, compNode: Cj,< Mi, pk_{Mi} >> is broadcast in C-sensor nodes, the message is verified by the receiving node using the criteria listed below::
   1. Verify the existence of whistleblowers' identities and public keys in the registration list.
   2. Verify whether the whistleblowers' public key and identity match.

4.3. Node Movement

The C-sensor nGj must appropriately update the cluster key when a node departs or enters a cluster, alert other C-sensors to the altered node status, and edit the list so that it can be recorded to the blockchain.

4.3.1. Node Exit

M-sensor nodes are not required to report whether they are leaving the cluster actively or passively. Since when n_{Cj} does not get the beacon message from n_{Mm} for a while, it can identify a departing node n_{Mm} using the heartbeat method. When n_{Cj} notices that n_{Mm} is departing, it broadcasts the information to all other C-sensor nodes. As soon as consensus nodes have verified the report, they put the report in the pool for further verification of the block. A node has left the cluster if more than 50 percent of the consensus nodes synchronise the block.

4.3.2. Node Addition

Nodes can join a cluster in two different ways: by joining another cluster or by leaving the current cluster. We suppose that n_{Mm} wishes to join the l^{th}-cluster or go back to the j^{th}-cluster in order to make our explanation more straightforward.

4.4. Key Revocation

Key revocation for a sensor node will be done by a trusted cluster head, which is a part of the blockchain. We propose a deterministic technique that utilizes blockchain technology which helps to simply key revocation.

5. Security Analysis

5.1. Forward and Backward Security

Forward secrecy is a security concern. If a node nMm has left the cluster but is still listening for cluster messages, HIBE is not secure. This approach has a double benefit and uses less node energy while simultaneously updating the cluster keys. Using random values, the cluster head generates a new cluster key whenever a new sensor node joins the cluster and transmits it to the member nodes. This ensures backward security because the new cluster key cannot decode the data encrypted earlier.

5.2. Resistance to Pseudo-HN Attack

Pseudo-HN attacks can potentially harm the entire network and steal sensitive data from WSNs. Our scheme's HN uses only the private-public key pair and the distribution of a list of authorised sensor nodes. Because the node generates the entire key pair, the node cannot authenticate the usage of an incomplete private-public key pair generated by the pseudo-HN. Even if the partial key is verified, the fake Head node cannot be told of the whole key.

6. Performance Evaluation

6.1. Simulation Parameters

MATLAB is used for simulation. The parameters are shown in Table 1.

Table 1. Simulation parameters

Parameter	Value
Number of sensor nodes	300-500
C-Sensors	15%
Empirical energy	20nJ

6.2. Storage Requirement

The C-sensor nodes' usage of blockchain technology improves communication and storing capacity among the C-sensors, which enhances security and ensures stable communications because there is little to no interaction with the HN required. Additionally, 85% of the nodes in our sensor network are M-sensor nodes, which perform the bulk of the work. In light of the storage overhead, we thus focus primarily on M-sensor nodes.

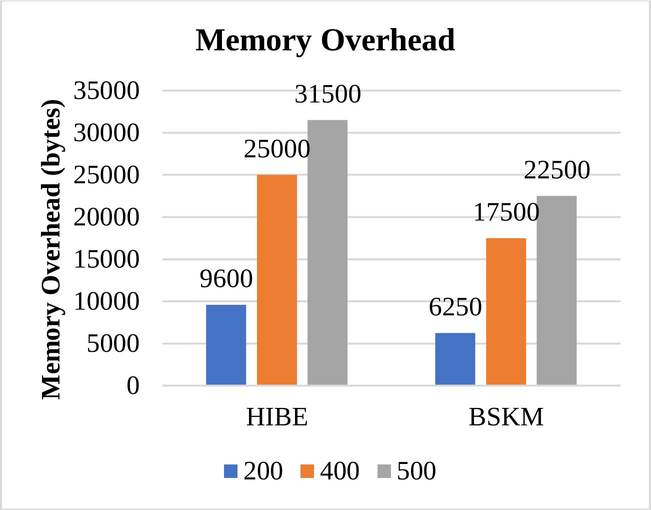

Fig. 3 Storage cost of M-sensor nodes

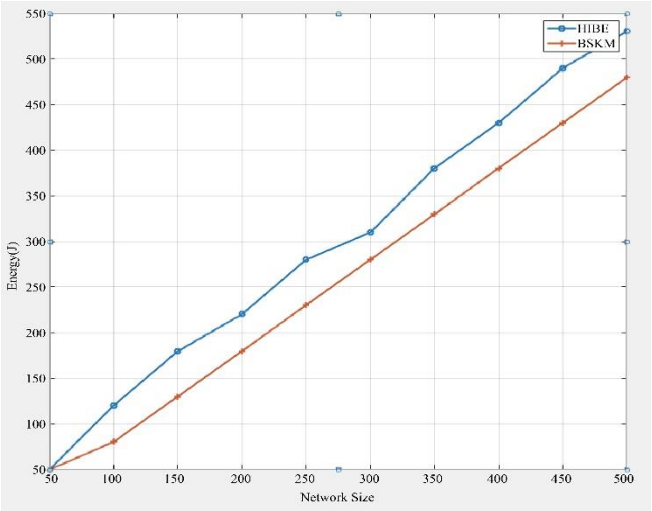

Fig. 4 Energy consumed during cluster formation

Figure 3 compares the storage costs of our scheme with HIBE to the number of M-sensor nodes, which make up 85% of all sensor nodes. In comparison to the BSKM, the HIBE overhead clearly rises as the number of M-sensor nodes grows. This is because, in contrast to the HIBE [28], the BSKM lacks the individual node key while including the pairwise, public-private, and cluster keys.

6.3. Energy Consumption

Additionally, Fig. 4 illustrates how the number of nodes in the WSNs affects the energy consumption of BSKM and HIBE. Information is sent between nodes over an average distance of 100 m. The obtained findings show the energy consumption of the HIBE, which refers to the energy consumed during the cluster formation. Consumption increases noticeably as the size of the WSNs grows. This is due to a number of factors, which include the following.

- We streamline the protocol stages involved in cluster creation, which means that after receiving the cluster key, M-sensor nodes no longer need to communicate with one another to confirm.
- A significant amount of energy is used when the C-nodes connect with the Head Node to assess the authenticity of the cluster members.

Instead of requiring the HN to take part in the verification process of the legitimate cluster members, our scheme uses blockchain technology to create a legitimate list of legitimate cluster members among the C-sensor nodes.

6.4. Reliability

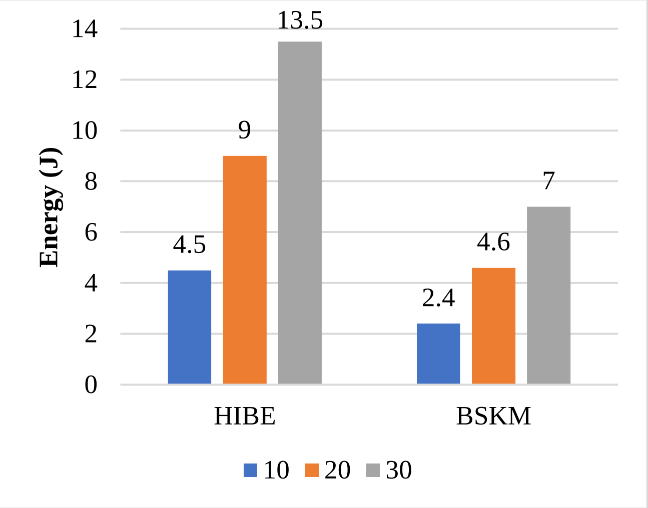

Fig. 5 Energy consumption of handling compromised C-sensor nodes

The dependability of WSNs requires treating compromised nodes to reduce their energy usage. Energy is often not used during the cluster formation if M-sensor nodes are hacked since C-sensor nodes simply disregard the signals from compromised M-sensor nodes. However, energy use has increased because of alert activities if C-sensor nodes are compromised. Because of the impaired C-sensor, Fig. 5 illustrates the increased energy consumption between our proposed scheme and HIBE. The energy overhead grows significantly compared to our system as the number of compromised C-sensor nodes rises.

6.5. Resilience Against Node Capture

The dependability of WSNs requires treating compromised nodes to reduce their energy usage. Energy is often not used during the cluster formation if M-sensor nodes are hacked since C-sensor nodes disregard the signals from compromised M-sensor nodes. However, energy use has increased because of alert activities if C-sensor nodes are compromised. Because of the impaired C-sensor, Fig. 5 illustrates the increased energy consumption between our proposed scheme and HIBE. The energy overhead grows significantly compared to our system as the number of compromised C-sensor nodes rises.

6.6. Resilience Against Node Capture

One potential drawback of Hierarchical Identity-Based Encryption (HIBE) compared to BSKM is its potential for scalability issues due to the hierarchical key structure, which may pose challenges when it comes to adding new users or groups. This can be a point of concern for applications that require the ability to incorporate new users or cater to sizable user groups swiftly.

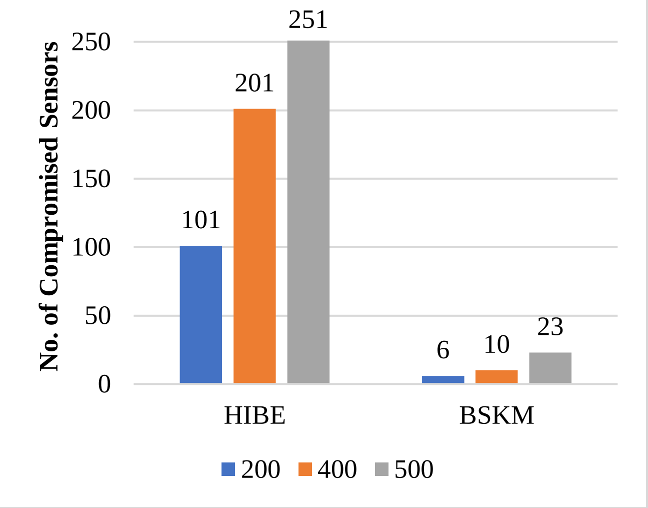

Fig. 6 Number of Compromised nodes

7. Conclusion

Here, we have presented a blockchain-based secure key management system (BSKM). The BSKM primarily employed blockchain networks to manage registration and cluster lists using a consensus process. Simulation results indicate that our method provides resistance to node compromise, pseudo-HN attacks, and other threats. Blockchain networks comprising C-sensors perform most of the functions of HN, such as reliable databases. This scheme provides efficient energy usage and less storage overhead. With higher resiliency, the entire WSN became a highly reliable network. Therefore, we can safely conclude that blockchain technology is promising for security management in WSN.

References

[1] Nickolaos Koroniotis et al., "The Sair-Iiot Cyber Testbed as a Service: A Novel Cybertwins Architecture in IIot-Based Smart Airports," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, 2023. [Crossref] [Google Scholar] [Publisher Link]

[2] Rajakumar Arul et al., "A Quantum-Safe Key Hierarchy and Dynamic Security Association for LTE/SAE in 5G Scenario," *IEEE Transactions on Industrial Informatics*, vol.16, no. 1, pp. 681-690, 2019. [Crossref] [Google Scholar] [Publisher Link]

[3] Sk.Md.Mizanur Rahman, and Khalil El-Khatib, "Private Key Agreement and Secure Communication for Heterogeneous Sensor Networks," *Journal of Parallel and Distributed Computing*, vol. 70, no. 8, pp. 858-870, 2010. [Crossref] [Google Scholar] [Publisher Link]

[4] Xiaojiang Du et al., "An Effective Key Management Scheme for Heterogeneous Sensor Networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24-34, 2007. [Crossref] [Google Scholar] [Publisher Link]

[5] Siddiq Iqbal, and B. R. Sujatha, "Secure Key Management Scheme for Hierarchical Network Using Combinatorial Design," J*ournal of Information Systems and Telecommunication (JIST*, vol. 10, no. 37, p. 20, 2022. [Crossref] [Google Scholar] [Publisher Link]

[6] B. Murugeshwari et al., "Trust Aware Privacy Preserving Routing Protocol for Wireless Adhoc Network," *International Journal of Engineering Trends and Technology*, vol. 70, no. 9, pp. 362-370, 2022. [Crossref] [Publisher Link]

[7] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP+ Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)*, pp. 62-72, 2003. [Crossref] [Google Scholar] [Publisher Link]

[8] Y. Akshatha, A. S. Poornima, and M. B. Nirmala, "Secure Data Collection in Clustered Wireless Sensor Networks Using Fuzzy Based Scheme to Detect Malicious Data Collector," *International Journal of Engineering Trends and Technology*, vol. 70, no. 11, pp. 240-248, 2022. [Crossref] [Publisher Link]

[9] Rolf Blom, "An Optimal Class of Symmetric Key Generation Systems," *Workshop on the Theory and Application of Cryptographic Techniques*, vol. 209, pp. 335-338, 1984. [Crossref] [Google Scholar] [Publisher Link]

[10] R.Rajesh, and Dr.K.Ramakrishnan, "An Assessment of Key Management Using Certificateless Cryptography in Mobile Adhoc Network," *International Journal of Computer & Organization Trends (IJCOT)*, vol. 7, no. 1, pp.18-2, 2017. [Crossref] [Publisher Link]

[11] Diego Ongaro, and John Ousterhout, "In Search of an Understandable Consensus Algorithm," *2014 USENIX Annual Technical Conference (Usenix ATC 14)*, pp. 305-319. 2014. [Google Scholar] [Publisher Link]

[12] Sarmadullah Khan et al., "Resource Efficient Authentication and Session Key Establishment Procedure for Low-Resource IoT Devices," *IEEE Access*, vol. 7, pp. 170615 – 170628, 2019. [Crossref] [Google Scholar] [Publisher Link]

[13] Ashwag Albakri, Lein Harn, and Sejun Song, "Hierarchical Key Management Scheme with Probabilistic Security in a Wireless Sensor Network (WSN)," *Security and Communication Networks*, vol. 2019, pp. 1-11, 2019. [Crossref] [Google Scholar] [Publisher Link]

[14] Mojtaba Jamshidi et al., "A Hybrid Key Pre- Distribution Scheme for Securing Communications in Wireless Sensor Networks," *JOIV: International Journal on Informatics Visualization*, vol. 3, no. 1, pp. 41-46, 2011. [Crossref] [Google Scholar] [Publisher Link]

[15] E. Sweetline Priya, R. Priya, and R. Surendiran, "Implementation of Trust-Based Blood Donation and Transfusion System Using Blockchain Technology," *International Journal of Engineering Trends and Technology*, vol. 70, no. 8, pp.104-117, 2022. [Crossref] [Publisher Link]

[16] Seung-Hyun Seo et al., "Effective Key Management in Dynamic Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Securit*, vol. 10, no. 2, pp. 371-383, 2015. [Crossref] [Google Scholar] [Publisher Link]

[17] V. S. Janani, and M. Devaraju, "An Efficient Distributed Secured Broadcast Stateless Group Key Management Scheme for Mobile Ad Hoc Networks," *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, pp. 1-5, 2022. [Crossref] [Google Scholar] [Publisher Link]

[18] Chin-Chen Chang, Wei-Yuan Hsueh, and Ting-Fang Cheng, "A Dynamic User Authentication and Key Agreement Scheme for Heterogeneous Wireless Sensor Networks," *Wireless Personal Communications*, vol.89, no. 2, pp. 447-465, 2016. [Crossref] [Google Scholar] [Publisher Link]

[19] G. Sahitya, N. Balaji, and C. D. Naidu, "An Improved Routing Protocol for Heterogeneous Wireless Sensor Networks," *International Journal of Engineering Trends and Technology*, vol. 70, no. 10, pp. 79-86, 2022. [Crossref] [Publisher Link]

[20] R. Surendiran, and K. Alagarsamy, "Privacy Conserved Access Control Enforcement in MCC Network with Multilayer Encryption," *International Journal of Engineering Trends and Technology*, vol. 4, no. 5, pp. 2217-2224, 2013. [Crossref] [Publisher Link]

[21] D. Larimer, "Delegated Proof-of-Stake (DPOS)," Bitshare White Paper, Murska Sobota, Slovenia, 2014.

[22] Youliang Tian et al., "A Blockchain-Based Secure Key Management Scheme with Trustworthiness in DWSNs," *IEEE Transactions on Industrial Informatic*s, vol. 16, no. 9, 2020. [Crossref] [Google Scholar] [Publisher Link]

[23] Karpaga Priya R et al., "A Novel Spider Swarm Optimized Energy and Security Aware Clustering Protocol for Smart Grid Wireless Sensor Network," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 9, no. 10, 2022. [Crossref] [Publisher Link]

[24] B Srinuvasu Kumar, S.G. Santhi, and S. Narayana, "A Novel Method for Enhancing the Network Lifetime Using Energy-Efficient Routing Protocol Approach for Wireless IoT Sensor Network Applications," *International Journal of Engineering Trends and Technology*, vol. 70, no. 11, pp. 277-287, 2022. [Crossref] [Publisher Link]

[25] Mcconaghy et al., "*Bigchaindb: A Scalable Blockchain Database*," White Paper, Bigchaindb, 2016.[Google Scholar]

[26] R.Sharmila, P.C.Gopi, and Dr.V.Vijayalakshmi ,"A Survey of Key Management Schemes in Wireless Sensor Networks," *International Journal of Computer & Organization Trends (IJCO T)*, vol. 3, no. 5, pp. 48-52, 2013. [Google Scholar] [Publisher Link]

[27] R. Surendiran, "Similarity Matrix Approach in Web Clustering," *Journal of Applied Science and Computations,* vol. 5, no. 1, pp. 267-272, 2018. [Google Scholar] [Publisher Link]

[28] Yan Liu, Xiumei Wu, and Xuemin Chen, "A Scheme for Key Distribution in Wireless Sensor Network Based on Hierarchical Identity-Based Encryption," *2015 IEEE 12th International Conference on Networking, Sensing and Control*, pp. 539-543, 2015. [Crossref] [Google Scholar] [Publisher Link]

[29] Gabin Heo, Kijoon Chae, and Inshil Doh, "Hierarchical Blockchain-Based Group and Group Key Management Scheme Exploiting Unmanned Aerial Vehicles for Urban Computing," *IEEE Access*, vol. 10, pp. 27990-28003, 2022. [Crossref] [Google Scholar] [Publisher Link]

[30] Sheikh Munir Skh Saad, Raja Zahilah Raja Mohd Radzi, and Siti Hajar Othman, "Comparative Analysis of the Blockchain Consensus Algorithm between Proof of Stake and Delegated Proof of Stake," *2021 International Conference on Data Science and Its Applications* (ICoDSA), 2021. [Crossref] [Google Scholar] [Publisher Link]

[31] S. Gavaskar, E. Ramaraj, and R. Surendiran, "A Compressed Anti IP Spoofing Mechanism Using Cryptography," *International Journal of Computer Science and Network Security*, vol. 12, no. 11, pp. 137-140, 2012. [Google Scholar] [Publisher Link]