Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Comprehensive Study on Energy-Efficient and Secure Communication Strategies in WSN

[1]N. Keerthikaa, [2]Dr. R. Tamilselvi
1Ph.D Research Scholar (PT), VET Institute of Arts & Science (Co-Ed) College, Thindal, Erode, Tamilnadu,India
2Head & Assistant Professor, VET Institute of Arts & Science (Co-Ed) College, Thindal,Erode ,Tamilnadu,India
keerthini10@gmail.com
rtamilu.sundar@gmail.com

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

Wireless Sensor Networks (WSNs) are group of sensor nodes (SN) distributed in space and linked through wireless communication. WSN include the processors, battery modules and wireless communication devices. SN gathers and transmits the environmental information to BS for efficient processing. WSN includes low-power and low-cost devices for administration because of critical roles of energy as well as security. SN is dependent on batteries that experienced the energy loss with minimum network lifetime. Consequently, energy efficient data broadcast is performed in WSN through optimization methods. Dissimilar researchers performed their research on energy efficient and secured information broadcast by optimization and cryptographic methods in WSN. However, energy consumption was not minimized and data confidentiality rate was not enhanced by existing techniques. The main aim of research work is to reduce energy utilization and increase the network security using cryptographic and optimization techniques.

Keywords: WSN, energy efficient data transmission, cryptography keys, encryption, decryption, network lifetime

I.INTRODUCTION

WSNs comprise the sensor nodes with processors, battery module and wireless communication devices. The nodes gathered and transmitted the environmental information to base stations for efficient processing. WSNs are dynamic networks to increase the capacity for efficient processing and data transmission. WSN used the routing algorithm to increase the Network performance. Clustering is used to perform reliable, flexible and energy-efficient distributed sensor networks. The basic structure of WSN is exposed in Figure 1. It shows the topology of WSN. It comprised the multitude of sensor nodes, central gateway and user access through internet.

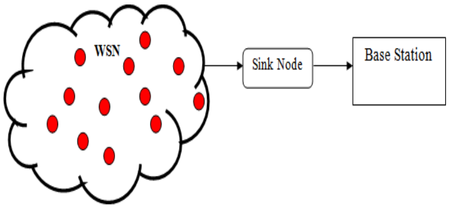


Figure 1 WSN Topology

In WSN, SNs are employed in the sensing area to autonomously gather information points. The nodes communicate through multi-hop manner to gather information at gateway and transmit the collected information to user through internet connectivity.

The main objective of the proposed contribution is provided as:

- To minimize the energy utilization and enhance the network security via cryptographic and optimization techniques
- To minimize the delay, the method of energy efficient data transmission is designed in WSN
- To improve the accuracy, the different sensor nodes used to authentication techniques in WSN
- To achieve the better confidentiality rate, the different secured data transmission methods compared to existing methods

The contents of this manuscript are organized as follows: Section 1 presents the introduction to energy effective as well as secured data broadcast at WSN. Section 2 presents the review of various methods for energy effective as well as secured data transmission in WSN. Section 3 explains the description of methodology. The energy effective and secured data transmission with neat diagram is clearly explained in section 4. Section 5 explains energy effective data broadcast in WSN with different performance metrics. Section 6 explains the secured data transmission methods with the performance metrics. Section 7 concludes the review work.

II. LITERATURE REVIEW

An energy optimization routing was performed [1] with enhanced ABC (EOR-iABC) for cluster based WSN. It chooses efficient cluster heads (CH) within periodic time intervals using distinctive search policy. In order to increase the network data collection efficiency, energy-efficient fitness node was to find optimal path from CH to base station (BS). But, hybrid energy saving algorithm was not employed to optimize the CH selection through mobile sink.

Taylor C-SSA was designed in [2] for energy effective multi-hop routing for cluster head (CH) selection and data transmission in WSN. The sensor nodes send the information over CH to the base station. Also, the trust model was utilized to perform security aware multi-hop routing. But, the multi-hop routing was not employed to attain high performance.

A hybrid Mayfly Optimization Algorithm-Enhanced ACO (MFOA-EACO) was presented [3] to select optimal cluster head (CH). According to determine the optimal route between CH and base station, Enhanced Ant Colony Optimization (EACO) technique was applied thereby, it achieves higher the energy efficiency and network lifetime in WSN. But, the hybrid swarm intelligence technique was not employed to select energy stabilized cluster heads.

An enhanced LEACH technique was developed [4] for energy effective CH selection. The designed technique was carried out random number generation by means of Rank-based CH selection. The selected CHs encompass lots of neighbors inside with lesser energy consumption. But, CH selection with swarm intelligence basis of optimization method failed to enhance energy efficiency and communication quality. Exceptional Key based Node Validation for safe Data broadcast with Asymmetric Cryptography (EKBNV-SDT-AC) method was designed [5] for node validation in WSN. The designed model achieves secure data transmission between source to destination node. However, the hash method was not employed for increasing the key length and security level. An improved dual-phased framework was introduced in [6] for cluster-based routing in WSNs. The designed framework was combination of Sailfish Optimization (SFO) and Spotted Hyena Optimization (SHO) for performing efficient clustering and optimal Cluster Head (CH) selection, respectively. The designed framework increases network performance through addressing energy consumption problems. But, intelligent research framework failed to improve the scalability and adaptability to operate seamlessly in real-time environments. An EKD-SOCBA was developed in [7] to boost up the data security and energy efficiency in WSN. EKD-SOCBA technique performs cluster heads selection and nodes clustering using golden jackal optimization (GJO). In key management, the encryption key maintains lesser energy utilization and overhead. But, EKD-SOCBA failed to perform efficient data aggregation to improve energy efficiency in WSN. Reduced k-means based on ANN (RKM-ANN) was presented [8] for routing depending on rendezvous points (RPs). The performance factors of latency was optimized by RkM-ANN. The DBRkM-ANN identifies delay bound paths for enhancing efficiency and guaranteeing the network coverage using the weight functions and k-means clustering process. But, RKM-ANN and DBRKM-ANN failed to accommodate the non-uniform data generation. A new energy-conscious routing method was presented [9] to optimize energy usage as well as improved network lifetime. The designed method selects the energy efficient cluster heads and optimal routing in network. Also, the designed routing method improves the network lifespan with number of aggregated data packets. However, energy effectiveness was not enhanced while packets traveling to the BS from CHs.

Machine Learning-based Energy Optimization Approach (ML-EOA) was developed [10] to mention energy constraints for efficient data aggregation. The CH selection and data transmission was performed using Artificial Neural Network (ANN). ML-EOA approach attains optimized energy network coverage with minimal latency. Also, it improves data reliability, monitoring and scalability in WSNs. However, optimization and machine learning failed to enhance energy effectiveness as well as data management in WSNs. LEACH Protocol based on Novel Trust Management with Cryptographic RSA algorithm (NTM-LEACH-RSA) was presented [11] to enhance network life span. In NTM-LEACH technique, cluster formation and cluster head election were performed. RSA cryptography technique was applied to protect the data transmission and to ensure data integrity. But meta-heuristic optimization technique was not employed to minimize the energy consumption. A novel hybrid model termed blockchain-machine learning (BC-ML) was presented [12] to combine machine learning for recognizing MNs in WSNs. During data communication, the node was validated by using Schnorr-like zero-knowledge-proof technique. But, BC-ML failed to enhance power efficiency performance. An energy-harvesting Q-learning secure routing method was designed [13] with authenticated encryption. In order to ensure reliable data transmission, physical functions and optimized Q-learning was utilized. The routing node energy value was computed via LSTM based prediction. The designed algorithm achieved maximum packet delivery rate and minimum node energy consumption. However, energy-harvesting Q-learning secure routing method failed to enhance resistance to trust model attack. A lightweight one-way hashing and OR operation was introduced in [14] for security analysis with the session keys. The designed method was more effectively avoids several types of attacks, data loss, forgery and impersonations. However, communication overhead was not minimized by lightweight one-way hashing and OR operation. Randomized Bi-Phase Authentication Scheme (RBAS) was introduced in [15] to improve the external and internal network security. The designed method keeps equilibrium between security measures and energy efficiency through data availability, confidentiality and authenticity handling. Also, it carried out error detection and data authenticity process using advanced hashing, cryptography and dynamic code verification techniques. However, RBAS failed to reduce computational overhead. An optimized Elliptic Curve Cryptographic (ECC) technique called IECC was developed [16] for secured data communication. However, IECC technique failed to minimize energy utilization to enhance network life span. An asymmetric Elliptic Curve Cryptography (ECC) technique was designed [17] through superior energy effectiveness as well as data security. The designed method performs key generation process for providing additional security during the data transmission. Also, it solves different types of security threats as well as side-channel attacks. The proposed asymmetric algorithm achieved minimal time consumption but performance delay was not minimized. A four-stage security level (FS-SSL) was designed [18] for secured data transmission. But, energy utilization performance was not reduced. Whale with Cuckoo Search Optimization-based Quantum Neural Network (WCSO-QNN) integrated through ECC was developed in [19] to accurately detect attacks and to guarantee the data protection through choosing the significant features. Encryption method was used to securely retrieve sensitive data files in the server. However, the processing time of QNN was remained high. RF method was presented in [20] to detect the network attacks and to perform efficient classification. But, the random forest model failed to enhance the applicability across different feature spaces and entities. A robust learning approach was designed in [21] for predicting and detecting hybrid attacks with higher detection accuracy. The security measures were implemented in the network for improving the reliability of information. A smart decision-making process was boost up through reducing number of samples. But, data confidentiality was not enhanced by designed approach. A hierarchical machine learning based hyper-parameter optimization algorithm was designed [22] for categorizing the intrusion through feature selection. However, it failed to enhance the attack detection accuracy through designed algorithm. Novel clustering method was designed [23] to balance energy based on distance, link lifetime, and delay characteristics. The designed clustering method integrates improved particle swarm optimization (PSO) and improved Ant colony optimization (ACO) techniques. The designed clustering method minimizes the cluster head energy consumption using relay nodes. But, security was not considered by clustering algorithm. The lightweight ML recognition method was introduced in [24] with Gini feature selection method to identify the DoS assaults at WSNs. But, attack recognition time was not minimized. A principal component analysis (PCA) and deep convolution neural network (DCNN) technique was developed [25] for DoS traffic anomaly detection in WSNs. The designed method was performs feature extraction in order to prevent feature loss. Also, the number of parameters used in the model was decreased. But, time utilization was not minimized. A novel defense system was designed in [26] to identify the intrusions. But, the designed system failed to provide security protection during effective data broadcast. Cybernet model was presented [27] to find the cyber attack behaviors with high accuracy. The aim of the model was to assess reliability of cybersecurity's and cyber DDoS attacks detection performance efficiency. However, it failed to identify different types of attacks with minimum time consumption. A distributed framework was introduced in [28] to identify diverse cyber attacks. However, attack detection time remained key issue. Adaptive Federated Learning Approach was introduced in [29] to find the DDoS attacks with minimum convergence time and higher classification accuracy. The designed approach was improves training process by means of overcoming cybersecurity applications with unbalanced issues. But, feature selection process in attack detection remained unaddressed. BOA was designed in [30] to choose best CH. A hybrid Energy Efficient Routing with Cluster based Genetic Harris Hawkeye Optimization Algorithm (EER-CGHHOA) is proposed in [31] to preserve the node energy and to find optimal routes. An improved three-factor-based data transmission authentication scheme (TDTAS) is proposed in [32] to offer proper authentication. The secure and energy-efficient clustering and routing techniques are developed in [33] to solve above mentioned issues in the edge-assisted WSN environment. However, packet delivery ratio was not enhanced by BOA. Moreover, it failed to optimize the CH selection through mobile sink by hybrid energy saving algorithm. The routing was difficult to obtain the better performance. The selection of cluster head optimization method was not improving the energy efficiency and communication quality. The energy consumption was failed to reduced and improve the data confidentiality rate by existing techniques. To overcome this issue, the energy utilization was minimized and improves the network security by using proposed cryptographic and optimization techniques.

III. METHODOLOGY

Data trust, data availability, authentication and data integrity are security concerns raised by sensor node deployment. Information security maintenance transmitted over WSN is complicated task due to popularity enhancement. Cryptography keys are employed for node authentication and for safe information transmission. Messages sent between nodes in WSN are encrypted and network has key for encryption and decryption. Each sensor node is allocated with a key set for node validation, encryption and decryption. Secured routing plays important role to address data confidentiality as well as data integrity problems.

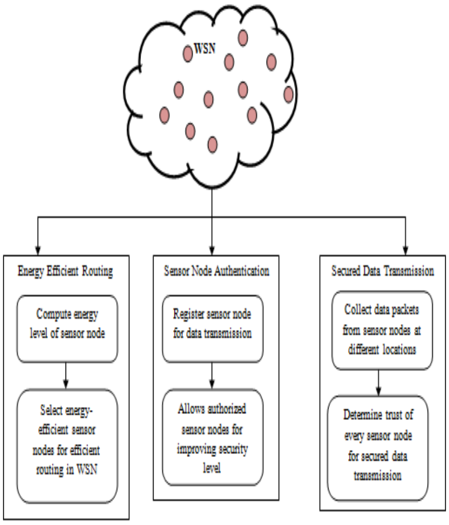

WSN
Energy Efficient Routing
Compute energy level of sensor node
Select energy-efficient sensor nodes for efficient routing in WSN
Sensor Node Authentication
Register sensor node for data transmission
Allows authorized sensor nodes for improving security level
Secured Data Transmission
Collect data packets from sensor nodes at different locations
Determine trust of every sensor node for secured data transmission

Figure 2 Architecture Diagram of Energy Efficient and Secured Data Transmission in WSN

Figure 2 illustrates structural design diagram of energy efficient and secured data broadcast in WSN. Number of SNs is considered as an input. The energy level of SNs is determined for performing energy efficient and secured data broadcast at WSN.

IV. ENERGY EFFICIENT DATA TRANSMISSION

WSN is an important architecture for performing efficient data collection. An integration of WSNs with IoT experienced energy-related challenges because of limited sensor node energy and increased energy utilization for wireless information sharing. An energy-efficient routing protocol is employed for performing reliable transmission and reduced energy consumption. The main aim of optimized energy-efficient routing protocol is improve the network life span and to achieve secured data transmission by identifying the optimal sensor nodes in the network.

A. Hierarchical Cluster based WSN

Technology advancement in WSNs has received large attention in smart computing across different applications. WSN comprised tiny sensor nodes with battery operated. Sensors are restricted to energy consumption. But, energy efficiency remained key problem in WSN routing. But, the existing clustering scheme not balanced the node energy without considering energy parameter. An energy optimization routing using improved artificial bee colony (EOR-iABC) is introduced for cluster based WSN. EOR-iABC routing is used to perform efficient energy optimization and to increase the network lifetime. EOR-iABC performed distinctive search policy through artificial bee colony algorithm for energy efficient cluster heads (CH) selection in regular time intervals through crossover and mutation. The delay convergence is removed through linking the employee and onlooker-bee stages to reform local search. An optimal path from CH to base station (BS) is identified through energy-efficient fitness node to increase the network data collection efficiency. Grenade explosion method (GEM) and Cauchy operator are used to increase the search policies dynamically from one region to another for large-scale WSN.

B. Secure and Energy aware Multi-Hop Routing Protocol

Energy remained as the key problem in WSN environment. Battery-operated sensor nodes in network consumed large quantity of energy during data transmission. Taylor based Cat Salp Swarm Algorithm (Taylor C-SSA) is introduced to address the energy issue through providing the energy efficient multi-hop routing in WSN. The designed technique performed two phases for carry out multi-hop routing, namely CH selection and data transmission. At first, the energy-efficient CH is selected during LEACH protocol for efficient data transmission. The sensor nodes transmitted the data over CH. Then, CH sends data to BS by chosen optimal hop. The optimal hop selection is carried out through Taylor C-SSA. After that, the security aware multi-hop routing is carried out through trust model with indirect trust, integrity factor, direct trust and data forwarding rate. Taylor C-SSA algorithm attained best performance with energy, number of alive nodes, delay and throughput.

C. Mayfly Optimization and Enhanced Ant Colony Optimization

WSNs are group of sensor nodes distributed in space for wireless communication. The sensor nodes collect and store the data about the real-world around them. The sensor nodes dependent on batteries experienced the energy loss that affects network lifetime. Hybrid Mayfly Optimization Algorithm-Enhanced Ant Colony Optimization (MFOA-EACO) is designed to minimum energy utilization and improves the network life span and stability. MFOA-EACO used Mayfly Optimization Algorithm (MFOA) to choose the best cluster head (CH) from collection of nodes. Enhanced Ant Colony Optimization (EACO) technique is employed to discover optimal route between CH as well as base station. Hybrid approach is introduced depending on metrics as number of active and dead nodes, node degree, distance and energy consumption.

D. Energy Efficient Routing with Cluster based Genetic Harris Hawkeye Optimization Algorithm

A wireless sensor network has multifunctional devices that are remotely accessed data in real-time scenarios with higher energy consumption. To solve this issue, hybrid Energy Efficient Routing with Cluster based Genetic Harris Hawkeye Optimization Algorithm (EER-CGHHOA) is proposed to preserve the node energy and to find optimal routes. Genetic based Harris Hawkeye optimization algorithm is used to improve optimal routing with minimum latency and energy consumption. Cluster header selection, and mutation operations are performed to increase network lifetime. Based on fitness calculation, each route is evaluated. Followed by, it only encouraging nodes with higher residual power and to eliminate routes with low fitness.

E. Experimental setting

Experimental evaluation of EOR-iABC, Taylor C-SSA, EER-CGHHOA and MFOA-EACO Method is implemented for Energy Effective Data Routing in WSN using NS3 simulator.

F. Performance Parameters for Energy Effective Data Routing in WSN

There are two performance metrics employed for energy efficient data transmission. They are: energy consumption and delay. Energy consumption is defined as amount of energy utilized by SNs for sensing and effective data broadcast in WSN. It is calculated in joules (J).

$$EC = \sum_{i=1}^{n} Sn_i * EC\ (OSN) \qquad (1)$$

From (1), 'EC' symbolizes the energy consumption, 'n' indicates number of sensor nodes. '$EC(OSN)$' represents energy consumed by one sensor node. The second performance parameter used is delay. It is referred to as dissimilarity among actual arrival time of a data packet at the base station and the observed arrival time of data packets. Therefore, the delay is mathematically calculated as follows,

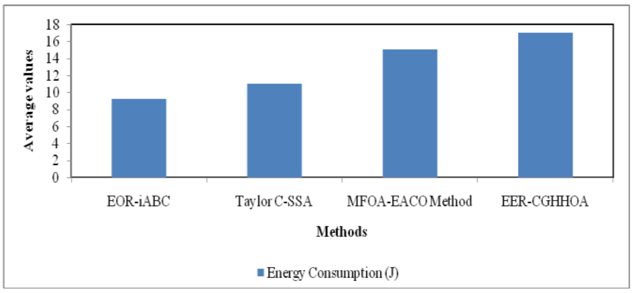
$$Delay = \ Time_{AA}(Dp) - Time_{OA}(Dp) \qquad (2)$$

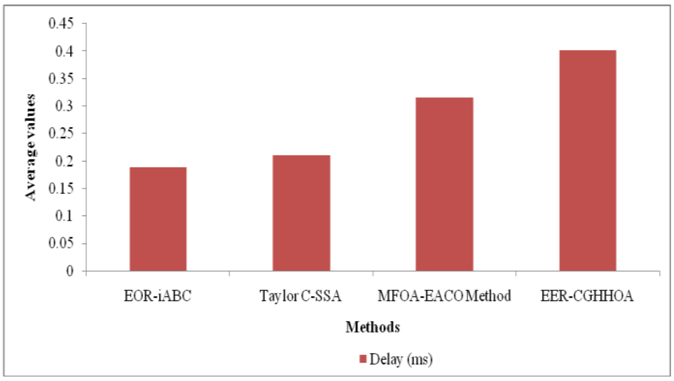
From (2), '$Time_{AA}(Dp)$' represent the actual data packet arrival time. '$Time_{OA}(Dp)$' symbolizes the observed arrival time of information packets. It is calculated in milliseconds (ms). When the delay is lesser, the method is more efficient.

Table 1 Tabulation for Energy Consumption and Delay

Methods/Parameters	**Energy Consumption (J)**	**Delay (ms)**
EOR-iABC	9.2	0.189
Taylor C-SSA	11.05	0.210
MFOA-EACO Method	15	0.315
EER-CGHHOA	17	0.402

Figure 4 (a) (b) shows the measurement analysis of energy consumption and delay for four different existing methods, namely EOR-iABC, Taylor C-SSA, EER-CGHHOA Method and MFOA-EACO.





Result of EOR-iABC is superior to Taylor C-SSA and MFOA-EACO Method. This is owing to with distinctive search policy during ABC method for energy efficient cluster heads (CH) selection through crossover and mutation. The delay is reduced through combining the employee and onlooker-bee stages for local search. EC of EOR-iABC model is reduced by 17%, 39% and 46% than the Taylor C-SSA, MFOA-EACO Method and EER-CGHHOA. The delay is reduced by 10, 40% and 53% than the Taylor C-SSA, MFOA-EACO Method and EER-CGHHOA.

V. SENSOR NODE AUTHENTICATION IN WSN

WSNs are the group of low-power and low-cost devices to gather the data for diverse applications. Wireless networks depend on Medium Access Control (MAC) features for administration due to security constraints. Lightweight cryptographic methods are employed to enhance security stage. Data trust, data availability, authentication and data integrity are security concerns raised by the node development. Cryptographic methods are used to perform secured data broadcast. A node validation process helps in performing secured data broadcast. Cryptography keys are employed for carry out efficient node authentication and secured data transmission.

A. Exceptional Key Based Node Validation

A node validation method is introduced in WSN for safe data broadcast through the characteristics of wireless sensor nodes. The information sent between nodes in WSN is encrypted by using cryptographic keys. The network maintained the key for encryption and decryption. Key management played important role in guaranteeing the WSN safety. Each node is allocated with key set for node validation, encryption and decryption. Secured data transmission in WSN depends on key arrangement in constrained resource setting. A new scheme for protecting sensor data during transmission and after it has been received by nodes. An Exceptional Key based Node Validation for Secure Data broadcast by Asymmetric Cryptography (EKbNV-SDT-AC) model is introduced with node validation, data encryption and data decryption in WSN to securely transmit the data from source to destination.

B. Trust Management with RSA Cryptography Algorithm

WSNs are employed for information gathering and transmission. Network type is employed in numerous relevance's because of low cost and simple communication. Cluster Head (CH) and network overload remained difficult problems for handling different applications. The recommended strategy provides LEACH Protocol based on Novel Trust Management with Cryptographic RSA algorithm (NTM-LEACH-RSA) to enhance network life span with minimum energy consumption. The designed methodology used for enhancing security at WSN. The cluster formation as well as CH election is performed in first phase of NTM-LEACH technique. The threshold value, distance and density between nearby nodes and trust value are employed to select cluster head. Threshold value is determined depending on energy and distance domain. RSA cryptography technique is used in second phase to preserve information through transmission and to enhance data integrity.

C. Efficient Key allocation for Secure and Energy-Optimized Communication

A lightweight key distribution technique is used for preserving security as well as privacy of data transmission with minimum computational overhead and energy consumption. The safe communication is performed to enhance efficacy and trustworthiness in WSNs through preserving valuable energy resources. EKD-SOCBA is developed for WSN. EKD-SOCBA technique is developed to enhance security as well as energy efficiency in WSNs. EKD-SOCBA technique uses the golden jackal optimization (GJO) based clustering approach to gather the nodes and choose the cluster heads (CHs). A lightweight Dynamic Step-wise Tiny Encryption Algorithm (DS-TEA) is introduced to carry out safe data transmission in network. Lightweight key management phase is employed to preserve the encryption key and to reduce the energy utilization and overhead costs.

D. Three-factor-based data transmission authentication scheme

In wireless mobile communication, higher user secrecy attainment is challenge one. An improved three-factor-based data transmission authentication scheme (TDTAS) is proposed to offer proper authentication. The designed authentication scheme for 5G-enabled IoT environments with a fuzzy extractor. As well, TDTA scheme resist numerous known attacks and security features. The Real-or-Random (RoR) model is employed to verify formal security analysis that provides secure against variety of attacks and attains more security features. Also, it ensures key security for enhancing data authentication**.**

E. Experimental setting

Experimental evaluation of EKbNV-SDT-AC model, NTM-LEACH-RSA, EKD-SOCBA technique and TDTAS implemented for Energy Effective Data Routing in WSN using NS3 simulator.

F. Performance Metrics for Sensor Node Authentication in WSN

There are two result metrics employed for sensor node authentication in WSN. They are: sensor node authentication accuracy and authentication time. Sensor node authentication accuracy is defined as ratio of number of sensor nodes which are accurately classified as authenticated nodes. It is calculated in percentage (%) and calculated as,

$$SNAA = \frac{Number\ of\ sensor\ nodes\ that\ are\ accurately\ classified\ as\ authenticated\ nodes}{Number\ of\ sensor\ nodes} * 100 \quad (3)$$

From (3), SN authentication accuracy is computed. When SN authentication accuracy level is higher, technique is more efficient. Sensor node authentication time is described as product of number of sensor nodes and time consumed by one sensor node for authentication in WSN. It is calculated in milliseconds (ms) and calculated as,

$$SNAT = \sum_{i=1}^{n} Sn_i * Time\ (consumed\ by\ one\ sensor\ node) \quad (4)$$

From (4), the SNAT is calculated. When the sensor node authentication time is minimum, technique is more efficient.

Table 2 Tabulation for Sensor Node Authentication Accuracy and Sensor Node Authentication Time

Methods/Parameters	Sensor Node Authentication Accuracy (%)	Sensor Node Authentication Time (ms)
EKbNV-SDT-AC model	98	11
NTM-LEACH-RSA	95	15
EKD-SOCBA technique	92	19
TDTAS	90	23

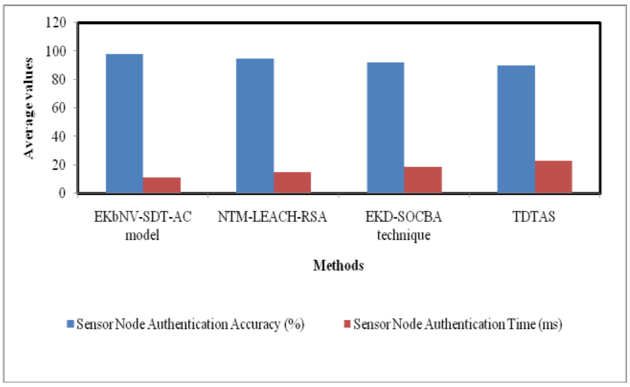


Figure 4 shows the measurement analysis of $SNAA$ and $SNAT$ for three different existing methods, namely EKbNV-SDT-AC model, NTM-LEACH-RSA, EKD-SOCBA technique and TDTAS. The performance of EKbNV-SDT-AC model is higher than NTM-LEACH-RSA and EKD-SOCBA technique. This is because of application of node validation method for secure data broadcast in wireless sensor nodes. The information sent between nodes in WSN is encrypted through cryptographic keys. The network maintained the key for node authentication in WSN. $SNAA$ of EKbNV-SDT-AC model is enhanced by 3% , 7% and 9% than the NTM-LEACH-RSA, EKD-SOCBA technique and TDTAS. The sensor node authentication time is minimized by 27%, 42% and 52% than the NTM-LEACH-RSA, EKD-SOCBA technique and TDTAS.

VI. SECURED DATA TRANSMISSION IN WSN

Secured data transmission in WSNs performed strong key distribution to protect against the malicious attacks and illegal access. Traditional techniques like centralized key management are unreasonable because of resource limitations in large-scale sensor systems.

A. Energy-Optimized Communication in WSN

A lightweight key distribution technique is used for improving security as well as privacy of data transmission with minimum computational overhead and energy consumption. Through optimizing the key distribution devices, the trustworthiness of WSNs performed safe communication while preserving the energy resources. EKD-SOCBA is developed for WSN. EKD-SOCBA technique is developed to enhance security as well as energy efficiency in WSNs. EKD-SOCBA technique used golden jackal optimization (GJO) based clustering approach to group SN and choose CHs. A lightweight Dynamic Step-wise Tiny Encryption Algorithm (DS-TEA) is employed to perform secured data broadcast in network. A lightweight key management phase is employed to preserve the encryption key with minimum energy consumption as well as overhead costs.

B. Block chain Machine Learning Fusion Method

A novel hybrid model termed Block chain-machine learning (BC-ML) is introduced to seamlessly combine the block chain and machine learning (ML) for finding the malicious nodes (MNs) in WSN. BC-ML model introduced an energy-efficient block chain among cluster heads (CHs) for efficient node authentication. Schnorr-like zero-knowledge-proof technique is introduced to validate the node data during communication process. A hybrid lightweight approach with symmetric and asymmetric ciphers increases the security of node data transmission. A new proof-of-authority method is introduced to employ the node digital certificates. The consensus mechanism minimized the processing overhead and increased energy efficiency as well as scalability. A hybrid unsupervised ML technique joined adaptive synthetic sampling with convolutional neural network for efficient node analysis with network features. ML model hosted on data server guaranteed ongoing oversight through CHs selection with security level for detected MNs. BC-ML model is introduced to address the storage and mitigating coordination challenges. BC-ML model detected MNs through optimal resource utilization with minimum delay and higher network lifetime.

C. SE2Bio-CR

In Wireless Sensor Network (WSN) arise lots of issues such as efficiency, security, and network lifetime insufficiency. The secure and energy-efficient clustering and routing techniques are developed to solve above mentioned issues in the edge-assisted WSN environment. Here, four different methods are performed to achieve secure clustering. At first, Quad tree-based structure is build to improve the network management with minimal complication. This designed construction utilized all the sensor nodes. Then, Encryption process is performed to avoid external attacks thereby achieves improved security. Followed by, the Devil Optimization algorithm is applied to carry out CH selection and clustering that provides reliable communication with higher energy efficiency and minimal latency. The Deep Deterministic Policy Gradient process is used to perform duty cycling for improving network lifetime without affecting energy consumption. Finally, the Generative Adversarial Network is applied to perform secure multipath routing.

D. Experimental setting

Experimental evaluation of Lightweight key distribution technique, SE2Bio-CR and BC-ML model is implemented for Energy Effective Data Routing in WSN using NS3 simulator.

E. Performance Metrics for Secured Data Transmission in WSN

There are two performance metrics used for performing secured data transmission is data confidentiality rate, data integrity rate and scalability. The data confidentiality rate is referred ratio of number of data packets which are received by the base station in WSN. It is expressed as,

$$DCR = \left[\frac{n_{AR}}{n}\right] * 100 \qquad (5)$$

From (5), 'DCR' denotes data confidentiality rate. 'n_{AR} ' represents the data received by base station. 'n' symbolizes total number of data packets considered as input. Data integrity rate is ratio of number of data packets that have not been altered or modified by any attack nodes. It is calculated as, From (6), 'DIR' denotes data integrity rate. It is calculated in percentage (%). When the data integrity rate is higher, technique is considered as more efficient.

$$DIR = \frac{\text{Number of data packets not altered by attack nodes}}{\text{Number of data packets}} * 100 \qquad (6)$$

Scalability is the ability of different algorithms to handle different sizes of input data. The quantitative analysis of scalability is measured as given below,

$$S = \left(\frac{D}{n}\right) * 100 \qquad (10)$$

Where 'S' denotes scalability, 'D' denotes the number of data that are correctly detected, 'n' indicates the total input. The scalability is measured in terms of percentage (%).

Table 3 Tabulation of Data Confidentiality Rate, Data Integrity Rate and scalability

Methods/Parameters	Data Confidentiality Rate (%)	Data Integrity Rate (%)	Scalability (%)
Lightweight key distribution technique	92	91	88
SE2Bio-CR	90	89	83
BC-ML Model	95	96	90

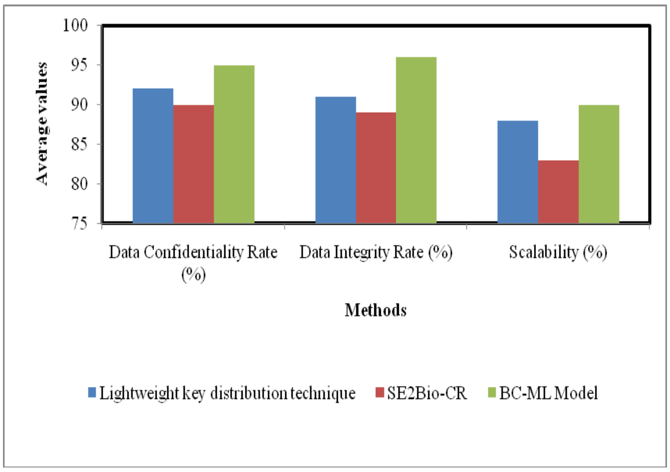


Figure 5 illustrates the measurement analysis of data confidentiality rate and data integrity rate for three different existing methods, namely lightweight key distribution technique and BC-ML model. Result of BC-ML model is superior to lightweight key distribution technique. This is owing to with hybrid unsupervised ML technique with convolutional neural network for efficient node analysis. ML model hosted on data server guaranteed oversight through CHs selection for detected MNs. BC-ML model addressed the storage and mitigating coordination challenges. DCR of BC-ML model is increased by 3% and 6% than the lightweight key distribution technique and SE2Bio-CR. The data integrity rate of BC-ML model is increased by 5% and 8% when compared to lightweight key distribution technique and SE2Bio-CR. The scalability of BC-ML model is increased by 2% and 8% when compared to lightweight key distribution technique and SE2Bio-CR.

7. CONCLUSION

In this study, energy effective routing and secured data transmission through sensor node authentication is performed by twelve different techniques. Different performance parameters are employed to find out energy efficient routing and secured data transmission through sensor node authentication methods. When the result is compared with another study, energy efficient routing and secured data transmission through sensor node authentication using optimization and block chain methods attained better results. Optimization and Block chain methods attain the highest performance result than all the other existing methods techniques. These results strongly propose that blockchain and optimization methods can be implemented in future for energy efficient routing and secured data transmission through sensor node authentication instead of the other conventional methods.

REFERENCES

[1] G. Santhosh and K.V. Prasad, "Energy optimization routing for hierarchical cluster based WSN using artificial bee colony", Measurement: Sensors, Elsevier, Volume 29, October 2023, Pages 1-8

[2] A. Vinitha, M.S.S. Rukmini and Dhirajsunehra, "Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm", Journal of King Saud University - Computer and Information Sciences, Elsevier, Volume 34, Issue 5, May 2022, Pages 1857-1868

[3] V. G. Saranya and S. Karthik, "Bio-Inspired Intelligent Routing in WSN: Integrating Mayfly Optimization and Enhanced Ant Colony Optimization for Energy-Efficient Cluster Formation and Maintenance", CMES - Computer Modeling in Engineering and Sciences, Elsevier, Volume 141, Issue 1, 20 August 2024, Pages 127-150

[4] Bhukya Suresh and G. Shyama Chandra Prasad, "An Energy Efficient Secure routing Scheme using LEACH protocol in WSN for IoT networks", Measurement: Sensors, Elsevier, Volume 30, December 2023, Pages 1-18

[5] Bhanu Priyanka Valluri and Nitin Sharma, "Exceptional key based node validation for secure data transmission using asymmetric cryptography in wireless sensor networks", Measurement: Sensors, Elsevier, Volume 33, June 2024, Pages 1-18

[6] Michaelraj Kingston Roberts, Jayapratha Thangavel and Hamad Aldawsari, "An improved dual-phased meta-heuristic optimization-based framework for energy efficient cluster-based routing in wireless sensor networks", Alexandria Engineering Journal. Elsevier, Volume 101, August 2024, Pages 306-317

[7] Adil O. Khadidos, Nawaf Alhebaishi, Alaa O. Khadidos, Mohammed Altwijri, Ayman G. Fayoumi, and Mahmoud Ragab, "Efficient key distribution for secure and energy-optimized communication in wireless sensor network using bio-inspired algorithms", Alexandria Engineering Journal, Elsevier, Volume 92, April 2024, Pages 63-73

[8] Muhammad Salman Qamar, Ihsan ul Haq, Amil Daraz, Atif M. Alamri, Salman A. AlQahtani and Muhammad Fahad Munir, "A Novel Approach to Energy Optimization: Efficient Path Selection in Wireless Sensor Networks with Hybrid ANN", Computers, Materials and Continua, Elsevier, Volume 79, Issue 2, 15 May 2024, Pages 2945-2970

[9] Tadele A. Abose, Venumadhav Tekulapally, Ketema T. Megersa, Diriba C. Kejela, Samuel T. Daka and Kehali A. Jember, "Improving wireless sensor network lifespan with optimized clustering probabilities, improved residual energy LEACH and energy efficient LEACH for corner-positioned base stations", Heliyon, Elsevier, Volume 10, Issue 14, 30 July 2024, Pages 1-15

[10] I. Surenther, K.P. Sridhar and Michaelraj Kingston Roberts, "Enhancing data transmission efficiency in wireless sensor networks through machine learning-enabled energy optimization: A grouping model approach", Ain Shams Engineering Journal, Elsevier, Volume 15, Issue 4, April 2024, Pages 1-15

[11] S. Anitha, S. Saravanan and A. Chandrasekar, "Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission", Measurement: Sensors, Elsevier, Volume 29, October 2023, Pages 1-15

[12] Osama A. Khashan, "Blockchain-machine learning fusion for enhanced malicious node detection in wireless sensor networks", Knowledge-Based Systems, Elsevier, Volume 304, November 2024, Pages 1-15

[13] Cuiran Li, Jixuan Wu, Zepeng Zhang and Anqi Lv, "Energy-harvesting Q-learning secure routing algorithm with authenticated-encryption for WSN", ICT Express, Volume 9, Issue 6, December 2023, Pages 1077-1084

[14] Vincent Omollo Nyangaresi and Ganesh Keshaorao Yenurkar, "Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks", High-Confidence Computing, Elsevier, Volume 4, Issue 2, June 2024

[15] Pendukeni Phalaagae, Adamu Murtala Zungeru, Boyce Sigweni, Selvaraj Rajalakshmi, Herbet Batte and Odongo S. Eyobu, "An energy efficient authentication scheme for cluster-based wireless IoT sensor networks", Scientific African, Elsevier, Volume 25, September 2024, Pages 1-15

[16] Esau Taiwo Oladipupo, Oluwakemi Christiana Abikoye, Agbotiname Lucky Imoize, Joseph Bamidele Awotunde, Ting-Yi Chang, Cheng-Chi Lee, and Dinh-Thuan Do, "An Efficient Authenticated Elliptic Curve Cryptography Scheme for Multicore Wireless Sensor Networks", IEEE Access, Volume 11, 2023, Pages 1306 – 1323

[17] Shabana Urooj, Sonam Lata, Shahnawaz Ahmad, Shabana Mehfuz, S Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network", Alexandria Engineering Journal, Elsevier, Volume 72, 2023, Pages 37-50

[18] Uras Panahi and, Cuneyt Bayilmıs, "Enabling secure data transmission for wireless sensor networks based IoT applications", Ain Shams Engineering Journal, Elsevier, Volume 14, Issue 2, 2023, Pages 1-11

[19] Heba Kadry, Ahmed Farouk, Elnomery A. Zanaty, Omar Reyad, "Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security", Alexandria Engineering Journal, Elsevier, Volume 71, 2023, Pages 491-500

[20] Tijana Markovic, Miguel Leon, David Buffoni, Sasikumar Punnekkat, "Random forest with differential privacy in federated learning framework for network attack detection and classification", Applied Intelligence, Springer, Volume 54, 2024, Pages 8132–8153

[21] D. Adhimuga Sivasakthi, A. Sathiyaraj, Ramkumar Devendiran, "HybridRobustNet: enhancing detection of hybrid attacks in IoT networks through advanced learning approach", Cluster Computing, Springer, Volume 27, 2024, Pages 5005–5019

[22] Sandeep Dasari and Rajesh Kaluri, “An Effective Classification of DDoS Attacks in a Distributed Network by Adopting Hierarchical Machine Learning and Hyperparameters Optimization Techniques”, IEEE Access, Volume 12, 2024, Pages 10834 – 10845

[23] P. Suman Prakash, D. Kavitha and P. Chenna Reddy, “Delay-aware relay node selection for cluster-based wireless sensor networks”, Measurement: Sensors, Elsevier, Volume 24, December 2022, Pages 1-15

[24] Muawia A. Elsadig, “Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach”, IEEE Access, Volume 11, August 2023, Pages 83537 – 83552

[25] Chengpeng Yao, Yu Yang, Kun Yin, and Jinwei Yang, “Traffic Anomaly Detection in Wireless Sensor Networks Based on Principal Component Analysis and Deep Convolution Neural Network”, IEEE Access, Volume 10, September 2022, Pages 103136 – 103149

[26] Antonio Paya, Sergio Arroni, Vicente García-Día, Alberto Gómez, “Apollon: A robust defense system against Adversarial Machine Learning attacks in Intrusion Detection Systems”, Computers &amp; Security, Elsevier, Volume 136, 2024, Pages 1-13

[27] Azar Abid Salih and Maiwan Bahjat Abdulrazaq, “Cybernet Model: A New Deep Learning Model for Cyber DDoS Attacks Detection and Recognition”, Computers, Volume 78, Issue 1, 2024, Pages 1275-1295

[28] Olivia Jullian, Beatriz Otero, Eva Rodriguez, Norma Gutierrez, Héctor Antona &amp; Ramon Canal, “Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework”, Journal of Network and Systems Management, Springer, Volume 31, 2023, Pages 1-24

[29] Roberto Doriguzzi-Corin, Domenico Siracusa, “FLAD: Adaptive Federated Learning for DDoS Attack Detection”, Computers &amp; Security, Elsevier, Volume 137, 2024, Pages 1-16

[30] Prachi Maheshwari, Ajay K. Sharma, Karan Verma, “Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization”, Ad Hoc Networks, Elsevier, Volume 110, January 2021, Pages 1-15

[31] J. Jayachandran and K. Vimala Devi, “EER-CGHHOA: A Hybrid Genetic Algorithm Driven Dynamic Clustering for Energy Efficient Routing in Border Surveillance WSNs”, IEEE Access, Volume 12, August 2024, Pages 108185 - 108200

[32] K. H. Vijayendra Prasad and Sasikumar Periyasamy, “Secure-Energy Efficient Bio-Inspired Clustering and Deep Learning-Based Routing Using Blockchain for Edge Assisted WSN Environment”, IEEE Access, Volume 11, December 2024, Pages 145421 – 145440

[33] Shreeya Swagatika Sahoo, Sujata Mohanty, Kshira Sagar Sahoo, Mahmoud Daneshmand , and Amir H. Gandomi, “A Three-Factor-Based Authentication Scheme of 5G Wireless Sensor Networks for IoT System”, IEEE Internet of Things Journal, Volume: 10, Issue: 17, September 2024, Pages 15087 - 15099