IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure Qos Routing In Blockchain-Enabled Wireless Sensor Networks: Efficiency And Performance Review

[1] Renukha M, [2]Sri Gokulam R, [3] Priya.P, [4]Suriyapriya, [5]Selvi.P, [6]R.V.Sudha

[1,2]Assistant Professor/ Bharathiyar Institute of Engineering For Women , [3,5,6] Assistant Professor/Knowledge Institute of Technology , [4]Assistant Professor/ Vivekanandha College Of Technology for Women,Tamilnadu

Abstract: A wireless sensor network (WSN) is made up of autonomous, geographically dispersed sensors that monitor the network and gather data about its surroundings. Although biomedical sensors gather data in an efficient and safe manner and prohibit potentially harmful user behaviors (i.e., attacks) within the network, recognizing assaults from ordinary sensor nodes remains a tough task. is. In wireless sensor networks (WSNs), authentication entails validating data requests and answers. As a result, authentication is the most important security precaution. In order for low-resource sensor nodes to function properly inside the Internet of Things, lightweight authentication mechanisms are required. In order to accomplish these goals, a brand-new authentication mechanism that uses three different factors was developed. According to the results of the study, the suggested system performs better than any prior similar protocol, making it well suited for applications using the WSN. Its efficiency may be quantified by looking at the costs of computation and transmission. The authentication of WSN is essential. This enables authorized users who have registered for the service to obtain real-time sensing data from WSN sensor nodes. WSN sensor and gateway nodes are required to validate a user before giving access to the network. They have some factors are the power efficiency, reliability, scalability and the mobility, Energy efficient can be performance. It is cannot consider noising and higher traffic. They are used some algorithm, protocols and modulation schemes and energy efficient performance. In this survey discussed about the cross-layer design with the wireless sensor network. Further implement new low power MAC protocol and dynamic node traffic analysis is improving the network life time and throughput.

Keywords: - Block chain, WSN, Cluster Protocol, Data Aggregation Authentication.

I. INTRODUCTION

A wireless sensor network is a network made up of sensors (also known as nodes) that collectively perceive physical and environmental factors such as temperature, sound, vibration, motion, object detection, and automation. A wireless sensor network is a network architecture comprised of measuring, computation, and communication elements that enables administrators to detect, observe, and respond to events and phenomena in a particular environment. Administrators are often employed by private, public, commercial, or industrial enterprises. The physical world, biological systems, and information technology frameworks are all examples of the environment [1-6].

There are no rules or limitations imposed for communication infrastructure. Shared wireless assistance imposes extra node communication constraints and presents current issues such as asymmetric and unreliable connections. But, with the broadcast benefit, all the sending node's neighbors can receive information transferred from one node to another. The process of identifying a user is known as authentication. This is a system that assigns identifying credentials to incoming requests. Node IDs, for example, can be used to perform authentication in wireless sensor networks.

Energy efficiency is a fundamental concern in wireless sensor networks. Intra-network aggregation is a well-known method for increasing energy efficiency. In intra-network aggregation, rather of transmitting several data items to a receiver, data items are consolidated and transmitted to the network. The application determines data aggregation. That is, it is dependent on the intended application and the data aggregation operator (or aggregator). As a result, numerous data aggregation techniques are required to suit various sensor network circumstances. Even though sums and averages are enough for many applications, there are situations when they are insufficient. WSNs need to be able to aggregate data effectively. Sensor network applications have a direct relationship with these features and performance measures. Data accuracy, communication, latency, energy efficiency, network longevity, overhead, and overhead are examples of critical performance indicators. Averages and sums are examples of aggregate measures that are adequate for many applications, but they might not be in others. WSNs need to be able to aggregate data effectively.

Sensor network applications are intimately linked to these characteristics and performance measures. Energy efficiency, network longevity, latency, communication, overhead, and data correctness are examples of critical performance measures. There are three types of methods: lossless, independent, and iteration-dependent aggregations. It is crucial to manage different aggregation needs in sensor networks. By aggregating data within the network, communication costs can be drastically decreased and data quality can be guaranteed to meet the necessary range. Getting the most representative data with the least amount of resources is the primary feature of a good aggregation method.

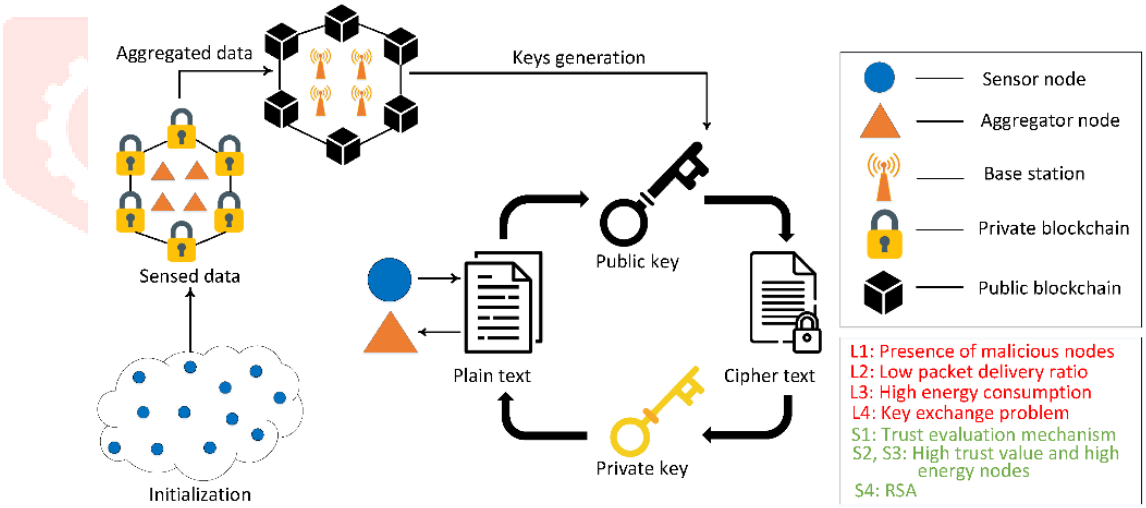

Figure 1 blockchain based sensor network [2]

Sensor nodes are widely dispersed throughout wireless sensor networks, and the surrounding physical environment produces a lot of identical data that is essentially redundantly transmitted. Consequently, all of these facts support the usage of some kind of sensor node grouping, whereby a group of sensor nodes can combine or compress data, allowing for the transmission of only compact data. This could lower global data or local traffic within a single group. Clustering is the process of organizing large-scale sensor nodes at high density into groups.

Data fusion (aggregate) is the process of merging and condensing data from a single cluster. Periodically, sensors gather, analyze, and transmit data to the base station. In wireless sensor networks, data aggregation is a significant technological advancement, and securing the combined data is a critical concern. By removing unnecessary data, data aggregation can significantly contribute to energy consumption reduction. Aggregators are susceptible to node compromise attempts, though, particularly

if their hardware isn't tamper-resistant. It is simple to alter the aggregation profile once an aggregator node has been hijacked and to provide the WSN a false profile.

Thus, effectively relaying sensor readings to the base station while making sure the reported data isn't altered is the definition of secure data aggregation. In WSNs, there are two types of secure data aggregation that are offered. Hop-by-hop and end-to-end aggregation is the name of the first group [15]. In the first, the aggregator is in charge of decrypting the encrypted data that is received from the sensors, while each sensor node is in charge of encryption. After gathering the data and encrypting it once more, the aggregator transmits the findings to the base station. Aggregation is limited to the encrypted data that is received from the sensor nodes by the aggregator node in the second node.

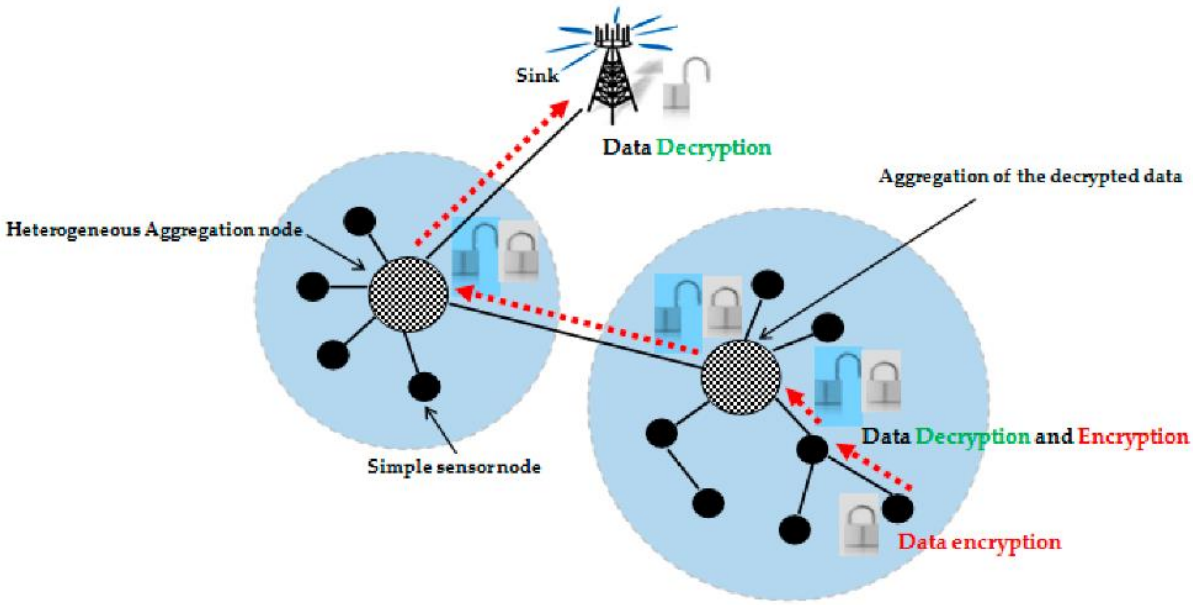

Figure 2: Data aggregation based wireless sensor network [5]

Cryptographic system design, including WSN user authentication, is risky and time-consuming. Cryptography is famously hard to penetrate. Several cryptographic methods have weaknesses years after they were released, showing how difficult it is to ensure their security. See "See" for cryptographic scheme weaknesses. Formal security evaluations have become popular because to the many problems found in published schemes in recent decades. Reasons include this. This research's main categories are computer security and computational complexity. The Dole–Yao adversarial paradigm emphasizes automated machine definition and analysis for computer security. This model uses black-box cryptographic primitives, ignoring some cryptography complexities. Black-box model. Intractability and undesirability plague this automated method. State explosion occurs because the opponent might behave in many ways. The opponent's unexpected behavior causes these issues. Cryptographic algorithms certified secure may have a weakness that causes a false positive. Several factors can cause this. Yet, the computational complexity approach derives a polynomial-time reduction by breaking the scheme into another difficult problem. An exhaustive computational proof led by a well-established cryptographic assumption can provide high confidence that the scheme's security characteristics are met. This will help you succeed. Because of this, cryptographic scheme designers now give a confirmed reduction for their schemes' security in the form of a cryptographic community-accepted model. This proves their schemes are secure. Human mathematical proofs are useful for developing secure cryptography techniques, despite their length and complexity.

1. Literature review

In this section focused on the review of the literature and provides a description, important findings after critical evaluation of related works in the relation to the proposed research [19, 20]. The proposed work is having a broad aim of providing QoS assurance in wireless sensor networks through routing algorithms based on the swarm intelligence method. So, in this chapter, existing routing protocols are studied at first, followed by QoS based routing protocols.

The primary goal is to address the security concerns related to data aggregation in wireless sensor networks. The majority of current data aggregation methods lack inherent privacy safeguards. Nonetheless, a difficult problem concerning security exists in sensor networks, as demonstrated by a BC-based authentication system aimed at enhancing WSN security [11]. The network was comprised of nodes created by the BS, standard SNs, and CHs. The BC model created a hierarchical BC system, comprising local BC and global BC, to verify the nodes within the network. In the hierarchical BC, local BC verified the authenticity of the regular nodes, while global BC validated the authenticity of the CH nodes[12]. A secure link was formed in the network through the hierarchical method. The results indicated that the model offered robust security and improved outcomes for data protection. Qing Fan et al. [16] introduced a secure authentication and distributed trust scheme for IoT networks employing the blockchain mechanism.

Several issues must be taken into account while designing routing protocol in WSN. First, for enhancing the network lifetime, the mechanisms used for route exploration and data transmission should be energy efficient. Second issue is related to the nodes in network which operate without manual intervention [17, 18]. The network is expected to exhibit autonomic properties, meaning that the protocol being used should be self-organizing and able to handle failures of individuals. Last oint to consider is that, the routing protocol must be able to handle large number of nodes which are scattered in networks.

The constraints and challenges of QoS management—which can be network- or application-specific—are covered in the study [12]. The authors suggested a modified clustering protocol termed his LEACH-APP [28] that considers network applications for QoS management in an effort to raise QoS awareness. LEACH-APP is intended for networks with a variety of traffic kinds coming from different sources. The authors draw attention to the issues brought about by improper cluster head selection in clustering methods like LEACH [29]. The authors concentrate on using fitness functions to choose the best cluster heads in order to minimize load balancing and energy usage.

Security requirements for a wireless sensor network (WSN) include confidentiality, integrity, availability, and dependability. Not every security solution created for traditional computer networks can be applied immediately to wireless sensor networks due to their limitations. Due to its high processing power needs, public-key cryptography was long regarded as being unsuitable for wireless sensor networks. However, research on curve-based encryption algorithms is opening up new possibilities for this technology. The possibility of it has been established. The most often used public key algorithm for WSNs is Rivest-Shamir-Adleman (RSA). Elliptic curve-based algorithms have been extensively researched in academic circles as RSA substitutes and have demonstrated strong performance with smaller keys.

2. BLOCKCHAIN BASED AUTHENTICATION UTILIZED IN WSN

The author [16] formed a three-factor authentication system that included session keys for WSNs, User registration, smart card revocation, authentication, and password renewal, sensor registration were all parts of the process. Compared with similar methods, this scheme outperformed them regarding security, which can typically run in an WSN context. It also has a practical application. Shadi Nashwan [8] presented the Anonymous Access Authentication strategy for WSNs in significant data contexts (AAA-WSN) for delivering security services.

Strong security features of the AAA WSN technique included perfect forward secrecy at every authen tication level, complete mutual authentication between all authentication entities, and anonymity to b oth the user

and the SN entities.The performance research showed that the AAAWSN maintained a desirable effic iency level while achieving a superior level of security when compared to existing WSN authenticatio n techniques.

For WSNs, this paper [6] proposed a threefactor authentication system that makes use of the honey lis t technique.Due to the limited capabilities of the sensor, this model also created an effective protocol t hat relies only on hash functions instead of public key-based ECC.

Compared to previous research, the results demonstrated that this authentication process was both app

ropriate and safe. An ECC-based three-factor authentication mechanism for WSNs was created in this work [10].

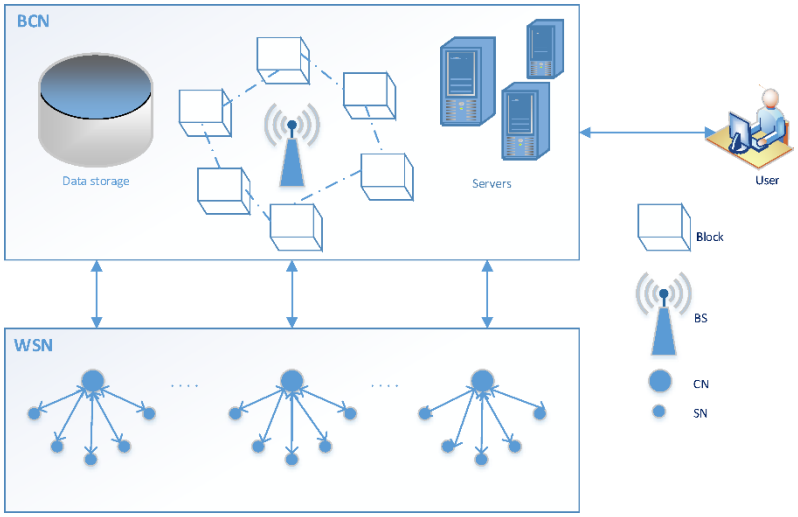

Figure 3 Authentication based WSN clusters

In this [61] proposed the SLUA-WSN protocol, a Secure and Lightweight three-factor-based User Authentication system for WSN. This SLUA-WSN can protect users from security threats while providing anonymity, untraceability, and mutual authentication. The author used the Burrows–Abadi–Needham (BAN) logic analysis to evaluate SLUA-WSN. The performance comparison revealed that SLUA-WSN provided greater security and efficiency than earlier methods and was suitable for real-world WSN applications. Mostafa Farhadi Moghadam et al. [22] developed a mutual authentication and key agreement protocol for WSNs centered on Elliptic-Curve Diffie–Hellman (ECDH). It was divided into three stages: two authentication phases and a password change. The analysis revealed that the protocol required less computation while providing complete security than state-of-the-art techniques.

Table 1 Blockchain based WSN security

Author/Year	***Method***	***Description***	***Drawback***
Zhihua Cui (2020) et., al [1]	blockchain based multi-WSN authentication	IoT nodes are classified as base stations, cluster head nodes, and ordinary nodes according on their functions, establishing a hierarchical network.	This network prone to single point failure.
Lakshmana Kumar Ramasamy (2021) et.al., [2]	blockchain techniques with WSNs (BWSN)	Storage for auditing, event logging, information analysis, and offline query processing is included.	Malicious node detection technologies use a centralized, one-time decision-making methodology, making security a critical consideration.
Muhammad Nouman (2023) et.al.,[3]	Adaptive Boost (AdaBoost), Gradient Boost (GB), Linear Discriminant Analysis (LDA),	deep blockchain and Markov Decision Processes (MDPs)	it is difficult to identify untrusted activities of routing nodes effectively

	Extreme Gradient Boost (XGB)		
Rekha Goyat(2020) et.al., [14]	blockchain-based decentralized framework	All critical characteristics and large amounts of data on the decentralized blockchain are transferred to cloud storage.	Due to low data processing power and limited storage capacity, ensuring network security is difficult from a security standpoint.
Khalid Haseeb (2019) et.al., [15]	intrusion prevention framework	To ensure cluster stability, overlapping and autonomously arranged clusters are produced based on the uncertainty principle.	Most solutions concentrate on static topologies, ignoring the dynamic topology of mobile sensor nodes.
Adeel Ahmed(2022) et.al., [12]	Energy-Efficient Data Aggregation Mechanism (EEDAM)	Mechanism for aggregating data at the cluster level in order to save energy.	To group nodes with strong data similarity, use fuzzy matrices.
Gang Li (2021) et,al.,[4]	disaster semantic blockchain (DSB)	sparsity-optimized and compressed sensing-based spatiotemporal data aggregation model is built.	There is low network lifetime efficiency and limited security.
Z. A. Khan(2023) et.al., [6]	heterogeneous gateway-based energy-aware multi-hop routing (HMGEAR)	the single point of failure issue, a decentralized blockchain is deployed on CHs and BS.	low throughput, and high network delay and high energy consumption.
Huanhuan Feng(2020) et.al., [7]	K-means and SVM algorithms	An application for classifying and forecasting mass loss in frozen shellfish.	Information storage relies on the centralized platform, it is possible to tamper.
Cuong Trinh (2020) et.al.,[10]	LBCbAP	Security against a variety of attacks, including secret leaks and asynchronous assaults.	There are limitations to the available power and computational capability.

Hanguang Luo et al. [23] developed a three-factor mutual authentication (3FA) model and a key agreement protocol for examining the data access performed in real time for WSNs. This approach was divided into four phases: registration, authentication and key exchange, password renewal, and dynamic node addition. The results demonstrated that the 3FA scheme was more secure and effectual when contrasted with state-of-the-art algorithms. In this work [24] projected an identity authentication protocol using lightweight cryptographic primitives for WSNs that included a physical unlovable function, a one-way hash function, and a bitwise exclusive operation. Furthermore, biometrics (like fingerprints and iris scans) have been used to obtain access to remote systems. According to the

comparative results, this strategy has much less communication overhead and computation complexity and is much more efficacious than baseline approaches.

3. Blockchain based various security in WSN

In [67] presented a BC-based authentication framework with a physically unlovable function (PUF) for IoT environments. The PUF guaranteed the privacy of the users with a decentralized BC. The combination of PUF and BC ensured data transparency and provenance in the network. Smart contracts based on BC provide decentralized digital ledgers that can withstand data tampering attacks. These advantages ensure the privacy and security of data which is outsourced in WSN networks. Saba Awan et al. [68] recommended a BC-based encryption and trust estimation technique with authentication of SNS and aggregator nodes (ANs). The authentication of SNs and ANs was done in private and public blockchains. To avoid malicious nodes in the network, the trust values of SNs were computed.

Author/year	***Technique***	***Methodology***	***Drawback***
Y. Wang/2019[7]	cloud-based road condition monitoring (RCoM)	Addressing three key issues in RCoM.	The main challenge for cloud servers is to distinguish the same traffic from many reports from the same place.
J. Tsai,/2014[9]	Elliptic Curve Digital Signature Algorithm (ECDSA)	It supports identity revocation and trace.	The key verifier only functions in RSU.
S. Tzeng,(2017) [11]	identity-based batch verification (IBV)	The verification of the scheme only requires a small constant for pairing and dot multiplication calculations	Not recognizing illegal signatures.
W. Ren,et.al(2019) [23]	secure proactive tree-based routing (SPTR)	The certificate-less ID-based cryptography to provide message authentication.	High communication overhead without involving any certificates.

In this paper [24] provided security to the assisted WSNs by taking advantage of the cryptographic tools and BC. The BC technology provided the decentralized architecture for secure data storage, which guaranteed the security and autonomy of an WSN environment. The accuracy of the approach was tested, and the results demonstrated that the approach met the essential needs of an WSN. The technique was dependable and was more secure for sending information between the users and devices. In addition, the technique protected the network from the most vulnerable WSN attacks. Liangqin Gong et al. [11] presented a BC architecture for WSN that stored the identity of each WSN device in a distributed ledger.

4. Result analysis of Qos parameters in Blockchain network

This section compares the performance of the proposed blockchain based efficient clustering approach (EJS-FCM) based clustering & BGOA based optimal CH selection) with existing approaches such as other methods utilizes a Proof of Authority (PoA) method. The techniques are compared regarding the metrics, say energy consumption (ECN), throughput (TPT), delay (DLY), NL, and packet delivery ratio (PDR).

Parameter used in simulation [26]

Simulation Parameter	Details
Simulation area	100x100 m^2
Number of nodes	500
Transmission Range	200m
Network Standard	WI-Fi
Mobility Speed	20MHz
Delay	10ms

That deals with the performance evaluation of the proposed model by comparing them with the prevailing models regarding some performance metrics. The presented approach is implemented in the working platform of Network Simulator3.26 (NS-3.26) [21], and the simulation details are given table.

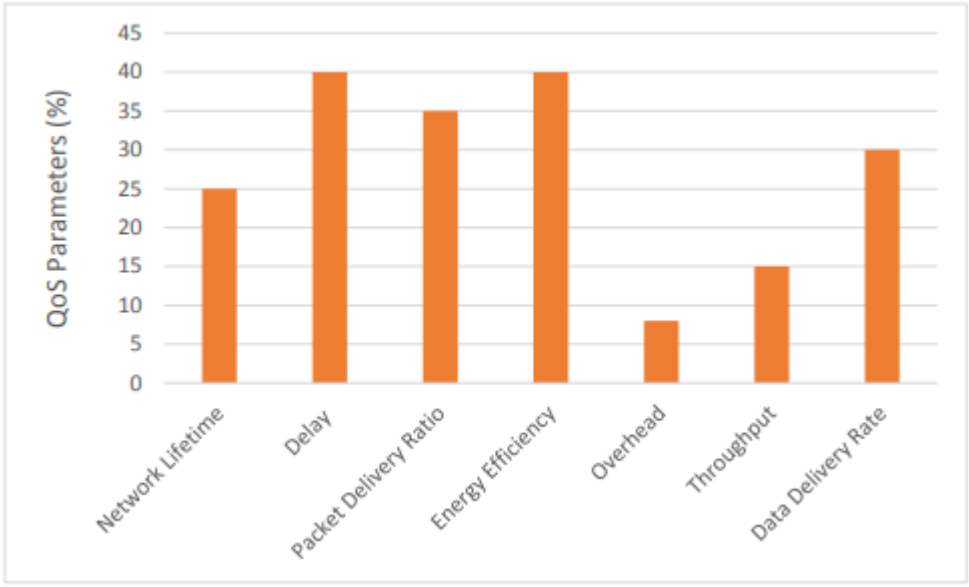

Figure 4 existing method QoS parameters [22]

This model shows the PDR attained by proposed and existing clustering approaches. PDR of the model is described as the ratio of total counts of generated data packets to the total counts destination received data packets.

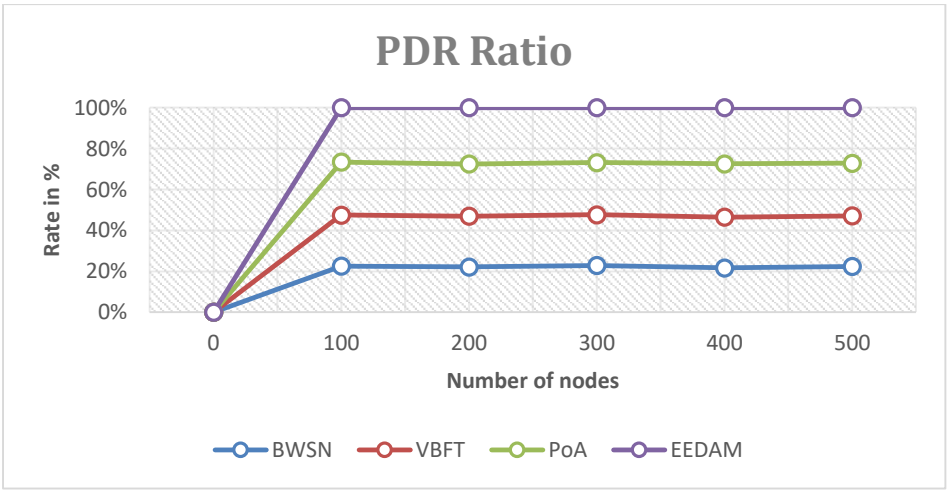

Figure 4 PDR analysis rate [28]

The PDR of the models is measured by varying the number of SNs in the networks from 100 to 500. For 100 nodes, the proposed model attains the PDR of 92%, whereas the existing models.

Table 3 PDR analysis [28]

Nodes	BWSN	VBFT	PoA	EEDAM
100	68	75	78	80
200	66	74	76	82
300	69	75	77	81
400	65	74	78	82
500	66	73	76	80

Table 3 existing techniques did not use any security models while performing EEDAM, which led to the packet drops of intruders in the network. So there is a higher packet loss presented in the previous approaches. In addition, the proposed model considers significant challenges of the WSNs, such as energy, QoS, and data security, that further increases the PDR of the presented model.

Conclusion

In this paper discussed various methodologies for providing WSN security. An efficient and secure BC-based protocol for authentication, blockchain is presented for attack detection, and a EEDAM-based security framework is presented to ensure data security. The many protocol achieves higher levels of security in all stages, including SN anonymity, authentication between SNs and BS, and data security. Furthermore, the formal security analysis is performed using the existing technique to demonstrate that the proposed system is more secure against various types of severe attacks. This is a problem because there is only a certain amount of storage capacity available. The Elliptic Curve Cryptosystem (ECC) in blockchain, on the other hand, provides an exceptionally high level of security while making the key size relatively reasonable. The authentication keys for each node so far discovered are included in this value. Slices of the data are encrypted and transmitted to the other nodes in the set using the authentication key that is specific to that node when one of the nodes in the set wishes to communicate data to the other nodes in the set. A percentage that represents the proportion of packets that have been successfully received so far to the total number of packets transmitted. In further work implement the detection framework to identify the malicious nodes using different trust schema and improve the node life time comparative previous method.

References

[1]. Awan, S.; Javaid, N.; Ullah, S.; Khan, A.U.; Qamar, A.M.; Choi, J.-G. Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks. Sensors 2022, 22, 411. https://doi.org/10.3390/s22020411

[2]. Z. Cui et al., "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN," in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 241-251, 1 March-April 2020, doi: 10.1109/TSC.2020.2964537.

[3]. L. K. Ramasamy, F. Khan K. P., A. L. Imoize, J. O. Ogbebor, S. Kadry and S. Rho, "Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey," in IEEE Access, vol. 9, pp. 128765-128785, 2021, doi: 10.1109/ACCESS.2021.3111923.

[4]. Boubiche, S.; Boubiche, D.E.; Bilami, A.; Toral-Cruz, H. An Outline of Data Aggregation Security in Heterogeneous Wireless Sensor Networks. Sensors 2016, 16, 525. https://doi.org/10.3390/s16040525

[5]. M. Nouman, U. Qasim, H. Nasir, A. Almasoud, M. Imran and N. Javaid, "Malicious Node Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs," in IEEE Access, vol. 11, pp. 6106-6121, 2023, doi: 10.1109/ACCESS.2023.3236983.

[6]. A. A. E. -M. And and S. M. Darwish, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach," in IEEE Access, vol. 9, pp. 103822-103834, 2021, doi: 10.1109/ACCESS.2021.3098933.

[7]. R. Goyat et al., "Blockchain-Based Data Storage With Privacy and Authentication in Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14203-14215, 15 Aug.15, 2022, doi: 10.1109/JIOT.2020.3019074.

[8]. K. Haseeb, N. Islam, A. Almogren and I. Ud Din, "Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things," in IEEE Access, vol. 7, pp. 185496-185505, 2019, doi: 10.1109/ACCESS.2019.2960633.

[9]. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad and Z. Mushtaq, "An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain," in IEEE Access, vol. 10, pp. 11404-11419, 2022, doi: 10.1109/ACCESS.2022.3146295.

[10]. G. Li, B. He, Z. Wang, X. Cheng and J. Chen, "Blockchain-Enhanced Spatiotemporal Data Aggregation for UAV-Assisted Wireless Sensor Networks," in IEEE Transactions on Industrial Informatics, vol. 18, no. 7, pp. 4520-4530, July 2022, doi: 10.1109/TII.2021.3120973.

[11]. Z. A. Khan, S. Amjad, F. Ahmed, A. M. Almasoud, M. Imran and N. Javaid, "A Blockchain-Based Deep-Learning-Driven Architecture for Quality Routing in Wireless Sensor Networks," in IEEE Access, vol. 11, pp. 31036-31051, 2023, doi: 10.1109/ACCESS.2023.3259982.

[12]. H. Feng, W. Wang, B. Chen and X. Zhang, "Evaluation on Frozen Shellfish Quality by Blockchain Based Multi-Sensors Monitoring and SVM Algorithm During Cold Storage," in IEEE Access, vol. 8, pp. 54361-54370, 2020, doi: 10.1109/ACCESS.2020.2977723.

[13]. Z. Cui, Y. Cao, X. Cai, J. Cai and J. Chen, "Optimal leach protocol with modified bat algorithm for big data sensing systems in internet of things", J. Parallel Distrib. Comput., vol. 132, pp. 217-229, 2019.

[14]. M. A. Khan and K. Salah, "IoT security: Review blockchain solutions and open challenges", Future Gener. Comput. Syst., vol. 82, pp. 395-411, 2018.

[15]. A. A. E.-M. And and S. M. Darwish, "Towards designing a trusted routing scheme in wireless sensor networks: A new deep blockchain approach", IEEE Access, vol. 9, pp. 103822-103834, 2021.

[16]. D. Sivaganesan, "A data-driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks", J. Trends Comput. Sci. Smart Technol., vol. 3, no. 1, pp. 59-69, May 2021.

[17]. J. Manuel, G. G. Deverajan, R. Patan and A. H. Gandomi, "Optimization of routing-based clustering approaches in wireless sensor network: Review and open research issues", Electronics, vol. 9, no. 10, pp. 1630, Oct. 2020.

[18]. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems", IEEE Internet Things J., vol. 4, no. 6, pp. 1832-1843, Dec. 2017.

[19]. L. Xiong, N. Xiong, C. Wang, X. Yu and M. Shuai, "An efficient lightweight authentication scheme with adaptive resilience of asynchronization attacks for wireless sensor networks", IEEE Trans. Syst. Man Cybern. Syst., vol. 51, no. 9, pp. 5626-5638, Sep. 2021.

[20]. Z. Abubaker, N. Javaid, A. Almogren, M. Akbar, M. Zuair and J. Ben-Othman, "Blockchained service provisioning and malicious node detection via federated learning in scalable internet of sensor things networks", Comput. Netw., vol. 204, Feb. 2022.

[21]. Z. Abubaker, A. U. Khan, A. Almogren, S. Abbas, A. Javaid, A. Radwan, et al., "Trustful data trading through monetizing IoT data using BlockChain based review system", Concurrency Comput. Pract. Exper., vol. 34, no. 5, pp. e6739, Feb. 2022.

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

[23]. F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs", Proc. IEEE Jordan Int. Joint Conf. Electr. Eng. Inf. Technol. (JEEIT), pp. 28-33, Apr. 2019.

[24]. L. Tang, Z. Lu and B. Fan, "Energy efficient and reliable routing algorithm for wireless sensors networks", Appl. Sci., vol. 10, no. 5, pp. 1-16, 2020.

[25]. J. Lockl, V. Schlatt, A. Schweizer, N. Urbach and N. Harth, "Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications", IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1256-1270, Nov. 2020.

[26]. S. Kumar, S. Duttagupta, V. P. Rangan and M. V. Ramesh, "Reliable network connectivity in wireless sensor networks for remote monitoring of landslides", Wireless Netw., vol. 26, no. 3, pp. 2137-2152, 2020.

[27]. U. S. Pacharaney and R. K. Gupta, "Clustering and compressive data gathering in wireless sensor network", Wireless Pers. Commun., vol. 109, no. 2, pp. 1311-1331, 2019.

[28]. W. Contreras and S. Ziavras, "Low-cost efficient output-only infrastructure damage detection with wireless sensor networks", IEEE Trans. Syst. Man Cybern.: Syst., vol. 50, no. 3, pp. 1003-1012, Mar. 2020.

[29]. M. Tolani and R. K. Singh, "Lifetime improvement of wireless sensor network by information sensitive aggregation method for railway condition monitoring", Ad Hoc Netw., vol. 87, pp. 128-145, 2019.