Journal of Modern Computing and Engineering Research
JMCER
Volume 2022, p. 84-93
https://jmcer.org

Detection of Security Attacks in Wireless Sensor Networks

Sura Alsharifi [1] and Mafaz Alanezi [2]

[1,2]Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Iraq

[1]sura.20csp80@student.uomosul.edu.iq, [2]mafazmhalanezi@uomosul.edu.iq

Received: November 10, 2022 *Revised: December 13, 2022* *Accepted: December 16, 2022*

Abstract:

One of the primary concerns in sensor networks is Security. Wireless Sensor Network involves a considerable number of nodes which can be known as" tiny sensor nodes". These nodes swap the information with other nodes by special wireless links in a short period. The information is perhaps private for many people or business dealings. These networks are exposed to many attackers due to deployment in distant areas and distributed behavior. At the sensor node level, the networks are controlled by different constraints like less memory capacity, low transmission range, and less battery power. Where at the network level, they are controlled by irregular connectivity and Adhoc networking. This research may analyze the main security issues, security breaches, and challenges in the Wireless Sensor Networks world based on the analysis of Low Energy Adaptive Clustering Hierarchy (LEACH), Which is a cluster-based routing protocol by varying the number of clusters to observe the effect on Sensor Network performance in terms of network lifetime, energy dissipation, and amount of data reaching the base station. A scheme has been proposed for collecting and processing the data and then producing 12 features. This ordered dataset is called Wireless Sensor Networks- Data Set (WSN-DS). Support Vector Machine (SVM) was trained on the dataset for detecting and classifying the DoS attacks where 80% for training and 20% for testing. The results section shows how the WSN DS increased the capability of the Intrusion Detection System (IDS) to realize a better classification accuracy rate. The classification accuracies of attacks were 100%, and 98% for Normal, Black hole, and Sinkhole attacks.

Keywords: *Support vector machine (SVM), DDos, Blackhole, Sinkhole, Low-Energy Adaptive Clustering Hierarchy (LEACH) Protocol, Wireless Sensor Networks (WSN).*

1 Introduction

Small sensor nodes make up the self-securing Wireless Sensor Networks (WSN). Each has a memory space, computational power, and low energy consumption. component of a sensor node consists of a microcontroller, the radio's front end, a sensor, and the main power source. Sensors' primary function is to measure or keep track of many physical and environmental parameters, including pressure, humidity, temperature, sound, and many others. Following the sensing procedure, they are transmitting the data they have gathered to their main location. This collected data has been requested by Sensor Networks (Yousif, 2021). WSN has many resource limits that present as a hindrance to using known security approaches. Because of the straightforward routing protocols, threats in sensor networks are highly susceptible. There are many insecurities and obstacles, such as limited resources and unreliable communication. Wireless sensor networks (WSNs) are networks of dedicated, spatially scattered sensors that track and record environmental physical variables and transmit the gathered information to a centralized point. WSNs can assess the state of the environment by measuring factors including temperature, sound, and pollution levels (Kamal, 2015). A WSN can be represented by hundreds or thousands of nodes, where each one communicates with other sensors. A node has several essential parts: a media transceiver with a connection to an external or an internal antenna, a circuit proposed to interface with the sensors, a microcontroller, and a power source such battery or another type of power source. From the size of a shoebox to (theoretically) a grain of dust, a sensor node can range in size (Ouni, 2022). A sensor node's price ranges from a few dollars to hundreds of dollars, depending on its size. Depending on how sophisticated it is, this range depends on its sophistication. Cost, size, and other things limit the sensor node manufacturing such as memory, energy,

Corresponding author: sura.20csp80@student.uomosul.edu.iq

communications bandwidth, and computational speed. WSN topology can differ from a kind of “simple star network” to an “advanced multi-hop wireless mesh network”. The Propagation can use flooding or routing (Widhalm, 2021), see Figure 1. We summarize the previous studies in Table1.

The rest of the paper is structured as follows: Section 2 collection process data set, Section 3, leach protocol, WSN-DS in Section 4, support vector machine (SVM) in Section 5, Motivation in Section 6, attacks in LEACH protocol LEACH in Section 7, and Confusion matrix in Section 8.

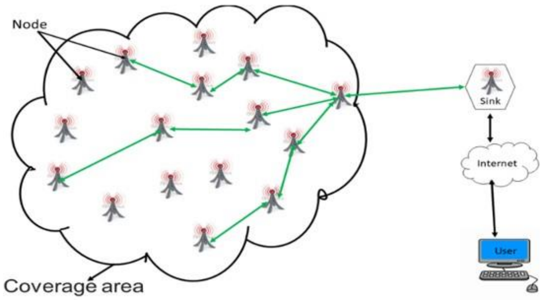

Figure 1. The general architecture of a wireless Sensor Network (Djedouboum, 2018).

Table 1: Summary of the studies on the WSNs localization in intrusion detection systems.

Study	*Method*	*Strength*
(Hidoussi, 2015)	Proposed intrusion Detection algorithm	Selective routing attacks and black holes
(Vinayakumar, 2019)	a deep neural network (DNN)	detecting future cyberattacks.
(Al-Maslamani, 2020)	Swarm Intelligence optimization (SI)	Detecting sinkhole attack
(Hachimi, 2020)	Multi-stage machine learning (ML-IDS)	detect 4 types of jamming attacks
(Hussain, 2020)	Multilayer Perceptron (MLP)	ANN classifier four types of DoS att.
(Singh, 2021)	Harmonic Search Algorithm (HSA)	Using uniform cluster size, a centralized Fixed-Cluster Architecture (FCA)
(Alsulaiman, 2021)	Waikato Environment for Knowledge Analysis (WEKA) to evaluate the efficiency of 5 machine learning algorithms	detecting flooding, grayhole, blackhole, and scheduling

2 Dataset Collection

Leach protocol is a TDMA (Time Division Multiple Access) based MAC protocol. The basic objective of this protocol is for improving the lifespan of WSN by reducing the consumed energy.
the Leach protocol can be divided into two phases:

1. Set-up phase
2. Steady phase

Self-adaptive and self-organized. Leach protocol uses round as a unit, each round is made up of a cluster set-up stage and steady-state storage to reduce unnecessary energy costs (Behera, 2022).

The process of acquiring data for use in research, strategic planning, business decision-making, and other applications. Effective data gathering offers the information required to provide answers, analyze corporate performance or other outcomes, and predict future trends, actions, and scenarios. It is a fundamental component of data analytics applications and research projects (Anarase, 2021).

3 Leach Protocol

LEACH “Low-Energy Adaptive Clustering Hierarchy” is a TDMA-based MAC protocol that is incorporated and integrated with a simple routing protocol and the clustering in WSN. The main target of the LEACH protocol is to reduce the power consumption required for creating and maintaining the clusters, thereby improving the lifetime of a WSN (Khediri, 2014).

The hierarchy of LEACH's structure allows for the transmission of nodes to the cluster leaders, who then gather and compress the data before sending it to the main station (sink). Every round, each node uses a random procedure to determine whether or not it will be a cluster head. LEACH assumes that each node has a medium capable of traveling straight to the base station or any other nearby cluster head but using a medium at its maximum power always results in energy loss (Tandel, 2016).

The nodes purposed for cluster heads couldn’t become cluster heads anymore for P rounds, where P is the required percentage of cluster heads. Then, the nodes again become cluster heads with a probability of 1/P. All nodes that did not represent a cluster head at the end of the round choose the closest cluster head and join that cluster. The cluster head has established a schedule for each node in its cluster to transmit data. Only the other nodes without cluster heads can connect with the TDMA cluster head via a specific technique, based on the cluster head's schedule. They do so using the minimum energy needed to reach the cluster head, and only need to keep their radios on during their time slot (Yang, 2014).

To reduce interference between clusters, LEACH also employs CDMA (Code Division Multiple Access), which assigns a unique set of CDMA codes to each cluster.

The paper's findings represent the most important security issues and challenges, as well as some security attacks in the WSNs. In addition, the collected data scheme was defined for processing to generate 12 features, which are known as WSN-DS. This dataset has been known as WSN-DS. This is the LEARN routing protocol of a WSN. In a field of 1000 square meters, it generates a network of 1000 nodes with random positions (Naeimi, 2012). The "threshold" parameter, which is part of LEACH's cluster head election probability p, is used to elect cluster leaders during the Set-Up phase. Data transmission takes place during the Steady State phase, during which energy dissipation values are computed. Graphs are presented towards the end, including one showing the number of transmissions. According to the outcomes you wish to attain, parameters are provided at the beginning and can be adjusted (Singh, 2017).

4 WSN-DS Data

For sensing data and transmitting it to the Base Station, the sensor nodes were diffused at particular locations for data collection, where data loss or delay depends on the sensor data transmission to BS and accuracy. The physical data can be sent to the BS by data collection data or dissemination. the main issue for sending or collecting the data from sensors to the BS is slow latency. The main objective of collecting data is for increasing the number of sensing cycles of sending data to the BS before the network shutdown (Nguyen, 2021). This leads to getting minimum power consumption and delay of each sensing operation. Signals have been picked up by all types of connected sensors and data acquisition units, then processed, and finally sending it to a specific node called a trough node.

The sink node orders the sensor information by sending a Query across the network. Then the node reacts to this query of data matching, then a response message is sent back to the storage node. Energy consumption in the network can be decreased by permitting the nodes moving which are called block headers. The collected data from nodes are collected and compressed by cluster heads. Then, the aggregated data was sent to the BS, but some problems are happening. The major problem is power consumption, which is located on the blockheads. to solve this problem, with the aid of cluster routing, will distribute power consumption over the cluster headers (Liu, 2018).

The capability of collected data refers to the efficiency of the basin for collecting sensor data from all distributed sensors when interference exists. The operation of the collected data function above the channel is causing massive waste of power. For example, in monolithic sensor networks, reinitiated is needed after operating for a while, which causes higher power waste. Minimum Distance is a key parameter for effective network lifespan and scalability. Distance is also a measure of node power at which transmission distance is reduced resulting in lower power consumption. The lifetime of a WSN can be determined in several ways. That is, it may be in terms of until the last node dies. If the first node dies. The power unit can be defined as the main unit in the WSN, which is in charge to supplies power to other units depending on the battery boundaries. so, the battery limits will affect the life of the WSN node therefore the sensor network’s lifespan. So, the main objective is for conserving energy and for improving the lifetime of the WSN. the block header in LEACH has been chosen by existing the ”maximum remaining power” and ”minimum distance between nodes” (Almomani, 2016).

1. No. of rounds: number of each round.
2. No. of the cluster: number of clusters in each round.
3. Time: the current simulation time of the round.

4-5 X, Y: the Site of each node.

6. Type: type of the node is cluster head or normal node.
7. packets-rcvd-CH: the number of data packets received from Cluster Head in normal (without attack).
8. packets-rcvd-CH: the number of data packets received from Cluster Head in (Blackhole attack).
9. packets-rcvd-CH: the number of data packets received from Cluster Head in (Sinkhole attack).
10. packets-sent-normal: the number of data packets sent to the BS (Base Station) in normal (without attack).
11. packet-sent-black: the number of data Black sent to the BS in (the Blackhole attack).
12. packet-sent-sink: the packets number of data sent to the BS (sinkhole attack).
13. min-dis: the minimum distance to the cluster Head.
14. Energy: energy of each node per round.

15. A _DV CH SENT: the number of advertising CHs broadcasting messages sent to the nodes.
16. distance: the distance to the CH.
17. Alive _nodes normal: the number of alive nodes per round in normal (without attack).
18. Alive _nodes _black: the number of alive nodes per round (Blackhole attack).
19. Alive _nodes _sink: the number of alive nodes per round in (Sinkhole attack).
20. Dead _nodes normal: the number of dead nodes per round in normal (without attack).
21. Dead _nodes _black: the number of dead nodes per round (Blackhole attack).
22. Dead _nodes sink: the number of dead nodes per round in (Sinkhole attack).

5 Support Vector Machine (SVM)

SVM can sometimes be called Support Vector Networks (SVMs). In machine learning, the SVN is defined as a special learning model that could be supervised and connected with specific learning algorithms for analyzing data for regression analysis and classification. Vapnik (1982, 1995) and Chervonenkis (1974) was conclude that the SVN or SVMs is one of the methods that can be a very robust prediction depending on the VC theory or statistical learning frameworks (Pal, 2006).

They used a collection of training examples, each example is marked as categories, and the SVM algorithm builds a prototype that specifies models to its category, which concludes an Unstable Binary Linear Classifier (Ahlawat, 2020).

Although SVM performs linear classification, it can easily perform an efficient non-linear classification using a Kernel Trick that is used for mapping the inputs to Large-Scale Feature Spaces. When the data is classified, the unsupervised learning approach is used instead of supervised learning because it is impossible to use in this classification, where it tries to discover the natural clustering of the data into categories which results to generate a map with this new data to these defined groups (Tang, 2019).

6 Motivation

Data classification is a prominent procedure in machine learning. Suppose that two classes of supplied data points exist, and the task is to determine which class a new data point will be in. In Support-Vector machines, a dataset is referred to as a p-dimensional vector, and it is possible to divide these points into different categories using a (p-1)-dimensional hyperplane; this technique is known as a linear classifier.

The data is classified by hyperplanes. The most popular option can be characterized as the greatest significant "Margin" or "Separation" between all classes (Wang, 2017). The purpose of selecting the hyperplanes is to maximize the amount of space on both sides between them and the following data point. The Maximum-Margin Hyperplane, if one exists, is where the linear classifier is located.

SVMs are useful for text and hypertext classification, the implementation of which can greatly reduce the need for categorized training cases in both standard inductive and inductive settings. Images can also be categorized using SVMs. Experimental results show that SVMs achieve (Meyer, 2015).

7 Attacks in LEACH Protocol

LEACH can be defined in the world of communication as a routing protocol with a hierarchical type utilized in WSN to raise the life of the networks. LEACH is a protocol used for self-organizing, formable, and clustering.

LEACH supposes that Base Station exists away from sensor nodes. In addition, the sensor nodes can be homogeneous and have bounded memory and energy. Sensors may contact together in addition they may contact the BS directly (Alnawafa, 2018). The LEACH protocol's popular idea is for arranging the nodes to divide the power consumed for all nodes in the network itself. According to the above, each cluster has a lot of nodes one of them is known as" Cluster Head" (CH), which collects the sensed data from the connected sensors in its cluster, then forwards them to the BS.

Each cycle in the LEACH protocol contains phases: the "Setup phase and the Steady-State phase ".Clusters in the Setup phase are formed, while in the case of the Steady-State phase, collected data from sensors will be sent to the sink node (Abid, 2018).

7.1 Sinkhole

Domain Name Service (DNS) Sinkhole "also can be known as a Blackhole DNS, Sinkhole Server, or Internet Sinkhole" is defined as a DNS server that was prepared to distribute Non-Routable addresses for a specific group of domain names. Computers that use the Sinkhole are failing to reach the required site (Alhawas, 2019). If the DNS resolution chain gets higher up the Sinkhole deals with more requests will be failed, the reason is due to the more significant number of lower NS needed to serve a more significant number of clients. Larger Botnets are becoming useless because of diffused TLD Sinkholes in the entire Internet (Abraham, 2018). DNS Sinkholes are active whenever detect and block threats, Bots, or other traffic, see Figure 2 The local host's file on a client's computer must be checked before the DNS servers are checked and could be used for blocking sites when checking. Sinkholes can be used for containing threats like WannaCry and Avalanche, and devastating them, for example, DNS services are disrupted in a DDoS attack.

Holing the DNS sink could be utilized for protecting clients by intercepting the requests of DNS trying for connecting to malware domains and returning an IP address of a Sinkhole server specified by the administrator of the DNS Sinkhole (Kumar, 2017).

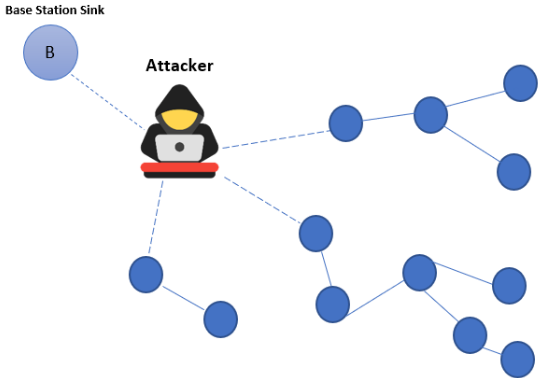

Figure 2. DNS Sinkholes(Khorgade, 2015).

7.2 Blackhole

Routing with filtering of a DDoS blackhole (sometimes called blackholing), is a countermeasure that reduces an attack of DDoS where the traffic of the network is guided into a "Black hole," and will lose.

When operating the filtering for the Blackhole is executed without any restriction criteria, where both harmful and normal network traffic is diverted to a blackhole or null route and ignored by the network (Rani, 2018).

There is no warning for erased data that will be a reversion to the source when protocols for connectionless communication, such as UDP, are proposed. An alert will be sent when the e-data has been dropped when utilizing "connection-oriented" protocols like TCP, which need a handshake to contact the target system, as seen in Figure 3.

Blackholing is the most readily available and dependable alternative for groups or communities that have no other justification for thwarting an attack (Bilgin, 2019). This approach to reduction in this example of a DDoS attack may have ramifications, making it an unsatisfactory choice for mitigating a DDoS attack. Like antibiotics, which kill both harmful and helpful germs" When this kind of DDoS is used incorrectly, it will haphazardly produce traffic sources that harm any service or network. Modern types of attacks use renewable attack vectors and IP addresses #. One of the best uses of Blackhole routing is when affected by good traffic, where the attacker's primary objective is to obstruct traffic to the target service or network. Blackhole routing can still be helpful even though it can aid a malevolent person in achieving their objective (Kaur, 2014).

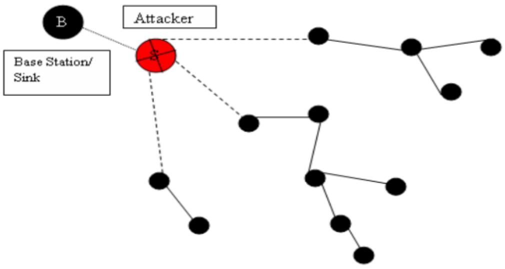

Figure 3. Blackhole routing (Rathod, 2011).

Figure 4 shows the structure of the network leach network protocol Where the network consists of a sum of cluster heads and one sink node or one base station. In the Leach protocol, nodes are randomly distributed in an area and then grouped into groups, each node is a member of a group and each group is its own. CH The nodes such as CH are chosen according to the distance of the nodes. The contract is CH (normal nodes) transmit their data to CH.

Figure 5 shows the nuclei that survive after each rhubarb, and it turned out that the node with weak energy will fade and die.

Figure 6 shows that we chose the nodes with the highest energy and it became clear to us after selecting the nodes that they were classified as the main nodes because they are the highest in terms of energy. The head of the cluster (CH) is chosen, so the node with the highest energy has the highest probability of becoming a CH. If a low-power node is identified as CH, it will quickly die affecting the network.

Figure 7 shows the Packet Sink node base station me Turns out it has information about the node. The packet is sent to the base station, which contains information about the nodes. The transmission of the CH to BS beam involves a long distance with high power consumption. CH-BS transmissions will quickly reduce CHS power.

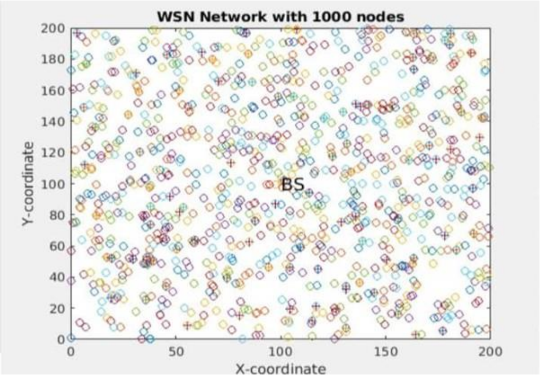

Figure 4. Leach network protocol

To avoid CHs dying faster than other nodes, the role of CH is cycled between nodes each round. Once a node becomes CH, it will not be eligible to become CH again during the following 1/P rounds. This approach effectively avoids a single node experiencing frequent long-distance transfers within a short period. This approach balances the load between nodes, extends network life, and ensures network quality is maintained for a longer period.

Figure 8 shows that we chose the nodes that receive packets form CH. In a certain period, the nodes in the cluster continue to send data to the CH node, otherwise, the node stops sending data and goes to sleep. If the source node is the normal node, it will send its data packets either directly to the BS, when it is closer to the BS than the CH, or indirectly via its CH. If a node is a CH, it will send data packets and packets collected from its members to the next CH as the next step to its final destination (BS).

Figure 9 shows that we chose the nodes that advertise CHs broadcasting messages sent to the nodes. Once the CHs are elected, they broadcast an ADV message. The Leach protocol works with a random set of CH each round. For each round, blocks are formed according to the announcement message sent by CH. The node broadcasts a CH-ADV announcement message to all nodes in the current round, announcing that it has become a CH via CSMA, even if the node is not a CH node (normal node). Each block header node broadcasts an ADV message using non-persistent carrier sense multiple access (CSMA).

This message is a small message containing the node identifier and a header that identifies this message as an advertisement message. Each non-clustered head node determines which cluster it belongs to by selecting the cluster header, which requires minimal communication power based on the strength of the signal received in an advertisement from each cluster header.

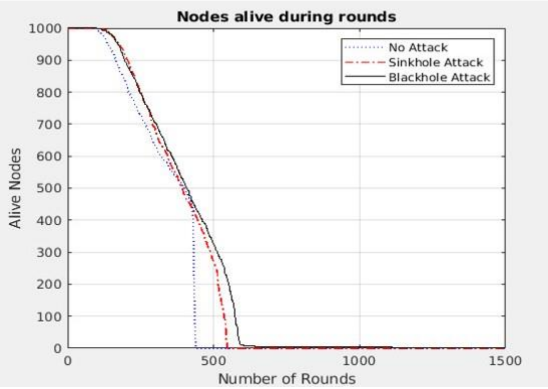

Figure 5. Alive nodes

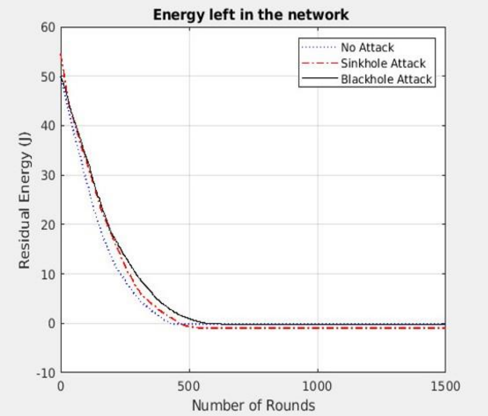

Figure 6. Energy.

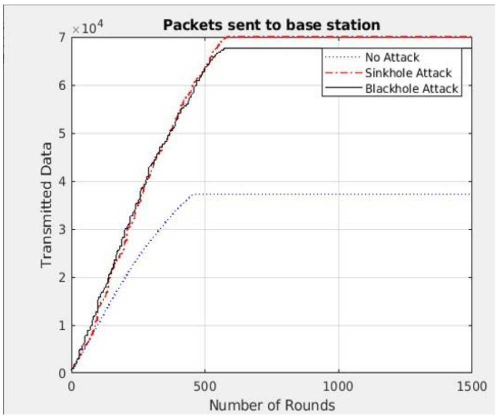

Figure 7. The packet sends to the base station.

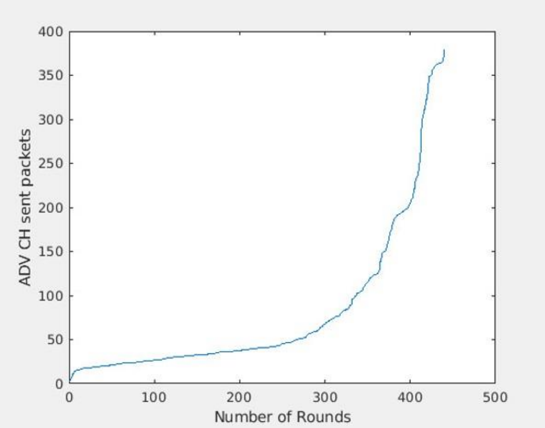

Figure. 8: packet received CH.

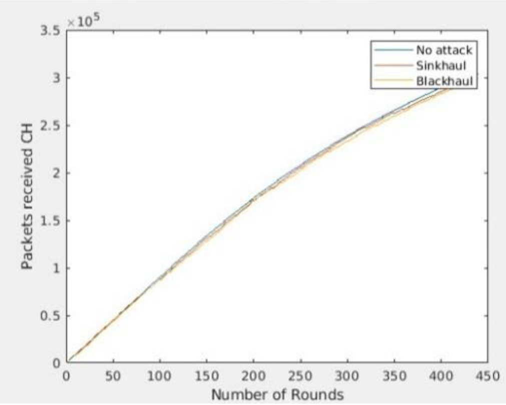

Figure 9. ADV_CH sent the packet.

8 Confusion Matrix

The Confusion matrix is a common measure proposed for fixing classification problems. It can be utilized for multiclass classification problems and binary classification (Maxwell, 2021).

Confusion matrices can be represented as actual and predicted values. The output "TN" stands for a True Negative, which is the accurately counted negative cases that were categorized. On the other side, “TP” represents a True Positive which refers to the classified accurate number of positive examples. The symbol “FP” refers to a False Positive value, which represents the number of actual negative examples that are classified as positive; and “FN” refers to a False Negative value, which represents the number of actual positive examples that are classified as negative. While performing classification, accuracy is the most popular metric used, through a confusion matrix the accuracy of a model could be calculated using Equation 1 (Ren, 2016).

$$\boldsymbol{Accuracy} = \frac{TN + TP}{TN + FP + FN + TP} \qquad (\mathbf{1})$$

Since accuracy can be deceptive when applied to unbalanced datasets, other metrics based on the confusion matrix can help assess performance. The "confusion matrix function" in the "sklearn" package of Python can be used to create a confusion matrix. The Python command "learn. metrics import confusion matrix" can be used to import this function. Users must supply the function with both actual and expected values to get a confusion matrix (Mittal, 2021).

The correctly categorized TP values, FP values that belong in another class but are in the relevant class, FN values that belong in another class but are in the relevant class, and correctly classified TN values that belong in the other class are all represented in the confusion matrix. Accuracy (ACC), precision (P), sensitivity (SN), specificity (SP), and F-score values are the most often utilized performance measures for classification based on these parameters.

According to Equations 2 and 3, both performance indicators are calculated based on the values in the confusion matrix (Dener, 2022).

$$precision = \frac{TP}{TP + FP} \quad \dots \qquad (\mathbf{2})$$

$$Recall = \frac{TP}{TP + FP} \quad \dots \qquad (\mathbf{3})$$

Table 2 shows the results of the detection rate for the training dataset.

Table 3: The results of the detection rate.

Attacks types	Accuracy	precision	Recall
Normal	1.00	1.00	1.00
Black hole	0.99	0.98	0.99
Sinkhole	0.99	0.98	0.99

Table 3 shows the results of the detection rate for the testing dataset.

Table 3: The results of the detection rate.

Attacks types	Accuracy	precision	Recall
Normal	1.00	1.00	1.00
Black hole	0.99	0.98	0.99
Sinkhole	0.99	0.98	0.99

9 Conclusions

Nowadays, mechanisms for effective security in Wireless Sensor Networks are needed. This article has described goals, constraints, security breaches, and obstacles by applying security mechanisms, defensive measures, and LEACH protocol layers for Wireless Sensor Networks. LEACH protocol that was used widely in WSN has several types of attacks, but the most popular are black holes and sinkholes. The SVM machine was selected to train the data train and test using a newly collected data set. The accuracy in the absences and presence of attacks in the case of the black hole and sinkhole ratios was excellent. As a suggestion in the future test new attacks on the network and use another AI technique.

Acknowledgments

We thank the "Computer Science Department, College of Computer Science and Mathematics, University of Mosul, Iraq" for helping us in doing this research.

References

Abid, S.H. 2018. OSCH-LEACH: Optimum Secondary Cluster Head Selection for LEACH Protocol. *AL-MANSOUR JOURNAL*AL-MANSOUR JOURNAL, (30)

Abraham, R.a.M., S. 2018. A study of Low Energy Adaptive Clustering Hierarchy (LEACH) Protocol in Wireless Sensor Network. *International Journal of Engineering Science Invention* 7(8 Ver. V) 99-102

Ahlawat, S.a.C., Amit 2020. Hybrid CNN-SVM classifier for handwritten digit recognition. *Procedia Computer Science* 167 2554--2560. doi:10.1016/j.procs.2020.03.309

Al-Maslamani, N.a.A., Mohamed 2020. Malicious node detection in wireless sensor network using swarm intelligence optimization. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. pp. 219--224.

Alhawas, A.a.T., Nigel 2019. Abandonment Attack on the LEACH Protocol. *European Workshop on Performance Engineering*. Springer. pp. 1--15.

Almomani, I.a.A.-K., Bassam and Mousa, AL 2016. Akhras. WSNDS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks. *Journal of Sensors* 2016. doi:10.1155/2016/4731953

Alnawafa, E.a.M., Ion 2018. New energy efficient multi-hop routing techniques for wireless sensor networks: Static and dynamic techniques. *Sensors* 18(6) 1863. doi:10.3390/s18061863

Alsulaiman, L.a.A.-A., Saad 2021. Performance evaluation of machine learning techniques for DOS detection in wireless sensor network. *arXiv preprint arXiv:2104.01963*arXiv preprint arXiv:2104.01963,

Anarase, D.S.a.o. 2021. Study and Implementation of Routing Protocols in Wireless Sensor Network for IoT Applications. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12(10) 4223--4230

Behera, T.M.a.S., Umesh Chandra and Mohapatra, Sushanta Kumar and Khan, Mohammad S and Appasani, Bhargav and Bizon, Nicu and Thounthong, Phatiphat 2022. Energy-Efficient Routing Protocols for Wireless Sensor Networks: Architectures, Strategies, and Performance. *Electronics* 11(15) 2282. doi:10.3390/electronics11152282

Bilgin, B.E.a.B., Selccuk 2019. A light-weight solution for blackhole attacks in wireless sensor networks. *Turkish Journal of Electrical Engineering and Computer Sciences* 27(4) 2557--2570. doi:10.3906/elk-1809-23

Dener, M.a.A., Samed and Orman, Abdullah 2022. STLGBM-DDS: An Efficient Data Balanced DoS Detection System for Wireless Sensor Networks on Big Data Environment. *IEEE Access* 10 92931--92945. doi:10.1109/ACCESS.2022.3202807

Djedouboum, A.C.a.A.A., Ado Adamou and Gueroui, Abdelhak Mourad and Mohamadou, Alidou and Aliouat, Zibouda 2018. Big data collection in large-scale wireless sensor networks. *Sensors* 18(12) 4474. doi:10.3390/s18124474

Hachimi, M.a.K., Georges and Gagnon, Ghyslain and Illy, Poulmanogo 2020. Multi-stage jamming attacks detection using deep learning combined with kernelized support vector machine in 5g cloud radio access networks. pp. 1--5.

Hidoussi, F.a.T.-C., Homero and Boubiche, Djallel Eddine and Lakhtaria, Kamaljit and Mihovska, Albena and Voznak, Miroslav 2015. Centralized IDS based on misuse detection for cluster-based wireless sensors networks. *Wireless Personal Communications* 85(1) 207--224. doi:10.1007/s11277-015-2734-2

Hussain, M.a.R., Jiadong and Akram, Awais 2020. Classification of DoS Attacks in Wireless Sensor Network with Artificial Neural Network. 22(3) 540--547

Kamal, Z.-E.a.S., Mohammad Ali and others 2015. Introduction to wireless sensor networks. *Wireless sensor and mobile ad-hoc networks*. Springer. pp. 3--32.

Kaur, G.a.S., Mandeep 2014. Detection of black hole in wireless sensor network based on data mining. *2014 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence)*. pp. 457--461.

Khediri, S.E.a.N., Nejah and Wei, Anne and Kachouri, Abdennaceur 2014. A new approach for clustering in wireless sensors networks based on LEACH. *Procedia Computer Science* 32 1180--1185. doi:10.1016/j.procs.2014.05.551

Khorgade, S.A.a.N., D Ghuse 2015. Attacks and Preventions in Wireless Sensor Network. *International Journal of Engineering Research and General Science* 3 2 Part 2

Kumar, S.R.a.T., M. and Umamakeswari, A. 2017. Analysis of Sinkhole Attack in Leach Based Wireless Sensor Network *International Journal of Pure and Applied Mathematics* 116(24) 185-197

Liu, Z.-z.a.L., Shi-ning 2018. Sensor-cloud data acquisition based on fog computation and adaptive block compressed sensing. *International Journal of Distributed Sensor Networks* 14(9). doi:10.1177/1550147718802259

Maxwell, A.E., Timothy A. Warner, and Luis Andrés Guillén. 2021. Accuracy assessment in convolutional neural network-based deep learning remote sensing studies—part 1: Literature review. *Remote Sensing* 13(13) 2450. doi:10.3390/rs13132450

Meyer, D.a.W., FT 2015. Support vector machines. *The Interface to libsvm in package e1071* 28 20

Mittal, M., Rocío Pérez de Prado, Yukiko Kawai, Shinsuke Nakajima, and José E. Muñoz-Expósito. 2021. Machine learning techniques for energy efficiency and anomaly detection in hybrid wireless sensor networks. *Energies* 14(11) 3125. doi:10.3390/en14113125

Naeimi, S.a.G., Hamidreza and Chow, Chee-Onn and Ishii, Hiroshi 2012. A survey on the taxonomy of cluster-based routing protocols for homogeneous wireless sensor networks. *Sensors* 12(6) 7350--7409. doi:10.3390/s120607350

Nguyen, M.T.a.N., Cuong V and Do, Hai T and Hua, Hoang T and Tran, Thang A and Nguyen, An D and Ala, Guido and Viola, Fabio 2021. Uav-assisted data collection in wireless sensor networks: A comprehensive survey. *Electronics* 10(21) 2603. doi:10.3390/electronics10212603

Ouni, R.a.S., Kashif 2022. Framework for Sustainable Wireless Sensor Network Based Environmental Monitoring. *Sustainability* 14(14) 8356. doi:10.3390/su14148356

Pal, M. 2006. Support vector machine-based feature selection for land cover classification: a case study with DAIS hyperspectral data. *International Journal of Remote Sensing* 27(14) 2877--2894. doi:10.1080/01431160512331314083

Rani, B.a.S., H. 2018. Blackhole attack detection and prevention in wireless sensor networks: a study. *Journal of Emerging Technologies and Innovative Research* 5(3) 461-465

Rathod, V.a.M., Mrudang 2011. Security in wireless sensor network: a survey. *Ganpat university journal of engineering & technology* 1(1) 35--44

Ren, D.a.A., Saleema and Lee, Bongshin and Suh, Jina and Williams, Jason D 2016. Squares: Supporting interactive performance analysis for multiclass classifiers. *IEEE transactions on visualization and computer graphics* 23(1) 61--70. doi:10.1109/TVCG.2016.2598828

Singh, R.a.R.K., C and Sharma, Rajnish and Vig, Renu 2021. Energy efficient fixed-cluster architecture for wireless sensor networks. *Journal of Intelligent & Fuzzy Systems* 40(5) 8727--8740. doi:10.3233/JIFS-192177

Singh, S.K.a.K., Prabhat and Singh, Jyoti Prakash 2017. A survey on successors of LEACH protocol. *IEEE Access* 5 4298--4328. doi:10.1109/ACCESS.2017.2666082

Tandel, R.I. 2016. Leach protocol in wireless sensor network: a survey. *International Journal of Computer Science and Information Technologies* 7(4) 1894--1896

Tang, T.a.C., Shengyong and Zhao, Meng and Huang, Wei and Luo, Jake 2019. Very large-scale data classification based on K-means clustering and multi-kernel SVM. *Soft Computing* 23(11) 3793--3801

Vinayakumar, R.a.A., Mamoun and Soman, KP and Poornachandran, Prabaharan and Al-Nemrat, Ameer and Venkatraman, Sitalakshmi 2019. Deep learning approach for intelligent intrusion detection system. *IEEE Access* 7 41525--41550. doi:10.1109/ACCESS.2019.2895334

Wang, H.a.X., Jinbo and Yao, Zhiqiang and Lin, Mingwei and Ren, Jun 2017. Research survey on support vector machine. *10th EAI International Conference on Mobile Multimedia Communications*. pp. 95--103.

Widhalm, D.a.G., Karl M and Kastner, Wolfgang 2021. An Open-Source Wireless Sensor Node Platform with Active Node-Level Reliability for Monitoring Applications. *Sensors* 21(22) 7613. doi:10.3390/s21227613

Yang, M.a.H., Jingsha and Zhang, Yuqiang 2014. Calculating the number of cluster heads based on the rate-distortion function in wireless sensor networks. *The Scientific World Journal* 2014. doi:10.1155/2014/602875

Yousif, Y.K.a.M., Omar H and Rashed, Zainab Abdulateef 2021. An Overview of Wireless Sensor Network (WSN) and Its Applications. 8 7

Biography

Sura Alsharifi is an M.Sc. student in Computer Science at the University of Mosul / Iraq.

Mafaz Alanezi is a faculty member at the Department of Computer Science, University of Mosul, Iraq. She obtained her Ph.D. degree in Computer Science in the field of Computer and Network Security from University of Mosul / Iraq in 2012. Her M.Sc. degree was also in Computer Science in the field of Image Processing from the University of Mosul/ Iraq in 2003. Her current scientific degree Prof. Dr in Cybersecurity and Information Security.