As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 9(04): 115-119, 2023
Copyright © 2023International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0904019
Available online at: http://www.ijmtst.com/vol9issue04.html

Prevention of Malicious Attacks and Anomaly Identification in Wireless Sensor Networks using PA

Dr. D.Sirisha, Karuturi Gayathri, P L Bhavana, Y R S Nishitha, G K Subhiram Chowdary

Department of Information Technology, Pragati Engineering College (A), Surampalem (East Godavari) A.P,India.

To Cite this Article
Dr. D.Sirisha, Karuturi Gayathri, P L Bhavana, Y R S Nishitha and G K Subhiram Chowdary. Prevention of Malicious Attacks and Anomaly Identification in Wireless Sensor Networks using PA. International Journal for Modern Trends in Science and Technology 2023, 9(04), pp. 115-119. https://doi.org/10.46501/IJMTST0903019

Article Info
Received: 02 March 2023; Accepted: 25 March 2023; Published: 31 March 2023.

ABSTRACT

The use of Wireless Sensor Networks (WSN) has increased significantly in recent years. Because of their small size and low cost, WSNs attract many companies to use them in various applications. Environmental monitoring, building security, and precision agriculture are just a few examples from many other industries. Since most of them are located in hostile and unattended environments, WSNs pose a serious security risk. Many options have been proposed to protect the confidentiality of the data during its transport from the sensors to the base station to ensure secure processing of the data to enable in the WSN. The purpose of this work is to detect attacks, a key responsibility for network and data security. To protect WSNs from malicious attacks, variance detection is a crucial task. Researchers are currently using various machine learning techniques to identify anomalies using offline learning algorithms. However, e-learning classifiers have not received enough attention in the literature. The goal is to provide an intrusion detection model that works with the unique properties of WSN. This approach is based on the passive-aggressive online classifier and the information gain factor. First, the relevant aspects of the sensor data are selected with an information gain factor. The Online Passive Aggressive algorithm also learns to detect and classify different types of denial-of-service attacks. The test was conducted in using a wireless data set from the Wireless Sensor Network Discovery System "WSNDS" used for the survey. The proposed ID-GOPA model achieves a 96% success rate in determining whether a network is functioning normally or is vulnerable to all types of attacks. In addition to 99% for normal operation, the detection accuracy for planning, gray hole attacks, flood attacks, and black hole attacks is 86%, 68%, 63%, and 46%, respectively. These results indicate that our offline learning methodology can replace online learning and provide effective detection of WSN anomalies in certain circumstances.

KEYWORDS – wireless sensor networks (WSNs), intrusion detection system (IDS).

1. INTRODUCTION

People are constantly developing new technologies in response to their needs. The revolution of miniaturization of electronic components with wireless technology is affecting our daily life. In the post-PC era, smartphones, laptops and other smart electronic devices have gained popularity, making computing devices more convenient, portable, widespread and ubiquitous in society [16]. It is now conceivable to build a wallet-sized embedded system with the same storage space as a personal computer from the 1990s. Windows or Linux operating systems can support such embedded devices to some extent. In this sense, the latest trend of Moore's Law towards the miniaturization and ubiquity of computing devices the emergence of Wireless Sensor Networks (WSN) is essentially what "the emergence of WSN" means. A unique category of ad hoc networks is wireless sensor networks [15]. They are composed of a few small-diameter, low-power, multifunctional intelligent sensor nodes (also called nano computers). These network nodes are designed to be easily and randomly distributed in a given space, thus have an intrinsically spontaneous mode of organization (BS), can also process data, process real-world events, and communicate with each other. This data is then sent over the network to a facility for processing, where the user can perform analysis, evaluate the data, and make decisions. The concepts of these applications are based on the cooperation and reliability of each participating node. However, this is not the case in real implementations, where nodes are subject to various disturbances that seriously disrupt and reduce the functionality of the network can affect system performance. Unfortunately, since the nodes consist of cheap electronic devices with negligible hardware capabilities, it is difficult to guarantee the security of this type of network against many hostile attacks. Encryption algorithms require large amounts of processing, memory, and power. As a line of defense, detection-based methods are offered to defend WSN against both known and emerging cyber attacks. One of the most flexible and practical techniques to protect the WSN against known and unknown attacks is the "IDS" Intrusion Detection System. IDS monitors and analyzes network events, looks for unusual elements and reports intrusion attempts to network nodes. Sensor Anderson is the one who originally came up with the idea. The widespread methods of creating IDSs currently used to detect attacks have a strong connection to machine learning methods.

2. Preliminaries and Related Work

WSNs are not immune to disruptive attacks and security threats that result in information security leaks or compromise their presentation and effectiveness. To this end, it encourages ongoing research to construct efficient error indicators for sensor networks that are adapted to their particular properties. Various studies have proposed AI responses for IDS to detect deficiencies in the WSN. Existing gap detection strategies 927 essentially consist of decoupled learning approaches 927 such as helper vector machines, 927 irregular forests, 927 false brains 927 organization, tree selection 927 and various techniques 927. There aren't many articles written in that highlight the use of online advances to tackle the use of these strategies. Almomani et al. [5] created a new dedicated WSN record and the collected record is called WSN-DS. Contains normal traffic from the organization and several DoS situations (Flood, Sun opens, Blackhole and sets up a raid) in the WSN. It is based on the drain convention, is one of the most popular different directional conventions in WSN, and uses the NS2 network test system for inventory information. Brain (ANN) to distinguish and sort 4, crises. The results were organized using 10-layer cross-validation and split technique. WSN-DS performed a large number of DoS attacks, except for the weak opening attack, considering that its detection rate is very poor in contrast to others. Dong et al. [6] proposed a outage detection model given the data growth rate and storage calculations to identify DoS attacks in clustered WSNs. The developers used the data gain ratio to reduce redundant elements. Sacking calculations were used to create harvesting calculations to prepare C4.5 selection tree clusters for further development. The proposed model was built independently using the NSL-KDD and WSN-D datasets to test the presentation of the model. This technique offers a more advanced execution than other strategies. Sindhu et al. [7] has developed another lightweight IDS that displays the anomaly detection in the WSN in light of the DT feature calculation in the WSN. To run the developers decided to use Kddcup' 99 as a record for relevant information. The model consists of three steps, in the initial step a component determination strategy was performed to eliminate extraneous components for better results. Significant elements were then used in range-based highlight selection calculations to identify a reasonable subset. The final step was the neurotrauma learning worldview change in the IDS. The developers explain that using proper highlighting with the neuro-tree is a promising identification of glitches in the system. Certainly, the model resulted in higher detection accuracy Pachauri et al. [8] examined AI methods, programming, and repeat calculations on the authentic clinical datasets with a proposed framework for identifying errors and inconsistencies.

The evaluation of the proposed model depended on the accuracy of the predictions and measurements of the perturbation. Bosmana et al. [11] proposed a decentralized anomaly detection framework for WSN using Internet self-learning. Focus methods have several disadvantages, so with a selection of real organizations and datasets was used for singularity detection, which 1087 similarly reduces power consumption and range by integrating a local data approach and using recursive least squares (RSL) for learning. Single models. Rasa et al. [12] introduced a variant of the PCA called One-Class Head Part Classifier (OCPCC) to detect near and unattended anomalies when energy in WSN using CCIPCA (Genuine Covariance free Gradual Head partial exam). Identify gaps in no time. The run includes GSB as a dataset and the methodology is split into two steps, the decoupled phase of the PCA model is prepared 1087 using the typical information 1087 collected from each sensor to build a common behavioral model, Web detection phase, sensor hubs group each packet as common or odd based on the boundary defined in the Global Common Model (GNM). The regular PCA model is updated in and improved with the new mean and standard deviation of the information. The creators involved in the reconstruction of the KDD Cup99 as an information index really consider the implementation of the framework. The proposed ISVMM model can predict each of the 41 components well without reducing the dimensionality of it index information. In this article, we use a specific -WSN-DS record in our example to characterize four types of DoS attacks: Blackhole, Dim Opening, Flooding, and Booking out typical organization traffic. We compare three-item selection techniques to the Detached Forceful online classifier and examine exposure with each strategy and find a pair of s that perform better. We will design an active, productive and learnable model using an online force classifier using backlight reduction and ensuring model similarity with WSN features. Obstacles of existing frameworks: 1) Due to its remote nature, it has been hacked by developers. 2) Cannot be used for high-speed adaptation as it is intended for low-speed applications. 3) Setting up such an organization is expensive and therefore cannot be accessible to everyone.

3. SYSTEM FRAMEWORK

The transmission of sensors to the base station to avoid all types of attacks. The model is trained by the SVM algorithm with other algorithms such as ANN, Random Forest and Decision Tree. To know the existing network activities better and learn the activity flows during the offline phase (training data collection) where the processed and tagged training datasets are used to create a learnable and testable model. In the online phase, the same standard engine uses the model trained in the offline phase to select only the relevant attributes based on the gain method and classify each packet as normal or as in real time Classify attack. WSN-DS dataset: The study used a replicated Remote Sensor Network Discovery (WSN-DS) dataset obtained from Almomani et al. In addition, the test system of the organization NS-2 was used to reproduce the climate of the remote sensor network in the light of SVM calculations and other calculations. Gather information from the organization and preprocess it to produce 23 components that detect the status of each sensor. The survey recreates four different types of DoS (Administrative Disavowal) attacks: Blackhole, Dark Opening, Flooding. The record contained only 19 distinctions, including the class mark, as shown in -Table 2. This dataset was created as an IDS dataset to be used with AI to distinguish and order DoS attacks. Figure 2 shows the deviation of the information. Here are some of the personal computer mechanical components used in the runtime: of resection.

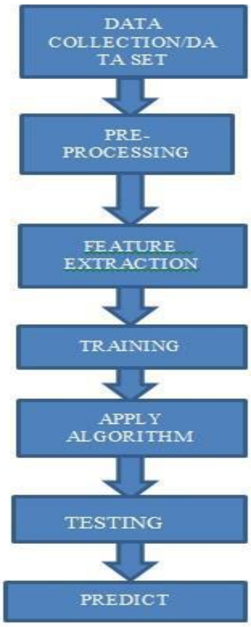

FIGURE 1. Block diagram of proposed system.

- **Arbitrary access memory:** 8 GB; CPU: Intel(R) Core (TM) i7-4610M computer processor @ 3.00 GHz;

- **Framework**: Windows 7 Star 64-bit used 60% of the information to create the dataset and 40% to test the dataset. The dataset was divided into dataset creation and testing two series shown.

Performance Evaluation: 1087 The effects of this study are evaluated using four 1087 models, namely 1087 Accuracy (ACC), Precision (PR), f1 score (F), and 1087 Recall (RE). This multiplicity of patterns has a value between 0 and 1. Approaching 1, the power of increases, while approaching 0 decreases. These presentation scores are determined as follows:

- **Accuracy (Acc):** Evaluates the contribution of accurately perceived records to the total test information. Accuracy is a decent metric for the test data set, which includes custom classes and functions:

$Exactness = T\ P + T\ N/T\ P + F\ P + F\ N + T\ N$

- **Exactness (PR):** Or Positive Prescient Worth (PPV) addresses the proportion of information accurately named an assault to all information delegated an assault and is characterized as follows:

$Exactness = T\ P/T\ P + F\ P$

- **Recall (RE):** Additionally called True Positive Rate (TPR) or (Awareness), it gauges the proportion of information named an assault to all go after information:

$Recall = T\ P/T\ P + F\ N$

- **F1-Score (F):** or F1-Measure addresses the symphonious mean of the two Accuracy and Review networks. This idea is utilized to communicate in general achievement:

$F1 - Score = 2 \times P\ R \times RE/P\ R + RE$

Four features are used and are summarized below:

- True Positive (TP) refers to attacks that were carefully planned times.
- True Negative (TN) refers to the amount of simple information actually grouped as typical (correct rejection).
- Positive Misleading Error (FP) is the number of misclassified attacks.
- A false negative result (FN) is the number of commonly misclassified cases.

4. CONCLUSIONS

It is difficult to provide security management in WSNs that rely on outages with a site image to accurately distinguish threats. In this investigation of, we introduced calculations to identify sharp breaks, keeping artificial intelligence in mind. SVM calculations are used with other 1087 calculations such as KNN, 1087 Timberland Arbitrary, Select Tree to track singularity detection. In order to reduce the overhead of the and reduce the number of limitations of the, data gain ratio was selected as a selection item.

The calculation of SVM as a continuously learning machine has been improved to correct, which is a critical component. According to the reconstruction results, our model is a very accurate, in contrast to the decoupled models with an overall accuracy of 96%. Unlike current models, which are suitable for explicit uses, our methodology is appropriate in all circumstances. We plan to advance by consolidating various calculations to detect anomalies in future efforts to improve. In principle, would provide better location accuracy as different calculations work together to make exceed the limits.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Thanuja, N., & Deepak, N. R. (2021, April). A convenient machine learning model for cyber security. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 284-290). IEEE.

[2] Rassam MA, Maarof M. und Zainal A. American Journal of Applied Science, 2012, Volume 9, Page 1636

[3] Marriwala N. und Rathee P., (2012). Life Extension Method Remote Sensori Network Advances Data & 2012 World Congress (IEEE) Corrispondenza, p.495–499

[4] Sivatha Sindhu, SS, Gita, S., & Kannan, A. (1999). (2012). Development of decision rules optimized for intrusion detection using the particle swarm paradigm. International Journal of Systems Science, 43(12), 2334-2350.

[5] Cauteruccio, F., Fortino, G., Guerrieri, A., Liotta, A., Mocanu, D. C., Perra, C., & Vega, M. T. (2019). Detection of short-term anomalies in wireless sensor networks based on machine learning and multi-parameter range modification. Information Fusion, 52, 1330.

[6] Gawas, M., Parab, A., & Patil, HY (2022). Use and challenge to protect online privacy of things. Industrial

Internet of Things: Technologies and Research Directions, 103.

[7] Data Combination 2017 33 41-56 di Bosman H, Iacca G, Tejada A, W ortche HJ e Liotta A. Rassam M .A., Maarof M. A. i Journal A. Information Based Frameworks 60, 44-57

[8] Energy-efficient correspondence convention for remote microsensor networks, einzelman W R, Chandrakasan An, and Balakrishnan 200 Procedures of the 33rd Annual Hawaii Global Framework Sciences Meeting (IEEE), pp. 10–11.

[9] Bunch number changeability issue in drain, Liu H, Li L, and Jin S 2006, Global Gathering on Pervasive Knowledge and Figuring (Springer), pp. 429–437

[10] Interruption identification using an irregular woodlands classifier with ruined and highlight reduction, Tesfahun An and Bhaskari D L 2013, 127–132, 2013 Global Conference on Cloud and Pervasive Figuring and Emerging Innovations

[11] Manjula Devarakonda Venkata1, Sumalatha Lingamgunta & K Murali, Health Care Automation in Compliance to Industry 4.0 Standards: A Case Study of Liver Disease Prediction ,Journal of Scientific & Industrial Research , Vol. 82, February 2023, pp. 263-268, DOI: 10.56042/jsir.v82i2.70215

[12] Manjula Devarakonda Venkata1, Sumalatha Lingamgunta & K Murali, Health Care Automation in Compliance to Industry 4.0 Standards: A Case Study of Liver Disease Prediction ,Journal of Scientific & Industrial Research , Vol. 82, February 2023, pp. 263-268, DOI: 10.56042/jsir.v82i2.70215

[13] Deepak, N. R., & Balaji, S. (2016, April). Up link Channel Performance and Implementation of Software for Image Communication in 4G Network. In Computer Science On-line Conference (pp. 105-115). Springer, Cham.

[14] 15. Thiagarajan, R., Balajivijayan, V., Krishna moorthy, R., & Mohan, I. (2022). A robust, scalable, and energy-efficient routing strategy for UWSN using a Novel Vector-based Forwarding routing protocol. Journal of Circuits, Systems and Computers.

[15] NR, D., GK, S., & Kumar Pareek, D. (2022). A Framework for Food recognition and predicting its Nutritional value through Convolution neural network.

[16] Sirisha, D., Srilatha, Y., Sowjanya, N.V.S. (2022). Classification and Recognition of Traffic Signs Using Deep Learning. In: Bhateja, V., Khin Wee, L., Lin, J.CW., Satapathy, S.C., Rajesh, T.M. (eds) Data Engineering and Intelligent Computing. Lecture Notes in Networks and Systems, vol. 446. Springer, Singapore. DOI: 10.1007/978-981-19-1559-8_40

[17] D Sirisha, S Sambhu Prasad, "MPEFT: A Makespan Minimizing Heuristic Scheduling Algorithm for Workflows in Heterogeneous Computing Systems", CCF Transactions on High Performance Computing. Aug. 2022. DOI: 10.1007/s42514-022-00116-w