ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 3, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 6.551

+91 9940572462 +91 9940572462 ijarasem@gmail.com www.ijarasem.com

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |

AI-Based Anticipation of Attacks on Wireless Sensor Network

Ms.P.Chitra[1], Pundi Vaishnavi[2], G.Rajeshwari[3] and B.Rishitha[4]

[1]Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[2] UG Scholar, Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[3] UG Scholar, Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

[4] UG Scholar, Department of Computer Science and Engineering, Velammal Institute of Technology, Panchetti, Chennai, India

ABSTRACT: Wireless sensor network has attracted significant attention in research and development due to its tremendous applications in medical, military and defence, medical, environmental, industrial, infrastructure protection, and commercial applications to enable to interact with each other controlled remotely. A Wireless Sensor Network (WSN) has wide applications such as environmental monitoring and tracking of the target nodes for communication. The sensor nodes are equipped with wireless interfaces used for communication between the nodes and another network. Wireless Sensor Network suffers from many constraints that make security a primary challenge. When the sensor node is deployed in a communication environment unattended, the nodes are vulnerable to various attacks. The analysis of dataset by supervised machine learning technique(SMLT) to capture several information's like, variable identification, univariate analysis, bivariate and multivariate analysis, missing value treatments etc. A comparative study between machine learning algorithms had been carried out in order to determine which algorithm is the most accurate in predicting the type WSN attacks. The results show that the effectiveness of the proposed machine learning algorithm technique can be compared with best accuracy, precision, Recall, F1 Score, Sensitivity, and Specificity.

KEYWORDS: WSN Attacks, Security Challenge, SMLT,F1 Score, Recall

I.INTRODUCTION

A wireless sensor network consist of spatially distributed autonomous small tiny sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a base station[1]. The development of wireless sensor networks was motivated by military applications such as battle field surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on[2].

Cost constraints and detection possibility of sensor nodes have been one of the most researched areas of WSN [3]. WSNs find many applications in environmental observation and forecasting systems, habitat monitoring, intrusion detection and tracking, seismic monitoring, etc[4].

Every sensor in a WSN has a limited sensing range and the union of the sensing ranges of all sensors reflects how well the area of sensor field is monitored known as the coverage area [5]. Random deployment is normally used in case of inaccessible terrains, disaster areas and war zones. In random deployment, sensors are usually scattered for example air dropped [6]. Deterministic deployment finds applications in border surveillance, intrusion detection, and structural healthcare among others [7].

The subsets of nodes which can monitor all the target points in a region are considered to constitute a set cover[8]. In such cases, the coverage problem emphasizes on determining as many number of set covers as possible, such that network lifetime is maximized. The related problem with coverage is the connectivity problem, which ensures the existence of path between every two nodes [9].

Deterministic deployment is selectively deciding the locations of the sensors for uniform coverage by optimizing one or more parameters. Deterministic deployment finds applications in border surveillance, intrusion detection, and structural healthcare among others [10].

This paper is organised as follows, Section 2 describes the related works. In Section 3 we describe the proposed method and Section 4 displays the experimental results. The conclusions are given in Section 5.

II. RELATED WORKS

This paper addresses the security issues in WSN by establishing potential automated solutions for identifying associated risks. It also evaluates the effectiveness of various machine learning algorithms on two types of datasets, mainly, KDD99 and WSN datasets. The aim is to analyse and protect WSN networks in combination with Firewalls, Deep Packet Inspection (DPI), and Intrusion Prevention Systems (IPS) all specialized for the overall protection of WSN networks. Based on the finding, the most accurate algorithm and the least time processing were suggested for both datasets[11].

Machine learning also inspires many practical solutions that maximize resource utilization and prolong the lifespan of the network. In this paper, we present an extensive literature review over the period 2002-2013 of machine learning methods that were used to address common issues in wireless sensor networks (WSNs). The advantages and disadvantages of each proposed algorithm are evaluated against the corresponding problem. We also provide a comparative guide to aid WSN designers in developing suitable machine learning solutions for their specific application challenges[12].

This paper conducted an experiment using Waikato Environment for Knowledge Analysis (WEKA)to evaluate the efficiency of five machine learning algorithms for detecting flooding, grayhole, blackhole, and scheduling at DoS attacks in WSNs. The evaluation is based on a dataset, called WSN-DS. The results showed that the random forest classifier outperforms the other classifiers with an accuracy of 99.72%[13].

In this paper, we present an extensive literature review over the period 2002-2013 of machine learning methods that were used to address common issues in wireless sensor networks (WSNs). The advantages and disadvantages of each proposed algorithm are evaluated against the corresponding problem. We also provide a comparative guide to aid WSN designers in developing suitable machine learning solutions for their specific application challenges [14].

Machine learning techniques survey for WSNs provide a wide range of applications in which security is given top priority. To secure data from attackers the WSNs system should be able to delete the instruction if any hackers/attackers are trying to steal data [15].

III. PROPOSED METHOD

The proposed model is to build a machine learning model for predicting WSN attacks. Previously they finds the accurate leak detection and isolation results only. WSN attack detection is an important technique for recognizing fraud activities, suspicious activities, network intrusion, and other abnormal events that may have great significance but are difficult to detect. The machine learning model is built by applying proper data science techniques like variable identification which is the dependent and independent variables. Each and every column's features are analyzed. Then the pre-processing and visualization of the data are done. The model is built based on the previous dataset where the algorithm learns data and gets trained different algorithms are used for better comparisons. The performance metrics are calculated and compared.

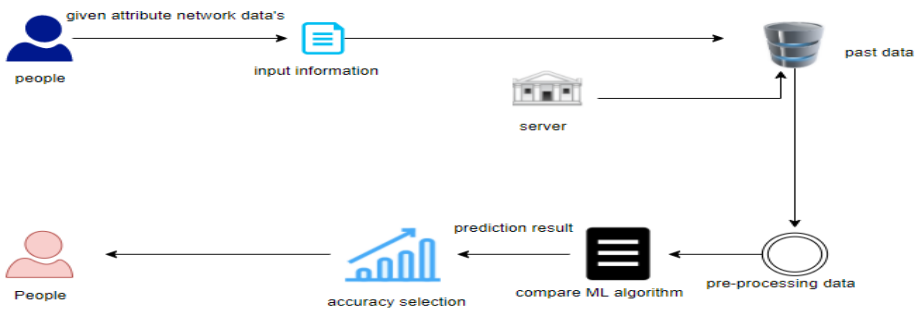


Figure 1. Architecture of proposed method

3.1 Description

3.1.1 Data Pre-processing

Validation techniques in machine learning are used to get the error rate of the Machine Learning (ML) model, which can be considered as close to the true error rate of the dataset. If the data volume is large enough to be representative of the population, you may not need the validation techniques. However, in real-world scenarios, to work with samples of data that may not be a true representative of the population of given dataset. To finding the missing value, duplicate value and description of data type whether it is float variable or integer. The sample of data used to provide an unbiased evaluation of a model fit on the training dataset while tuning model hyper parameters.

3.1.2 Data Collection

The data set collected for predicting given data is split into Training set and Test set. Generally, 7:3 ratios are applied to split the Training set and Test set. The Data Model which was created using Random Forest, logistic, Decision tree algorithms and Support vector classifier (SVC) are applied on the Training set and based on the test result accuracy, Test set prediction is done.

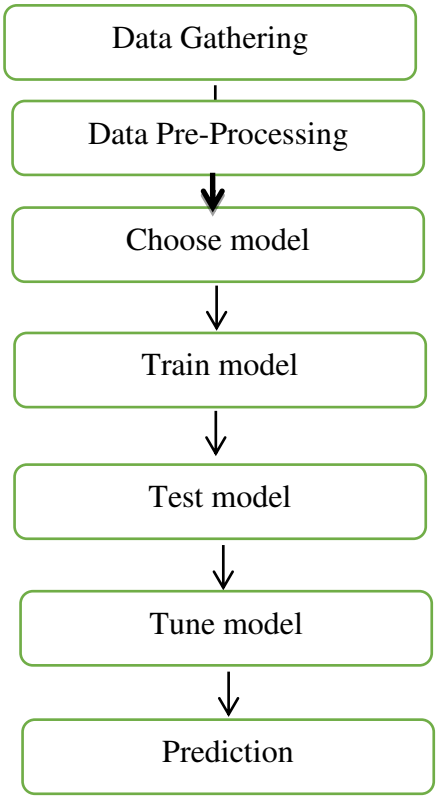


Figure 2.Process of dataflow diagram

Algorithms

Used Python Packages:

Sklearn:

- In python, sklearn is a machine learning package which include a lot of ML algorithms.
- Here, we are using some of its modules like train test split, DecisionTreeClassifier or Logistic Regression and accuracy score.

NumPy:

- It is a numeric python module which provides fast maths functions for calculations.
- It is used to read data in numpy arrays and for manipulation purpose.

Pandas:

- Used to read and write different files.

- Data manipulation can be done easily with data frames.

Matplotlib:

- Data visualization is a useful way to help with identify the patterns from given dataset.
- Data manipulation can be done easily with data frames.

IV. EXPERIMENTAL RESULT

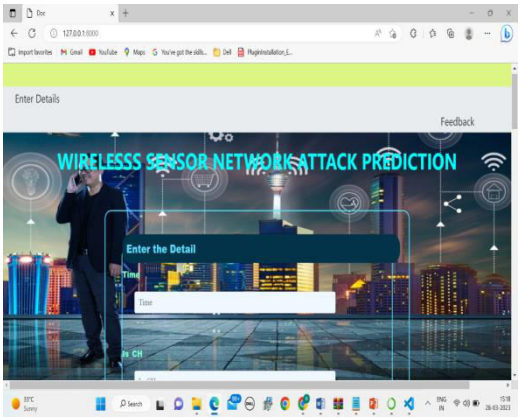


Figure 3 .Home Page

Figure 4.Input Collection

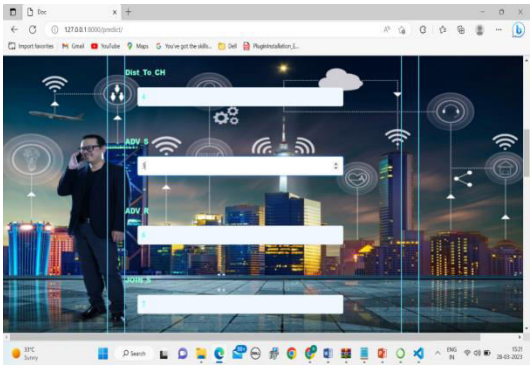


Figure 5.Input Collection

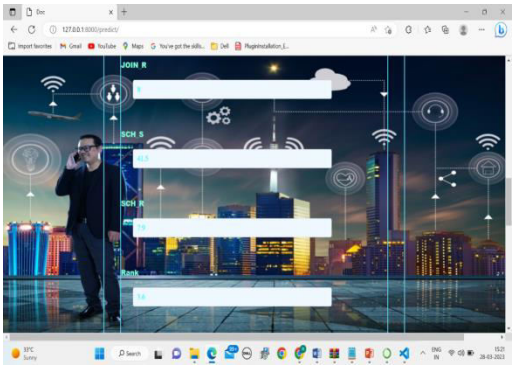


Figure 6.Input Collection

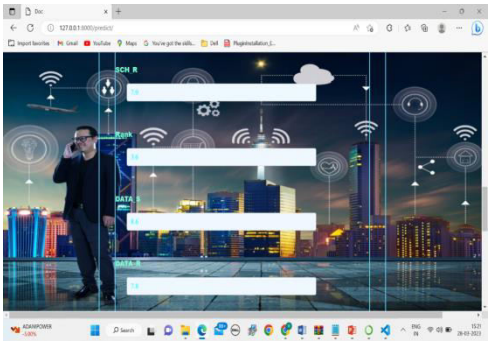


Figure 7.Input Collection

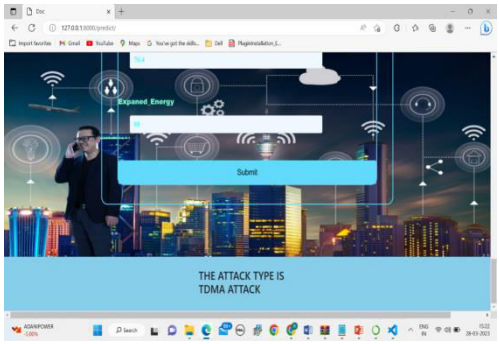
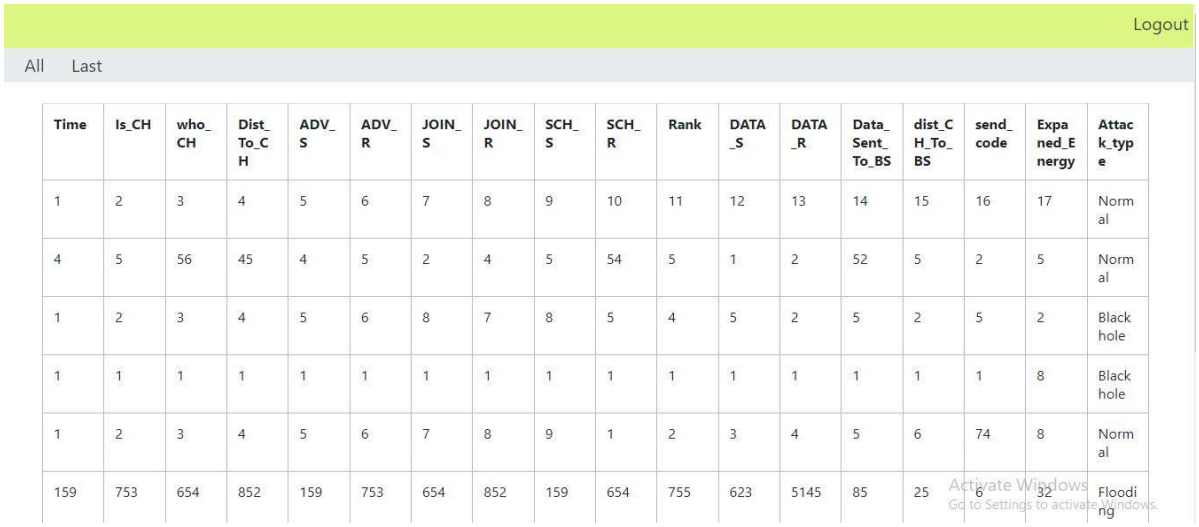


Figure 8.Result showing the type of attack

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 3, May 2023 |



Logout

All Last

Time	Is_CH	who_CH	Dist_To_CH	ADV_S	ADV_R	JOIN_S	JOIN_R	SCH_S	SCH_R	Rank	DATA_S	DATA_R	Data_Sent_To_BS	dist_CH_To_BS	send_code	Expaned_Energy	Attack_type
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	Normal
4	5	56	45	4	5	2	4	5	54	5	1	2	52	5	2	5	Normal
1	2	3	4	5	6	8	7	8	5	4	5	2	5	2	5	2	Black hole
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	8	Black hole
1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	74	8	Normal
159	753	654	852	159	753	654	852	159	654	755	623	5145	85	25	6	32	Flooding

Figure 9.Sample Inputs and Result obtained

V. CONCLUSION AND FUTURE ENHANCEMENT

The analytical process started from data cleaning and processing, missing value, exploratory analysis and finally model building and evaluation. The best accuracy on public test set is higher accuracy score will be find out by comparing each algorithm with type of all WSN Attacks for future prediction results by finding best connections. This brings some of the following insights about diagnose the network attack of each new connection. To presented a prediction model with the aid of artificial intelligence to improve over human accuracy and provide with the scope of early detection. It can be inferred from this model that, area analysis and use of machine learning technique is useful in developing prediction models that can helps to network sectors reduce the long process of diagnosis and eradicate any human error.

Some further work is required to be done inNetwork sector to automate and detecting the attacks of packet transfers from eligibility process (real time) based on the connection detail.

REFERENCES

[1] J. C. Jian, S.W. ren , X. min and T.X. lun, \Energy-balanced unequal clustering protocol for wireless sensor networks", The Journal of China Universities of Posts and Telecom-communications, 2010, 94- 99. [4] S. Mao, C. Zhao, Z. Zhou and Y. Ye, \An Improved fuzzy unequal

[2] A. Bari, S. Wazed, A. Jaekel and S. Bandyopadhyay, \An Genetic Algorithm based approach for energy e cient routing in two-tiered sensor networks", Ad-hoc Networks, 2009, pp. 665-676.

[3] Kumar S, Lobiyal DK. Sensing coverage prediction for wireless sensor networks in shadowed and multipath environment. Sci World J. 2013.

[4] Wang Y, Zhang Y, Liu J, Bhandari R. Coverage, connectivity, and deployment in wireless sensor networks. In: Recent Development in Wireless Sensor and Ad-Hoc Networks. Springer; 2015:25-44.

[5] Wang Y, Wang X, Agrawal DP, Minai AA. Impact of heterogeneity on coverage and broadcast reachability in wireless sensor networks. In: Proceedings of 15th International Conference on Computer Communications and Networks. ; 2006:63-67.

[6] Ishizuka M, Aida M. Performance study of node placement in sensor networks. In: Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on. ; 2004:598-603.

[7] Deif DS, Gadallah Y. Classification of wireless sensor networks deployment techniques. IEEE Commun Surv Tutorials. 2014;16(2):834-855.

[8] Mulligan, R. and Ammari, H.M. (2010) 'Coverage in wireless sensor networks: a survey', Network Protocols and Algorithms, Vol. 2, No. 2, ISSN: 1943-3581

[9] Thai, M.T., Wang, F. and Du, D-Z. (2008) 'Coverage problems in wireless sensor networks: designs andanalysis', International Journal of Sensor Networks, May, Vol. 3, No. 3, pp.191–200.

[10] Deif DS, Gadallah Y. Classification of wireless sensor networks deployment techniques. IEEE Commun Surv Tutorials. 2014;16(2):834-855.

[11] Mohammed S.Alsahli, Marwah M.Almasri, Mousa Al-Akhras, Abdulaziz I.Al-Issa, Mohammed Alawairdhi (2021) Evaluation of Machine Learning Algorithms for Intrusion Detection System in WSN doi:DOI 10.14569/IJACSA.2021.01205741

[12] Mohammad Abu Alsheikh, Shaowei Lin, Dusit Niyato and Hwee-Pink Tan(2015) Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications
DOI:10.1109/COMST.2014.2320099

[13] Lama Alsulaiman and Saad Al-Ahmadi(2021)Performance Evaluation of Machine Learning Techniques For Dos Detection In Wireless Sensor Networkdoi: 10.1049/iet-com.2019.0172

[14] Mohammad Abu Alsheikh, Shaowei Lin, Dusit Niyato and Hwee-Pink Tan(2015)Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and ApplicationsDOI**:** 10.1109/COMST.2014.2320099

[15] Dr. E. Baraneetharan (2020) Role of Machine Learning Algorithms Intrusion Detection in WSNs: A SurveyDOI: 10.36548/jitdw.2020.3.004

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com