SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Towards Secure Data Transfer: Novel Approach For Route Selection And Attack Identification In Wireless Sensor Network Cyber Security

Dr. C Pandeeswaran[1] , B. Muthuraj[2]

[1]Professor, Department of ECE, Green Electronics , Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS) Chennai 602105, TN, India. pandeeswaranc.sse@saveetha.com
[2]Professor, Department of EEE Panimalar Engineering College Chennai-600123 muthurajbose@gmail.com

Abstract
Route selection in wireless sensor network (WSN) cybersecurity involves selecting safe routes for data transfer, whereas attack detection searches and eliminates any potential risks or criminal activity in the network to protect communication integrity and dependability. In this paper, we select the secure node and then select the optimal path using Quasi-Bee Reflection Optimization (QBRO). We gathered the NSL-KDD dataset from Kaggle and we proposed Fine-tuned Elman neural network (FTENN) as a classification method for detecting the attack in WSN, then transferring the non-attack data with secure using fine-tuned ElGamal Cryptography algorithm (FTEC). As a result, we evaluate the performance of our proposed method and compare it with the existing method. Our proposed approach demonstrates superior performance in cybersecurity selecting the optimal path, classification and data transfer compared to existing methods.

Keywords: wireless sensor network (WSN), cybersecurity, optimal path, Quasi-Bee Reflection Optimization (QBRO), Fine-tuned Elman neural network (FTENN) and Fine-tuned ElGamal Cryptography algorithm (FTEC).

1. Introduction

Route selection is a critical component of wireless sensor networks (WSNs) which serves to maintain network security while providing effective and dependable data transfer. Route selection algorithms choose the best paths for data packet transfer from source to destination nodes by considering factors including packet delivery ratio, energy efficiency and network structure. Secure route selection intends to lessen security risks such as data manipulation, routing assaults and listening [1].

Recognizing and countering Wormhole attacks is an essential part of WSN cybersecurity. In a Wormhole attack, two malicious nodes work together to create a virtual connection that allows packets to be traversed through a shortcut and around standard routing protocols. It provides the attackers the ability to intercept or change the data that are transmitted, obstruct communication, or carry out other assaults [2].

In general, network architecture analysis, packet transmission delay monitoring and methods for identifying anomalies are used to find unusual activity to detect Wormhole assaults [3]. Secured protocols for routing, cryptographic authorization and segmentation of networks are countermeasures against Wormhole attacks that help to lessen the attack's impact.

Researchers and practitioners concentrate on creating sophisticated cryptography algorithms, compact authenticating processes and systems for intrusion detection that are appropriate to the limited resources nature of WSNs to increase the path safety of route selection and combat Wormhole attacks in WSNs [4]. Furthermore, by recognizing and preventing attacks at the physical layer, the application of security measures

at the physical layer techniques, such as channel characteristics analysis and identification based on signal intensity, can support conventional security efforts [5].
Wormhole attack detection and prevention techniques are necessary to address the problems in wireless sensor networks [6]. Secure localization techniques, which are capable of accurately identifying the actual positions of the sensor nodes, contribute greatly to limiting the construction of unwanted networks. The multimodal strategy attempts to improve the entire security architecture of WSN against both known and future threats [7].
The purpose of this paper is to strengthen WSN cybersecurity through Quasi-Bee Reflection Optimization (QBRO) as a selection of optimal paths, Fine-tuned Elman neural network (FTENN) as a classification and Fine-tuned ElGamal Cryptography algorithm (FTEC) for transferring the data with security.
Part 2 provides related work, part 3 discusses the methodology, part 4 represents the result as well as discussion and part 5 discusses the conclusion of the paper.

2. Related Works

Study [8] proposed employing a Strategic Security System (SSS) in both static and dynamic global WSNs to identify duplicate locations. A random-walk-based method for detecting cloning attempts and single state memory random walk with networks divisions (SSRWND) were features of the current system (Random Walk (RAWL)). Considering improved detection accuracy, the proposed approach required less memory.
Study [9] proposed a deep neural network (DNN) based detection of intrusion solution. The best characteristics of the collection of data were using the cross-correlation procedure and the variables were employed as the foundation for a DNN architecture that detects intrusions. The experimental findings demonstrated that the proposed method effectively detected attacks and outperformed traditional machine learning models including support vector machines, decision trees and random forests.
Study [10] proposed an optimized multilayer perception artificial neural network (MLPANN) for security, detection and location against numerous threats. The two main components of the suggested approach were machine learning and localized methods for detecting and locating WSN, coupled with DoS attacks. The simulation's outcomes show how well the suggested method works to identify and safely localize dangerous threats on regularly distributed, scaled wireless sensor networks and the outcome was a higher average localization accuracy and maximum localization error.
A WSN technique for DDoS using a Spotting Hyenas Optimization with Quantum Neural Networks- Attack Classification (SHOQNN-AC) was developed in study [11]. The SHOQNN-AC technique used a min-max scaler to do the data scaling procedure to achieve the objective. The Benchmark WSN-DS dataset was used to assess the SHOQNN-AC technique's effectiveness evaluation. The results of the experiment show the importance of the SHOQNN-AC algorithm in comparison to other models.
The ability to identify instances of flooding attacks served as the foundation for the adaptive neural fuzzy inference system (ANFIS) and the fuzzy inference system has been applied in study [12]. The proposed approach was contrasted with the current approaches. The simulation research's findings show that the proposed method enhanced the lifespan and efficiency of the sensor nodes while detecting flooding threats.
In order to identify denial-of-service (DoS) assaults in WSNs, an effective artificial intelligence detection method using a Gini feature selection and the decision tree (DT) method in study [13]. An enhanced version of the WSN-DS data was used to train and assess the proposed approach. In comparison to other methods, the proposed approach has demonstrated good performance by obtaining an accuracy rate with low costs.
Study [14] focused on detecting DDoS attacks in WSNs using artificial intelligence. They evaluated five artificial intelligence methods with the CIC-IDS2017 dataset, one of which was the random forest classifier. Improving WSN security was one of the practical implications of the high accuracy. The research's identification of potential flaws and suggestions for improvements in the future were crucial components.
Study [15] proposed a new model for detecting breaches in WSNs named the “Stacking convolutional neural network with bidirectional long short-term memory (SCNN-Bi-LSTM)”. Federated learning (FL) was used in the framework to protect privacy and improve intrusion detection efficiency. The suggested method FL-SCNN-BiLSTM technique showed a superior rate of detection for complicated and unidentified assaults than conventional Artificial Deep Neural Network (ADNN) models, greatly enhancing IDS performance.
Study [16] offered a cluster-based identification strategy method coupled with a distributed unscented kalman filter (DUKF) for estimating the state in the presence of intentional network attacks. Four steps were measured to get a good estimate of the scenario when the secure node's data was unidentified: revision, cluster-based

attractiveness identification, data fusion and predictions. The method's resilience against random, FDI, reverse and delayed assaults was further demonstrated by the simulation findings.
Study [17] introduced a portable, multi-layer artificial intelligence detection technique created to prevent assaults directed toward WSN. Four network-layer local DoS assaults that were seen in the WSN-DS sample can be identified by the proposed approach. When an attack happens, the monitoring nodes identify the event and the mobile robot proceeded to the affected cluster to forward the updates to the base station (BS) for more investigation and second-layer detection.
Study [18] proposed a deep learning-based cyberattack detection mechanism for WSNs. The Message Queuing Telemetry Transport (MQTT) protocol-dependent data transmission and the WSN node's behavior were both adopted by this strategy. The outcomes show that, according to the dataset, the efficiency of combining deep learning LSTM approaches was 96.02% for precision in training and 95.08% for validating performance.
In order to determine the best measures to identify malicious and security threats utilizing block-chain technology, a new strategy that makes use of heuristics, signatures and voting detection techniques was developed in study [19]. To identify the rogue sensor nodes in the proposed method, the cluster head node (CN) uses three Blockchain-based detection mechanisms. The total findings statistic demonstrated that during the simulation of the technique, a higher percentage of malicious messages were recognized and identified.
A lightweight intelligent intrusion detection model for WSN was proposed in study [20] and combining the sine cosine algorithm (SCA) with a k-nearest-neighbor (kNN) method can dramatically lower the false alarm rate and increase the precision of classification, allowing for the intelligent detection of a wide range of threats, even unknown attacks. The intended detection of intrusions algorithm produced acceptable outcomes.

3. Methodology

In this section, we provide a comprehensive explanation of secure node selection, optimal path selection using QBRO, classification using FTENN and securely transfer non attack data using FTEC. Figure 1 illustrates the entire progression of the methodology.

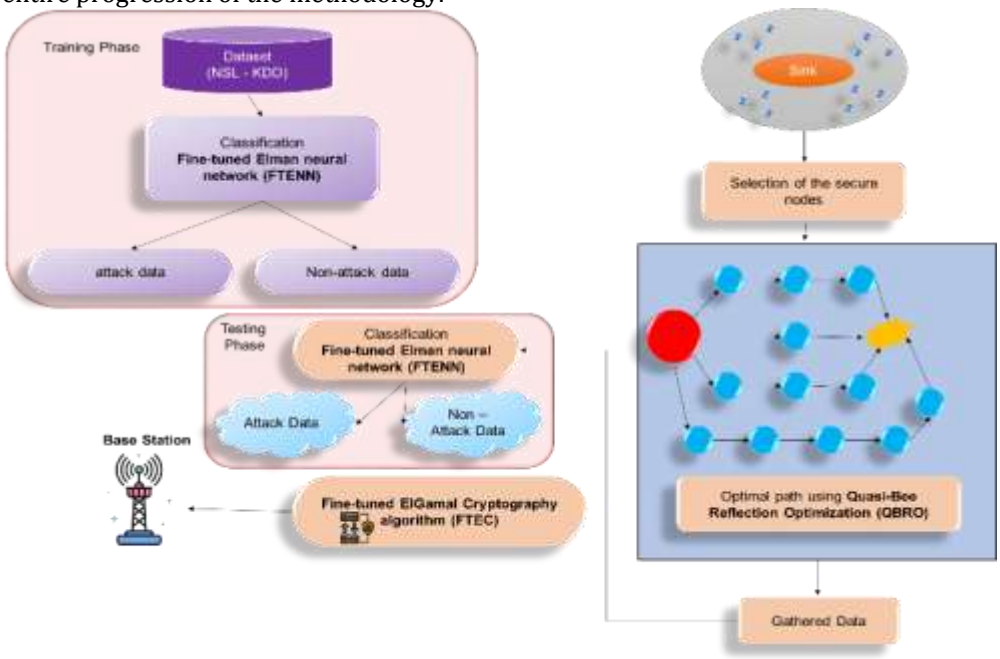

Figure 1: Process of methodology

3.1. Configuring a Network

A significant portion of the dispersed network's sensors are deployed uniformly and arbitrarily. Assuming a set of MT, denoted as follows, a network with multiple hops is considered:

$$MT = \{mt_1, mt_2, mt_3, \ldots . mt_n\} \quad (1)$$

In this case, mt_n denotes the n-number of the MT and TM denotes the multi-hop connection. The network also contains a single BS.

3.2. Node selection

In a WSN, selecting secure nodes requires carefully evaluating them according to several factors. Confidence, safe initialization, energy-security compromises and detection of intrusions abilities are some of the elements that are considered throughout this evaluation process. Nodes are selected according to their dependability, ability to be securely configured during deployment, ability to balance security and energy efficiency concerns, along with the ability to effectively monitor network traffic for possible intrusions. The objective is to choose nodes that support a stable and secure network environment.

3.3. Selecting optimal path using Quasi-Bee Reflection Optimization (QBRO)

Due to the fundamental characteristics that set WSNs apart from all other wireless connections, including cellular networks and ad hoc mobile networks, path selection is far more difficult in these networks. The suggested method, named Quasi-Bee Reflection Optimization (QBRO), was inspired by the added improvements to select the optimal path. QBRO is a combination of Quasi-reflection-based learning (QRL) and artificial bee colony (ABC).

3.3.1. Artificial Bee Colony (ABC)

The ABC is an algorithm for evolution that derives inspiration from honeybee intelligence. When dealing with multi-modal and noisy optimization situations, the ABC method has proven to generate optimal solutions. It is an iterative process, similar to other swarm-based methods. A collection of randomly created foods or solutions is the starting point. The subsequent actions are carried out up until a termination requirement is satisfied.

3.3.1.1. Establishing the group's initial state

The total number of M_O sources of food is initialized as the first stage in the procedure

$$w_{ji} = k_i + \text{rand}(0,1).(v_i - k_i),$$
$$i = 1,2,\dots,c; j = 1,2,\dots,M_O, \quad (2)$$

Where w_{ji} denotes a source of food, j is the j-th food source and i is the searching space's i -th dimensions. The lowest limit in every dimension is denoted by k_i and the upper limit is indicated by v_i. In the remaining section, the indexes j and i will be utilized under the same definition.

3.3.1.2. Distribute engaged bees

The quantity of these bees is proportional to the number of food resources, the employed bees are utilized to produce novel solutions.

$$A_{ji} = w_{ji} + \emptyset_{ji}(w_{ji} - w_{li}), \forall\, j \neq l$$
$$l \in rand\{1, M_O\}, i\epsilon\{1,2,\dots,c\} \quad (3)$$

To produce a novel source of food utilizing the employed bee manager, an l source of food in the i dimension is randomly chosen. The variable A_{ji} is an arbitrary number chosen among [1, 1], where j is a number corresponding to the j-th feeding resource and i is the dimensions issue index. The value of fitness is employed to assess the caliber of a food resource. It can be produced for a reduction issue by applying the expression that follows:

$$fit_j = \begin{cases} \frac{1}{1+i_j} & if\ i_j \geq 0 \\ 1 + abs(i_j) & if\ i_j \geq 0 \end{cases} \quad (4)$$

Here i_j represents the value of the function of the objective concerning the potential solution w_{ji}.

3.3.1.3. Observer bees choose the food sources

The amount of bees who are watching and the quantity of food sources must first be explained to fully understand the observer phase.

$$prob_j = \frac{fit_j}{\sum_{j=1}^{M_O} fit_j} \quad (5)$$

fit_j, which is associated with the food source's objective function, represents the fitness score of the j -th source of nourishment in this instance.

3.3.1.4. Identify the scavenger bees

The scouting bee procedure is the last phase. In this instance, the bees are used to modify a food supply that has been deemed unsuitable for improvement based on a predefined trial limit number. In this case, the food item is modified by an observer bee rather than being abandoned.

3.3.2. Quasi-reflection-based learning (QRL)

It is a powerful tool that can enhance exploration, exploitation balancing and speed of convergence. The following process generates the quasi-reflected constituent i of equation w, w_i^{rq}:

$$w_i^{rq} = rnd\left(\frac{ka_i + ka_i}{2}, w_i\right) \quad (6)$$

Where the lowest limit (ka_i) and higher bound (ka_ij) of the average of the i -th element are written as $\frac{ka_i+ka_i}{2}$ and $rnd\left(\frac{ka_i+ka_i}{2},\ w_i\right)$ produces randomized integer from normal distributions in range $\left(\frac{ka_i+ka_i}{2}, w_i\right)$.

3.4. Classification using Fine-tuned Elman neural network (FTENN)

A Fine-tuned Elman neural network (FTENN) outperforms a standard Elman neural network (ENN) in terms of its learning effectiveness when the output layer's feedback is considered. The input and contextual synapses' outputs feed the hidden layer neurons in a typical ENN. A typical ENN has inadequate speed and precision of resolution since it solely uses concealed contextual nodes to spread the message. The input layer (j layer), contextual layer (q layer), secret layer (i layer) and output layer (p layer) of the suggested FTENN, which has a pair of inputs along with a single output. The following introduces each layer's fundamental purpose and method of signal transmission:

Each node's input and output are expressed as in Level 1 (input layer).

$$W_j(l) = e_j\left(net_j\right) = net_j = f_j(l) \quad (7)$$

Where l denotes the l th repetition as well as $f_j(l)$ and $W_j(l)$ are the inputs and outputs of the level of the input, correspondingly.

The node inputs and outputs are shown as in Level 2 (secret layer).

$$W_i(l) = T(net_j) \quad (8)$$

$$net_i = \sum_j x_{ji} W_j(l) + \sum_q x_{qi}\, W_q^d\ (l) \quad (9)$$

Where $W_i(l)$ and net_j represent the secret layer's inputs and outputs, accordingly and x_{qi} represents the contextual layer's output. x_{ji} and x_{qi} are the connection strengths that connect input synapses to neurons that are concealed and contextual neurons to secret neurons, correspondingly.

The node inputs and outputs are expressed as in Level 3 (contextual layer).

$$W_q^d(l) = \gamma W_q^d(l-1) + W_i(l-1) \quad (10)$$

Where the self-connecting return increase is $0 \le \gamma < 1$.

The node inputs and outputs are expressed as in Level 4 (output layer).

$$z_p(l) = e\left(net_p(l)\right) = net_p(l), \quad (11)$$

$$net_p(l) = \sum_i x_{ip}\, w_i(l) + x_p z^d(l), \quad (12)$$

$$z^d(l) = \varsigma z^d(l-1) + z_p(l-1) \quad (13)$$

where $0 \le \varsigma < 1$ is the self-connecting suggestions accomplished, $z_p(l)$ is the output of the FTENN and the controlling attempt of the suggested controller, $z^d(l)$ is the output of the feedback signal from the output neurons and wjo and wo are the connective tissue weights of the neurons that are hidden to the neurons that output and the produce suggestions neurons to the output neurons, correspondingly.

3.5. Safe Transfer of Data

The safe transmission of the non-attack data begins once the WSN values are verified by the Work Area Definition (WAD) system that has been trained previously. Here, we utilize fine-tuned ElGamal Cryptography algorithm (FTEC) to transfer the data securely. Every sensor node produces a set of private and public keys, with public keys being shared openly. A node employs the recipient's public key for encryption which involves random numbers and modular mathematical operations when it wishes to transmit an alert to a different node. After that, the encrypted text is sent and it can be decrypted and the initial text is recovered by the sender who has the corresponding secret key. ElGamal's asymmetric design makes it appropriate for devices in WSNs with limited resources, but given the computational and power limits associated with these networks, effective management of keys is essential. The maintenance of information security in the WSN is dependent upon the secure transmission of public keys [23].

4. Result And Discussion

In this paper, the Python platform has been used to implement the proposed method. We need a laptop with 32 GB of RAM, a 100 GB hard drive, an Intel i7 processor and Windows 10. We gather the NSL-KDD dataset from Kaggle (https://www.kaggle.com/code/jalindarkarande/nsl-kdd-security-attack-detection/notebook). We compared our proposed method to the existing method K- nearest neighbor (KNN), Decision tree (DT) and Particle Swarm Optimization with an Artificial Neural Network (PSO+ANN) [21].

Accuracy refers to the precision and correctness of attack detection in WSN to provide accurate and reliable outcomes. Figure 2 displays the performance of accuracy. The existing method, KNN, DC and PSO+ANN attained 85%, 80% and 97.5%, respectively. Compared to the existing method, our proposed method achieved 98% accuracy.

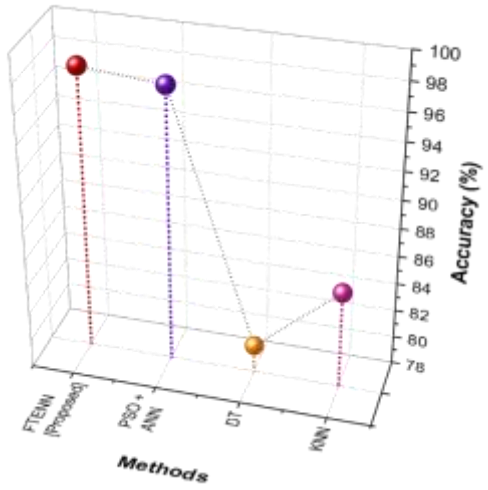

Figure 2: Performance of accuracy

The model's ability to accurately identify real negatives among all real negatives is measured by its specificity. Figure 3 shows the evolution of specificity. The existing method, KNN, DC and PSO+ANN attained 83%, 72% and 95%, respectively. Compared to the existing method, our proposed method achieved 97% specificity.

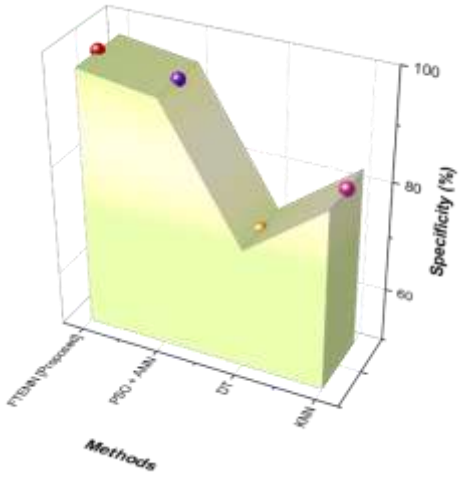

Figure 3: Evolution of specificity

Sensitivity, which is referred to as recall or true positive rate, is a statistic used in the context to detect the attack in WSN. Figure 4 displays the performance of sensitivity. The existing method, KNN, DC and PSO+ANN attained 86.5%, 82% and 96%, respectively. Compared to the existing method, our proposed method achieved a 97.5% sensitivity level.

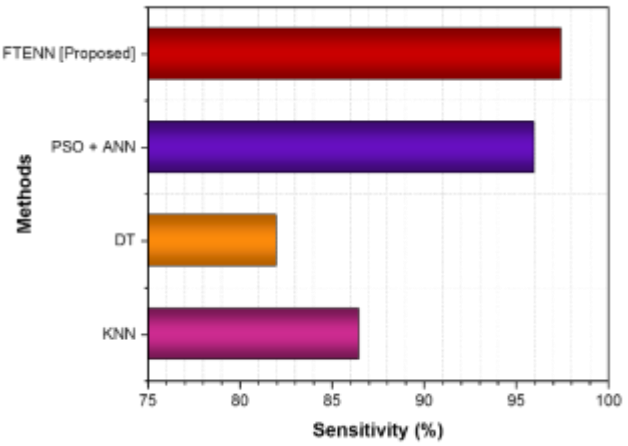

Figure 4: Performance of sensitivity

The outcomes indicate that the proposed method demonstrates better performance in comparison to the existing method.
Regarding encryption and decryption time, our proposed method (FTEC) is compared with the existing method data encryption standard (DES), Blowfish algorithms (BF) and advanced encryption standard (AES) [22].
Encryption time is used to describe the amount of time it requires to encrypt an instance of information or data. Figure 5 displays encryption time. We evaluate the time based on the data size (20KB, 40KB, 60KB, 80KB and 100KB). The existing method AES, DES and BF attained (3s, 5s, 8s, 11s and 14s), (1s, 3s, 5s, 8s and 10s) and (1s, 2s, 4s, 6s and 8s), respectively. Compared to the existing method, our proposed method (FTEC) attained (1s, 1s, 3s, 5s and 6s), respectively.

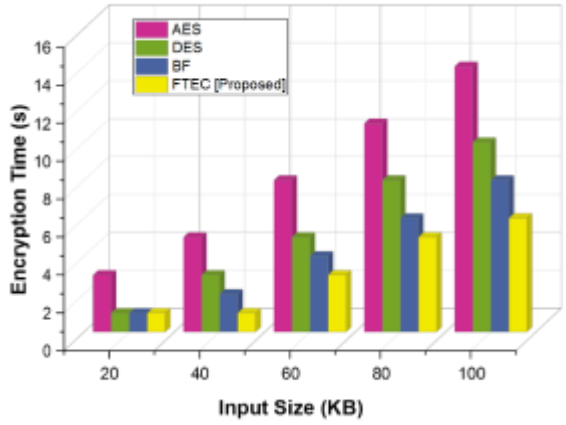

Figure 5: Encryption time

The time required to decrypt encrypted data and return it to its initial, readable state is referred as the decryption time. Figure 6 displays the decryption time. We evaluate the time based on the data size (20KB, 40KB, 60KB, 80KB and 100KB). The existing method AES, DES and BF attained (3s, 7s, 9s, 9s and 15s), (2s, 4s, 7s, 9s and 11s) and (2s, 3s, 3s, 7s and 9s), respectively. Compared to the existing method, our proposed method (FTEC) attained (1s, 2s, 3s, 5s and 7s), respectively.

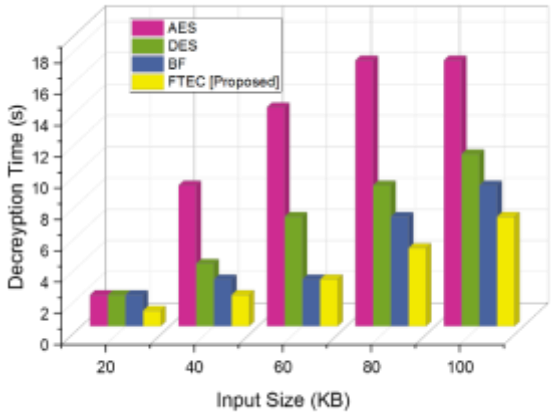

Figure 6: Decryption time

The results show that, when compared to the existing method, the proposed method performs superior.

5. Conclusion

In wireless sensor network (WSN) cybersecurity, route selection is the process of choosing secure paths for data transfer, while attack detection monitors for and removes any possible threats or illegal activities from the network to safeguard communications reliability and authenticity. We select the secure node and then select the optimal path using Quasi-Bee Reflection Optimization (QBRO). We gathered the NSL-KDD dataset from Kaggle and we introduced Fine-tuned Elman neural network (FTENN) as a classification method for detecting the attack in WSN, then transferred the no attack data with a secure used Fine-tuned ElGamal Cryptography algorithm (FTEC). As a result, we evaluated the performance of our proposed method and compared it with the existing method based on the matrices such as accuracy (98%), specificity (97%), sensitivity (97.5%), encryption (1s, 1s, 3s, 5s and 6s) and decryption time (1s, 2s, 3s, 5s and 7s). Our proposed approach demonstrates superior performance in cybersecurity selecting the optimal path, classification and data transfer compared to existing methods. The dataset, might not accurately reflect the variety and dynamic character of actual cyber threats in WSN. The proposed cybersecurity strategy for WSN will be improved in the future by incorporating cutting-edge machine-learning techniques.

Reference

1. Behiry, M.H. and Aly, M., 2024. Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods. Journal of Big Data, 11(1), p.16.
2. Liu, J., Tang, Y., Zhao, H., Wang, X., Li, F. and Zhang, J., 2024. Cps attack detection under limited local information in cyber security: An ensemble multi-node multi-class classification approach. ACM Transactions on Sensor Networks, 20(2), pp.1-27.
3. Meenakshi, B. and Karunkuzhali, D., 2024. Enhancing cyber security in WSN using optimized self-attention-based provisional variational auto-encoder generative adversarial network. Computer Standards & Interfaces, 88, p.103802.
4. Meleshko, A. and Desnitsky, V., 2024, February. The Modeling and Detection of Attacks in Role-Based Self-Organized Decentralized Wireless Sensor Networks. In Telecom (Vol. 5, No. 1, pp. 145-175). MDPI.
5. Jagwani, N. and Poornima, G., 2024. Machine Learning Algorithms to Detect Attacks in Wireless Sensor Networks. International Journal of Intelligent Systems and Applications in Engineering, 12(13s), pp.417-431.
6. Goud, B.H., Shankar, T.N., Sah, B. and Aluvalu, R., 2024. Energy optimization in path arbitrary wireless sensor network. Expert Systems, 41(2), p.e13282.
7. Bhatti, D.S., Saleem, S., Imran, A., Kim, H.J., Kim, K.I. and Lee, K.C., 2024. Detection and isolation of wormhole nodes in wireless ad hoc networks based on post-wormhole actions. Scientific Reports, 14(1), p.3428.

8. Sujihelen, L., Boddu, R., Murugaveni, S., Arnika, M., Haldorai, A., Reddy, P.C.S., Feng, S. and Qin, J., 2022. Node replication attack detection in distributed wireless sensor networks. Wireless Communications and Mobile Computing, 2022, pp.1-11.
9. Gowdhaman, V. and Dhanapal, R., 2022. An intrusion detection system for wireless sensor networks using deep neural network. Soft Computing, 26(23), pp.13059-13067.
10. Gebremariam, G.G., Panda, J. and Indu, S., 2023. Localization and detection of multiple attacks in wireless sensor networks using artificial neural network. Wireless Communications and Mobile Computing, 2023.
11. Murugesh, C. and Murugan, S., 2023, February. Modelling of Optimal Quantum Neural Network for DDoS Attack Classification in Wireless Sensor Networks. In 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS) (pp. 1054-1059). IEEE.
12. Beslin Pajila, P.J., Golden Julie, E. and Harold Robinson, Y., 2023. ABAP: Anchor node based DDoS attack detection using adaptive neuro-fuzzy inference system. Wireless Personal Communications, 128(2), pp.875-899.
13. Elsadig, M.A., 2023. Detection of Denial-of-Service Attack in Wireless Sensor Networks: A lightweight Machine Learning Approach. IEEE Access.
14. Devi, M., Nandal, P. and Sehrawat, H., 2023, February. DDOS Attack in WSN Using Machine Learning. In International Conference On Innovative Computing And Communication (pp. 859-872). Singapore: Springer Nature Singapore.
15. Bukhari, S.M.S., Zafar, M.H., Abou Houran, M., Moosavi, S.K.R., Mansoor, M., Muaaz, M. and Sanfilippo, F., 2024. Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks, p.103407.
16. Zhao, H., Chen, F. and Ye, M., 2023, February. Secure Distributed Unscented Kalman Filter Against Cyber Attacks: DUKF with cluster-based attack detection strategy. In Proceedings of the 2023 7th International Conference on Digital Signal Processing (pp. 162-167).
17. Ismail, S., Dawoud, D. and Reza, H., 2022, January. A lightweight multilayer machine learning detection system for cyber-attacks in WSN. In 2022 IEEE 12th annual computing and communication workshop and conference (CCWC) (pp. 0481-0486). IEEE.
18. Naser, S.M., Ali, Y.H. and OBE, D.A.J., 2022. Deep learning model for cyber-attacks detection method in wireless sensor networks. Periodicals of Engineering and Natural Sciences, 10(2), pp.251-259.
19. Almaiah, M.A., 2021. A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology. In Artificial Intelligence and Blockchain for Future Cybersecurity Applications (pp. 217-234). Cham: Springer International Publishing.
20. Pan, J.S., Fan, F., Chu, S.C., Zhao, H.Q. and Liu, G.Y., 2021. A lightweight intelligent intrusion detection model for wireless sensor networks. Security and communication Networks, 2021, pp.1-15.
21. Srivastava, A., Addimulam, S.C., Basu, M.T., Sindhuri, B.P. and Maurya, R.K., 2024. Network Intrusion Detection System (NIDS) for WSN using Particle Swarm Optimization based Artificial Neural Network. International Journal of Intelligent Systems and Applications in Engineering, 12(15s), pp.143-150.
22. Singh, A.K., Alshehri, M., Bhushan, S., Kumar, M., Alfarraj, O. and Pardarshani, K.R., 2021. Secure and energy efficient data transmission model for WSN. Intelligent Automation & Soft Computing, 27(3), pp.761-769.
23. Adeniyi, E.A., Falola, P.B., Maashi, M.S., Aljebreen, M. and Bharany, S., 2022. Secure sensitive data sharing using RSA and ElGamal cryptographic algorithms with hash functions. Information, 13(10), p.442.