International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Security in Wireless Sensor Networks: Related Approaches in Intruder Detection Techniques

M. Supriya [1], Dr. T. Adilakshmi*[2]

Submitted: 28/01/2024 **Revised**: 06/03/2024 **Accepted**: 14/03/2024

Abstract: WSNs are vulnerable to a number of security threats, each of which has the potential to lower the network's overall performance. The characteristics of distributed, infrastructure-less, fault-tolerant, scalable, and dynamic wireless sensor networks (WSNs) define them A WSN's Intruder Detection System (IDS) is an essential component that contributes to the network's security and integrity. The need for a reliable and secure IDS has grown increasingly important as a result of the growing reliance on WSNs in a variety of applications, including healthcare, the military, and industrial. Although secure routing protocols, key management, and authentication mechanisms ensure safe transmission, there is no assurance that messages will be delivered consistently. To put it another way, these strategies are capable of protecting the network from outside threats, but they are ineffective against inside threats. They want to make certain that the data are true, that they are accurate, and that they are private. These techniques disguise delicate data in case of an attack from an external perspective, when a foe endeavors to gain admittance to the information. An inside assault happens when a sensor hub that is coordinated into the sensor network starts acting in a threatening way without first endeavoring to gain admittance to the data that is remembered for the messages that have been gotten.

***Keywords**: Intrusion Detection Systems (IDS), Wireless Sensor Networks (WSN), Secure Histogram Inclination Boosting Classifier*

1.Introduction

In a WSN, the primary function of an IDS is to identify and prevent any malicious activity or unauthorised access that could compromise the network's data. This can be accomplished by employing a variety of methods, like intrusion detection algorithms, access control mechanisms, and patterns of network traffic monitoring. In order to safeguard against security threats and attacks and guarantee the confidentiality, availability, and integrity of the data transmitted over the network, a WSN needs an IDSthat is already integrated into the sensor network begins acting in a hostile manner without first attempting to get access to the information that is included in the messages that have been received.

Intruder Detection System (IDS) in a WSN is a critical component that helps to maintain the security and integrity of the network. With the increasing reliance on WSNs in various applications such as industrial, military, and healthcare, the need for secure and robust IDS has become crucial. The main function of an IDS in a WSN is to detect and prevent unauthorized access or any malicious activity that may compromise the network and its data. This can be achieved through the use of various techniques such as monitoring network traffic patterns, implementing access control mechanisms, and using intrusion detection algorithms. An IDS in a WSN is essential to ensure the confidentiality, availability, and integrity of the data transmitted over the network, and to protect against security threats and attacks.

Anomaly-based and rule-based intrusion detection systems are currently in use. Rule-based interruption location frameworks, which are otherwise called signature-based IDS, are put to use to recognize likely interruptions with the help of pre-introduced marks. Rule-based intrusion detection systems are able to identify well-known attacks with high accuracy; however, they are unable to identify new attacks for which the intrusion database does not contain a matching signature. By comparing traffic patterns or resource utilisation to known good examples, anomaly-based intrusion detection systems discover breaches. Intrusion detection systems (IDS) based on anomalies are able to identify both known and unknown threats, but they also get more false positive and false negative alerts. Some IDSs are only made to work with certain routing protocols or configurations. Watchers make use of a proactive routing protocol to spot routing flaws as soon as they happen. Since it is carried out on every hub, there should be some sort of coordination between the hubs to distinguish steering invasions. A couple of the procedures for interruption recognition likewise work with receptive steering frameworks. As a result of these standards, the organisation can pick a course that is reliable as far as possible, from the source to the objective.

[1] *Swami Vivekananda Institute of Technology,JNUTH, Secundrabad ,Telangana– 500003, INDIA*
ORCID ID : 0000-0001-6466-5843
[2] *Vasavi College of Engineering,,Ibhrahimpatnam,Osmania University,Hyderabad,Telangana,– 500031,INDIA*
ORCID ID : 0000-0002-8295-3029

Email: supriyasamuel@yahoo.com ,t_adilakshmi@staff.vce.ac.in
* *Corresponding Author Email: author@email.com*

These are the primary issues with wireless sensor network intrusion detection.Remote sensor networks highlight one-of-a kind dangers in the connection and organisation layers. Remote sensor networks can't get to customary PC network assets like organisations, documents, framework logs, and cycles; hence, we should think about highlighting data for interruption discovery.Attacks on wireless sensor networks are distinctive. Tackle the interruption recognition framework's ability to perceive startling dangers and pick appropriate techniques. Attacks, both known and unknown, can be identified by algorithms. There are algorithms for flat surface networks and hierarchical structures. The requirements of the network ought to direct algorithm choice.There is a lack of energy, bandwidth, storage, and computational power in wireless sensor networks. Due to limited storage, sensor nodes are unable to keep extensive system logs. Multiple incursion patterns must be stored by knowledge-based intrusion detection systems. Libraries are required to store invasion behaviour traits because pattern matching identifies incursion. The feature library size is increased by invasion types. The intrusion detection algorithm cannot be executed by the node due to a lack of processing power. Current remote sensor networks utilise low-speed, low-power correspondence innovations, and hubs have restricted energy. In ordinary PC organisations, the correspondence above isn't thought of; however, interruption recognition frameworks shouldn't.

An improved intrusion detection system (IDS) was proposed by Mukaram Safaldin et al. [9] by combining a support vector machine with a modified binary grey wolf optimizer (GWOSVM-IDS). To find the best number of wolves to use, the GWOSVM-IDS tried using 3, 5, and 7 wolves. The target of the proposed strategy is to work on the exactness of interruption identification as well as the discovery rate, as well as to diminish how much time is spent handling in the WSN climate. By reducing the number of features caused by IDSs operating in the WSN environment and the number of false alarms that occur, this will be accomplished. In fact, the NSL KDD'99 dataset is used to demonstrate the efficacy of the suggested strategy and contrast it with other existing ones.

Abhilash Singh et al. [10] focused on using a model-based machine learning approach known as Gaussian Process Regression (GPR) to quickly identify and prevent any kind of intrusion. The authors have presented three feature-scaling-based approaches—S-GPR, C-GPR, and GPR—to accurately predict the likelihood of k-barrier coverage. As potential characteristics, they have selected the intrusion route angle, required k, number of nodes, sensing range, sensor-to-intruder velocity ratio (SIVR), and mobile-to-static node ratio (MSNR).

Using methods that are both dependable and effective and are based on fuzzy logic and neural networks (NN), Somnath Sinha et al. [11] created the anomaly-based intrusion detection system (AIDS). It is possible to implement the suggested system at each node due to its light weight and lack of overhead resources. It can also independently monitor the actions of local nodes to determine whether a node can be trusted, mistrusted, or an adversary. the development of AIDS antiretroviral therapy that is both reliable and effective through the use of fuzzy and neural network (NN)-based methods. Since the recommended framework is extremely lightweight and doesn't need to deal with a tonne of the above assets, it could be carried out in every hub. It can also independently monitor the actions of local nodes to determine whether a node can be trusted, mistrusted, or an adversary. The execution of a prepared NN assists with sifting through the phony problems that are caused when fluffy rationale is utilized in the main stage, which at last adds to an expansion in the precision of the framework. ained NN sift through the deceptions that were brought about by the fluffy rationale that was applied in the underlying stage, which eventually adds to an expansion in the precision of the framework by introducing extra sensors to give counterfeit information to trick the interloper by 1.2-2.6%. The parameters were selected in such a way that the model would produce the best possible results with the fewest significant adjustments and issues possible. The model uses a multiple-layer network to learn new information from dataset samples for a more refined training process

An Online Locally Weighted Projection Regression, also known as an OLWPR, was developed by I. Gethzi Ahila Poornima et al. [13] in order to locate anomalies in wireless sensor networks. Linear Weighted Projection Regression uses non-parametric methods, and the current predictions are made by local functions that use only a portion of the data. Because this is one of the requirements for wireless sensor networks, the computational complexity is minimal. Online dimensionality reduction in least squares principle component analysis (LWPR) is used to manage redundant and unnecessary data in the input data in least squares principle component analysis (PCA).

A model for hierarchical intrusion detection in a WSN that groups nodes according to their roles was developed by Wenjie Zhang et al. [14]. In addition, the synthesis of multi-kernel functions using the classification algorithm of a kernel extreme learning machine in accordance with the Mercer property is being considered in this study to increase the WSN intrusion detection system's abnormal behaviour detection accuracy and decrease the number of false alarms.

A method for detecting intrusions that is based on game theory and an autoregressive model was proposed by Lansheng Han et al. [15]. The study consistently predicts attack patterns and transforms the autoregressive theory model into a non-cooperative, complete-information, static game model. The methodology that has been proposed is an enhancement for strategies that have been utilized in the past in two essential ways: (1) It considers the intrusion detection process's energy consumption; furthermore, (2) it gets the ideal safeguard technique by breaking down the model's blended Nash harmony arrangement, which finds some kind of harmony between the framework's recognition productivity and how much energy it consumes.

Djallel Eddine Boubiche et al. [16] analysed the most broadly utilised conventions and coordinated them as per the sort of safety issue they addressed. In addition, the authors discuss potential future research areas based on newly emerging application domains and provide a summary of the most significant security concerns and limitations.

Prithi et al. [18] suggested cultivating the network's dynamic aspect by employing a novel LD2FA, which stands for Learning Dynamic Deterministic Finite Automata. LD2FA-PPSO, on the other hand, provides information regarding the node, packet, and route inspection for the purpose of identifying and eliminating intruders. This guarantees that the data transmission is carried out in a manner that is both efficient and energy-efficient.

Mohammed Amin Almaiah et al. [19] came up with a novel system that uses heuristic, signature, and voting detection methods to figure out which countermeasures work best with blockchain technology to find security and harmful threats. In the framework, the group head hub (CN) joins the elements of the three identification frameworks with those of blockchain to distinguish malevolent sensor hubs. Additionally, essential criteria like sensor node-hash value, node-signature, and voting degree are used by CN to identify malicious nodes in WSNs.

A secure, reliable, and energy-efficient method for routing data in WSNs was presented by Azam Beheshtiasl et al. [20]. Fuzzy logic is used in the proposed system to determine the trustworthiness of each route. From that point onward, trust and security contemplations were incorporated into the method involved with choosing the fastest way from the beginning to the objective. The suggested method makes use of the optimal routing strategy known as multidimensional scaling maps (MDS-MAP), and fuzzy logic is used to evaluate the trust model. Both the Trust and Centrality Degree-Based Admittance Control (TC-BAC) and the Trust-Mindful Steering Structure (TARF) conventions were assessed and appeared differently in relation to the proposed method.

3. Proposed Model

Secure Histogram Inclination boosting Classifier (SHIBC) is an assortment of the procedure known as tendency support that is sensible for use in Far Off Sensor Association Interference Acknowledgment Systems (WSN IDS). The purpose of developing a security system known as the Wireless Sensor Network Intrusion Detection System (WSN IDS) was to identify potential threats or intrusions into wireless sensor networks. By employing the histogram representation of the data, SHIBC is an effective method that works on the viability of interruption recognition in WSNs.

3.1 Inclination Boosting classifier:

The objective of the slope-supporting model is to integrate the results of various powerless students into a vigorous forecast model. Slope support is utilised to prepare new models on various occasions, with the essential objective of making each new model less inclined to commit errors than the ones that preceded it. Using this iterative method, the model can steadily increase its ability to anticipate outcomes. Tendency-supporting beginnings with the improvement of a hidden model, which is much of the time a decision tree with a shallow significance. The initial model that was created is also known as the basis or initial model. The preparation information is utilised to prepare the basic model, and afterward, expectations are made for every individual event in the dataset. The algorithm then determines the difference between the predicted values for the target variable and the actual values. These distinctions, which are referred to as residuals, indicate the mix-ups that the base model presents. The magnitude and direction of the changes required by subsequent models can be determined using the residuals.

A brand-new weak learner is built to handle residuals. It is anticipated that this new model will place a greater emphasis on the areas of information analysis in which the older model did not meet expectations. It gets better at anticipating the residuals, and that implies it commits fewer errors than the main model. The preparation information is utilised to prepare the new model, with residuals going about as the objective variable and being considered during preparation. With each emphasis, the calculation will continue to develop new models, with each model focusing on the remaining errors or residuals. These models are trained using the gradient descent method. In order to find the ideal parameters, the learning algorithm minimises a loss function that quantifies the differences between the expected and actual values.

Eventually, the last conjecture is made by joining the forecasts from each model. Each model's prediction accuracy is evaluated based on its performance during the training phase. The weighted sum of all of the expectations generated by the various models is the definitive figure. The strategy of creating cutting-edge forecasts and developing new models is repeated until either a certain number of cycles have passed or the necessary level of execution has been achieved. The number of iterations and complexity of the weak learners can be altered to strike the best possible balance between the model's performance and the resources required to run it.

Two of its most striking advantages are the limit of the angle's ability to deal with muddled associations and recognise unpretentious examples in the data. It is generally regarded as one of the most impressive AI calculations when paired with choice trees. This is especially because of how well it groups data together. However, if its hyperparameters are not regularized and adjusted appropriately, it may be susceptible to overfitting. While utilising slope helping, regularisation techniques and hyperparameter tuning are consequently fundamental contemplations.

Secure Histogram Inclination Boosting Classifier

Gatecrasher location is a significant use of remote sensor organisations (WSN), which includes distinguishing any unapproved or vindictive movement inside the organization. Using machine learning algorithms to classify sensor data as normal or abnormal is one way to accomplish this. In this work, the Secure Histogram Inclination Boosting Classifier (SHIBC) is proposed to recognise the unapproved movement. The SHIBC is an ensemble learning technique that creates a strong classifier by combining multiple weak learners (decision trees). It works by adding decision trees to the ensemble iteratively and adjusting their weights based on how the previous trees misclassified each other. By combining the predictions of all the trees, the final prediction is made.In order to use SHIBC in WSN for intruder detection, sensor data must first be categorized as normal or abnormal. The SHIBC model is then trained using this labeled data. The SHIBC learns to recognise patterns in the data that indicate intruder activity during the training phase. The model can be deployed in the WSN to continuously monitor the incoming sensor data after it has been trained. The SHIBC determines whether new data is normal or abnormal as it arrives. An alarm can be triggered to notify the network administrator in the event that the data is categorized as anomalous.

Decision trees serve as the weak learners in the proposed SHIBC algorithm, which is an extension of the conventional Gradient Boosting algorithm. However, SHIBC uses histograms to discretize the input features and then constructs multiple decision trees based on the histograms rather than constructing a single decision tree. The algorithm's memory and computational requirements are reduced, and the model's accuracy is improved by this method, among other benefits. Figure 1 depicts the proposed flowchart for the SHIBC algorithm.

The main steps of the SHIBC algorithm are as follows:

Create Histogram: Histograms are first created by discretizing the input features. This is accomplished by counting the number of samples that fall into each bin after dividing the feature range into a predetermined number of bins.

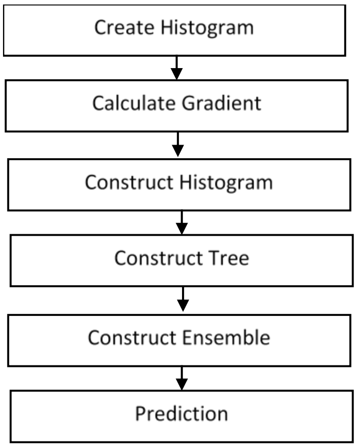

Fig. 1: Diagram of the proposed SHIBC algorithm

Calculate Gradient: The loss function's gradient in relation to the previous tree's predictions is calculated. The loss function will decrease most in this direction, as shown by this.

Construct Histogram : Utilizing the gradients from the previous step, a brand-new histogram is constructed. The slopes are utilized to refresh the loads of each example in the preparation set.

Construct Trees: Using greed, the histogram is used to build a decision tree. The histograms are divided in half recursively until a stopping condition is met before the tree is constructed.

Construct Ensemble: The tree is added to the group, and the cycle is rehashed until the ideal number of trees is reached.

Prediction : By combining the predictions of all the ensemble trees, the final prediction is made.

The SHIBC algorithm outperforms conventional gradient-boosting algorithms in a number of ways, including a reduction in the amount of memory and computational power required for the algorithm and an increase in the model's accuracy. Be that as it may, it likewise has a few restrictions, for example, being delicate to the decision of the histogram container size and the quantity of trees in the troupe. Sensor node-generated massive amounts of data are processed by WSN IDS. Because they are condensed and require less space, histograms are useful for representing data distributions. By converting raw data into histograms, SHIBC simplifies the issue's processing while also reducing its size. As a result, it is suitable for WSNs with limited resources because it allows for faster model training and more efficient data handling.

WSNs frequently demonstrate temporal or geographical correlations between their sensors' readings. Histograms are an effective method for capturing the data's statistical properties and local patterns. SHIBC doesn't do an examination of every individual piece of information; rather, it conducts a value distribution analysis. This permits the identification of anomalies or interruptions in light of deviations from the anticipated examples of the histogram.Complex non-linear correlations between the sensor data and the incursion patterns are frequently required by WSN intrusion detection systems. SHIBC is able to successfully learn and predict non-linear connections as a gradient-boosting technique. This ability is one of its numerous assets. Because it combines the limited learning abilities of several people, SHIBC is able to collect nuanced patterns and create a powerful prediction model that can adapt to the non-linear nature of incursion behaviours.

4.Simulation Results

A realistic and comprehensive WSN cyber security dataset is used in this section of the article. A wide range of wireless sensor network devices are responsible for producing the data that is gathered by the network. 14 threats related to connection protocols for the Industrial Internet of Things and the Internet of Things are identified and investigated in this dataset. These fourteen attacks can be divided into five distinct categories: DoS/DDoS attacks, information gathering, man-in-the-middle attacks, injection attacks, and malware attacks. After the realistic cyber security dataset has been processed and analyzed, intruder detection is carried out with the help of the proposed SHIBC model. Figure 2 provides a visual representation of these attacks.

The decision tree is the primary component of the proposed SHIBC model.

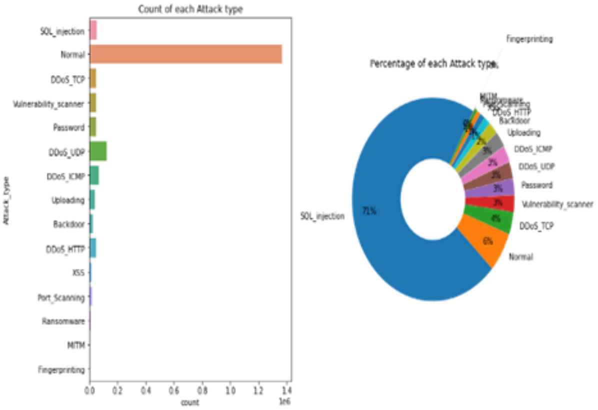

Fig 2:Visual representations of various attack types

The Inclination boosting Classifier uses choice trees as the base student. Each node in a decision tree represents a splitting rule based on a single feature, and the trees are constructed greedily and hierarchically. The selection of a feature that best separates the data is the first step in creating.The threshold is chosen so that the amount of information gained or the amount of impurity reduced is maximized. The information is then partitioned into two subsets in view of the limit. The left branch of the tree is assigned to the data points with feature values above the threshold, while the right branch is assigned to the data points with feature values below the threshold. For each subset, the steps of selecting features, setting a threshold, and splitting the data are repeated recursively until a stopping criterion, like the maximum tree depth or the minimum number of samples per leaf, is met. The decision trees in a gradient-boosting classifier are not constructed on their own but rather in a sequential fashion, with each tree learning to correct previous errors. A weighted sum is used to combine the predictions of the individual trees. The weights are set by the learning rate and the gradients of the loss function. The prediction results are obtained in the final step. The expected precision aftereffects of the proposed SHIBC for each attack for in Table 1.

Accuracy estimates the extent of genuine up-sides (TP) out of the relative multitude of anticipated up-sides (TP + misleading up-sides (FP)).

Table 1: The Prediction Accuracy results of Proposed SHIBC model for each attack

Attack type	**Precession**	**Recall**	**F1-score**
Normal	1	0.98	0.99
DDoS_UDP	0.7	0.9	0.78
DDoS_ICMP	1	1	1
DDoS_HTTP	1	1	1
SQL_injection	1	1	1
DDoS_TCP	0.83	0.72	0.77
Uploading	0.69	0.99	0.82
Vulnerability_scanner	1	1	1
Password	0.87	0.78	0.82
Backdoor	0.95	0.98	0.97
Ransomware	0.97	0.97	0.97
XSS	0.76	0.82	0.79
Port_Scanning	0.98	0.69	0.81
Fingerprinting	0.99	0.97	0.98
MITM	0.97	0.99	0.98

macro avg	0.91	0.92	0.91
weighted avg	0.94	0.94	0.94
Accuracy 94%			

Accuracy estimates the extent of genuine up-sides (TP) out of the relative multitude of anticipated up-sides (TP + misleading up-sides (FP)). It assesses the model's capacity to accurately identify positive instances and minimise false positives. Precision can be calculated as follows:

Precision = TP / (TP + FP). (1)

It assesses the model's capacity to accurately identify positive instances and minimise false negatives. The equation for review is:

Recall measures the proportion of true positives (TP) out of all actual positive instances (TP + false negatives (FN)).

Recall = TP / (TP + FN) (2)

The F1-score, which is the harmonic mean of precision and recall and provides an overall measure of the model's performance,It is a valuable metric when there is an imbalance between the no. of positive and negative occurrences in the information. The F1-score formula is:

F1-score = 2 * (precision * recall) / (precision + recall) (3)

Accuracy is another popular metric for evaluating classification models, such as the Gradient Boosting Classifier. It measures the proportion of instances in the dataset that have been correctly classified. Accuracy is calculated as:

Accuracy = (TP + TN)/(TP + TN + FP + FN) (4)

The proposed SHIBC model achieved 94% exactness. Precision, recall, and the F1-score can be calculated on either the training set or the test set in the context of the proposed Secured Histogram Inclination Boosting Classifier. The purpose of the evaluation will determine which dataset is selected. The evaluation ought to be carried out on the test set if the objective is to evaluate the model's capacity to generalize to new data. The proposed model is contrasted with other conditional-workmanship models.

Table 2 presents the comparison results

Model	Precession	Recall	F1-score	Accuracy
Gradient boosting	0.17	0.18	0.17	18.69%
Adaboost	0.19	0.32	0.21	32.19%
Logic Regression	0.31	0.38	0.27	38.06%
Naive bayes	0.54	0.39	0.36	39.96%
KNN	0.53	0.54	0.53	54.13%
Extra trees	0.92	0.92	0.92	92.30%
Decision tree	0.92	0.92	0.92	92.89%
Random Forest	0.93	0.93	0.93	93.10%
Proposed SHIBC	**0.94**	**0.93**	**0.93**	**93.70%**

The gradient-boosting classifier received the lowest score, as shown in Table 2. The adaboost, logic regression, and navive bayes each have an accuracy of 32.19%, 38.06%, and 39.96%, respectively. The KNN classifier outperformed gradient boosting, adaboost, logic regression, and naive Bayes classifiers with an accuracy of 54%. The extra trees and decision trees outperform the KNN classifier in terms of accuracy, with 92.30% and 92.89%, respectively. The Random Forest classifier achieved 93.10 percent, which is nearly identical to the performance of the proposed SHIBC model. However, the proposed SHIBC model achieved the highest level of accuracy, at 93.70 percent. In general, SHIBC can be used to detect intruders in WSN and can be an effective and efficient method for detecting malicious activity in the network. However, it is essential to keep in mind that the quality and quantity of the labelled data used for training have a significant impact on the model's performance.

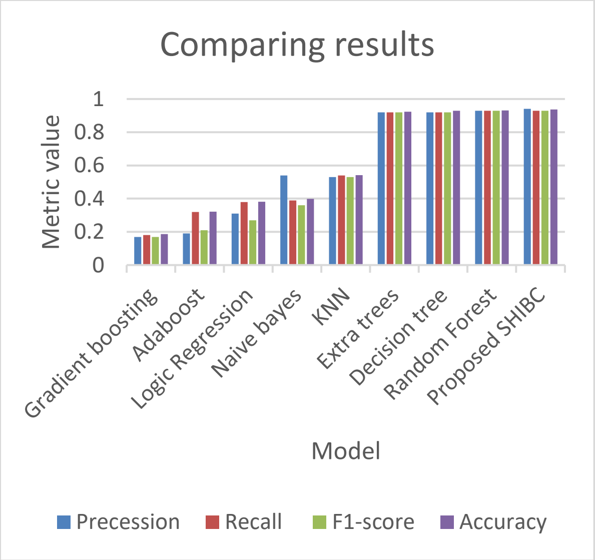

Fig3.graph comparing results with SHIBC

Conclusion: WSNs are utilized for the management of critical data in a variety of industries, including environmental sensing, industrial monitoring, and healthcare. By identifying any unauthorised modifications or harmful actions that could jeopardise the dependability of the acquired data, an IDS safeguards its integrity. By identifying and responding to security issues, IDS helps to maintain a WSN's overall dependability and availability. Histograms are a good way to represent data distributions in WSN IDS, which is responsible for processing huge volumes of data. Because it uses histograms to handle data effectively, the proposed model is suitable for WSNs with limited resources. For the purpose of intrusion detection, SHIBC effectively analyses deviations from expected histogram patterns because histograms capture local patterns. In addition, WSN IDS's predictive capabilities are enhanced by the fact that SHIBC excels at capturing intricate non-linear relationships. The proposed model acquired a precision of 93.7% in identifying and arranging various sorts of assaults in WSN.

Acknowledgements:

This research was supported/partially supported by my Swami Vivekananda Institute of Technology (SVIT) Engineering College We thank our HOD Dr.V.Sudha from [Osmania University] who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. We thank guide [Dr.T.Adilakshmi] for assistance with [MTCSA-HEA] from [VCE] for comments that greatly improved the manuscript.

Author contributions

Mrs.M.Supriya: Conceptualization, Methodology, Software, Field study , Data curation, Writing-Original draft preparation, Software, Validation., Field study **Dr.T.Adilakshmi:** Visualization, Investigation, Reviewing and Editing.

Conflicts of interest

The authors declare no conflicts of interest .

References

[1] Safaldin, Mukaram, Mohammed Otair, and Laith Abualigah. "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks." *Journal of ambient intelligence and humanized computing* 12 (2021): 1559-1576.

[2] Singh, Abhilash, Jaiprakash Nagar, Sandeep Sharma, and Vaibhav Kotiyal. "A Gaussian process regression approach to predict the k-barrier coverage probability for intrusion detection in wireless sensor networks." *Expert Systems with Applications* 172 (2021): 114603.

[3] Sinha, Somnath, and Aditi Paul. "Neuro-fuzzy based intrusion detection system for wireless sensor network." Wireless personal communications 114 (2020): 835-851.

[4] Sood, Tanya, Satyartha Prakash, Sandeep Sharma, Abhilash Singh, and Hemant Choubey. "Intrusion detection system in wireless sensor network using conditional generative adversarial network." Wireless Personal Communications 126, no. 1 (2022): 911-931.

[5] Poornima, I. Gethzi Ahila, and B. Paramasivan. "Anomaly detection in wireless sensor network using machine learning algorithm." Computer communications 151 (2020): 331-337.

[6] Zhang, Wenjie, Dezhi Han, Kuan-Ching Li, and Francisco Isidro Massetto. "Wireless sensor network intrusion detection system based on MK-ELM." Soft Computing 24 (2020): 12361-12374.

[7] Han, Lansheng, Man Zhou, Wenjing Jia, Zakaria Dalil, and Xingbo Xu. "Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model." Information sciences 476 (2019): 491-504.

[8] Boubiche, Djallel Eddine, Samir Athmani, Sabrina Boubiche, and Homero Toral-Cruz. "Cybersecurity issues in wireless sensor networks: current challenges and solutions." *Wireless Personal Communications* 117 (2021): 177-213.

[9] Premkumar, M., and T. V. P. Sundararajan. "DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks." *Microprocessors and Microsystems* 79 (2020): 103278.

[10] Prithi, S., and S. Sumathi. "LD2FA-PSO: A novel learning dynamic deterministic finite automata with PSO algorithm for secured energy efficient routing in wireless sensor network." Ad Hoc Networks 97 (2020): 102024.

[11] Almaiah, Mohammed Amin. "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, 2021.

[12] Beheshtiasl, Azam, and Ali Ghaffari. "Secure and trust-aware routing scheme in wireless sensor networks." Wireless Personal Communications 107 (2019): 1799-1814.

[13] Sharma, H.; Haque, A.; Blaabjerg, F. Machine learning in wireless sensor networks for smart cities: A survey. Electronics 2021, 10, 1012. [CrossRef]

[14] Schwendemann, S.; Amjad, Z.; Sikora, A. A survey of machine-learning techniques for condition monitoring and predictive maintenance of bearings in grinding machines. Comput. Ind. 2021, 125, 103380. [CrossRef]

[15] Liu, H.; Lang, B. Machine learning and deep learning methods for intrusion detection systems: A survey. Appl. Sci. 2019, 9, 4396. [CrossRef]

[16] Cui, L.; Yang, S.; Chen, F.; Ming, Z.; Lu, N.; Qin, J. A survey on application of machine learning for Internet of Things. Int. J. Mach. Learn. Cybern. 2018, 9, 1399–1417. [CrossRef] [17] Rezaee, A.A.;

Pasandideh, F. A Fuzzy Congestion Control Protocol Based on Active Queue Management in Wireless Sensor Networks with Medical Applications. Wirel. Pers. Commun. 2018, 98, 815–842. [CrossRef] [18]. Masdari, M. Energy Efficient Clustering and Congestion Control in WSNs with Mobile Sinks; Springer: Berlin/Heidelberg, Germany, 2020; Volume 111, ISBN 0123456789.

[17] Sangeetha, G.; Vijayalakshmi, M.; Ganapathy, S.; Kannan, A. A heuristic path search for congestion control in WSN. Lect. Notes Netw. Syst. 2018, 11, 485–495. [CrossRef] [20]. Chen, S.; Wen, H.; Wu, J.; Chen, J.; Liu, W.; Hu, L.; Chen, Y. Physical-Layer Channel Authentication for 5G via Machine Learning Algorithm. Wirel. Commun. Mob. Comput. 2018, 2018, 6039878. [CrossRef]