Anomaly Detection using Machine Learning Techniques in Wireless Sensor Networks

Samir Ifzarne, Hiba Tabbaa, Imad Hafidi, Nidal Lamghari
Department of Computer System and Technology, ENSA Khouribga, Morocco
E-mail: sifzarne@gmail.com

Abstract. The number of Wireless sensor network (WSN) deployments have been growing so exponentially over the recent years. Due to their small size and cost-effective, WSN are attracting many industries to use them in various applications. Environmental monitoring, security of buildings and precision agriculture are few example among several other fields. However, WSN faces high security threats considering most of them are deployed in unattended nature and hostile environment. In the aim of providing secure data processing in the WSN, many techniques are proposed to protect the data privacy while being transferred from the sensors to the base station. This work is focusing on attack detection which is an essential task to secure the network and the data. Anomaly detection is a key challenge in order to ensure the security and prevent malicious attacks in wireless sensor networks. Various machine learning techniques have been used by researchers these days to detect anomalies using offline learning algorithms. On the other hand online learning classifiers have not been thoroughly addressed in the literature. Our aim is to provide an intrusion detection model compatible with the characteristics of WSN. This model is built based on information gain ratio and the online Passive aggressive classifier. Firstly, the information gain ratio is used to select the relevant features of the sensor data. Secondly, the online Passive aggressive algorithm is trained to detect and classify different type of Deny of Service attacks. The experiment was conducted on a wireless sensor network-detection system (WSN-DS) dataset. The proposed model ID-GOPA results detection rate of 96% determining whether the network is in its normal mode or exposed to any type of attack. The detection accuracy is 86%, 68%, 63%, and 46% for scheduling, grayhole, flooding and blackhole attacks, respectively, in addition to 99% for normal traffic. These results shows that our model based on offline learning can be providing good anomaly detection to the WSN and replace online learning in some cases.

1. Introduction

Humans are always inventing new technologies according to their needs. The revolution of electronic components miniaturization process featuring wireless technologies influences our everyday life. With the popularity of smart phones, laptops and smart electronics in the post-PC era, Information Technology devices have become affordable, more mobile, more distributed and more omnipresent in the society. It is now possible to construct an embedded system in the size of a wallet with an equivalent capacity of a PC from the 90s [1]. Such embedded systems can be supported by the extent down Windows or Linux operating systems. In this regard, the appearance of Wireless Sensor Networks (WSNs) is essentially the latest tendency of Moore’s Law toward the miniaturization and ubiquity of computing devices.
Wireless sensor networks represent a special class of ad hoc networks [2]. They are made up of many smart sensor nodes of small sizes, limited power, at low-cost, and multi-functional (also called nanocomputers). In principle, these network nodes have a spontaneous mode of organization because they are intended to be deployed quickly and arbitrarily in a space of interest. They are powered by a power unit (battery) of limited capacity. They can capture (or collect) physical quantities from the environment such as temperature, wind speed, relative humidity, etc. They are also able to detect real-world events, process data, and communicate with each other to bring the information collected to a collection point called sink node or Base Station (BS) [3, 4]. This information is then transmitted via a transport network to a processing center where possible analyzes, interpretations, and decision-making are carried out by an end-user.

At the present time, wireless sensor networks have become one of the hottest research areas due to their wide range of real-time applications like critical military surveillance, battlefields, building security monitoring, forest fire monitoring, and healthcare [5]. The design of these applications assumes that all the nodes involved are cooperative and trustworthy. However, this is not the case in real-world deployments, where nodes are exposed to different types of attacks and intrusions that can downright damage the proper functioning of the network and degrades system performance. Unfortunately, ensuring the security of this type of network against various malicious attacks activities is a difficult task, especially when the nodes are made up of inexpensive electronic devices with limited hardware capabilities [6].

Cryptographic algorithms require significant energy consumption, processing, and memory. In general, cryptographic and authentication algorithms provide the services of confidentiality, integrity, and authentication, although, with the use of only an encryption algorithm and security level management, it is difficult to guarantee that the data is legitimate and did not suffer any type of attack that extracted sensitive data, and use them for a malicious reason [7]. Whilst the cryptographic techniques solutions have been found to reduce cyber-attacks, but they have not eliminated them completely. Detection-based approaches are then proposed to protect WSNs from well-know and new cyber-attacks, as a second-line defense [8].

Intrusion detection systems (IDS) are one of the most flexible and useful tools to guard WSNs from known and unknown attacks. IDS observes and analyzes the events generated in the network to detect anything unusual and alert sensor nodes about the intruder [4,6]. This concept was originally proposed by Anderson [9]. The strategies broadly utilized to develop IDS used for attack detection nowadays are vastly related to machine learning techniques. Most approaches, however, are based on offline learning which requires all, or at least a sample, of historical data to be kept in memory. But, there are few approaches of detection anomalies that are actually learning models online. The paper is organized as follows: In the next section, we present in related work. Section 3 describes feature selection algorithms with presenting the incremental learning model with a cluster-based WSN. The simulation results used to evaluate the performance of the proposed model are presented in Section 4. Finally, the paper ends with a conclusion and perspectives.

2. Related work

WSNs are not excluded from the intrusion attacks and security threats, which lead to data privacy leaks or a decrease in its performance and efficiency. This is why it motivates the growing research efforts to build efficient intrusion detectors for sensor networks adapted to their specific characteristics. Various studies proposed machine learning solutions for IDS to detect intrusion in WSNs. The existing intrusion detection methods mainly include offline learning approaches
such as Support vector machines, Random Forest, Artificial neural newtork, Decision tree and other methods. In literature there are only few works that aim to use online learning as an approach to benefit from the advantages of those techniques.

Almomani et al. [10] have developed a new specialized WSN dataset, and the collected dataset is called WSN-DS. It contained regular network traffic and several DoS (Flooding, Grayhole, Blackhole and scheduling attacks) scenarios in WSN. It is created based on LEACH protocol, which is one of the most popular hierarchical routing protocol in WSNs. Using the network simulator NS2 to collect data. A (WEKA) data-mining toolbox was used for implanting artificial neural network (ANN) to detect the 4 attacks and classify them. The results were classified using both 10 folds cross-validation and holdout splitting methods. From analyzing the research work, the mechanism using the algorithm ANN trained by WSN-DS achieved a high classification of DoS attacks excluding the grayhole attack since the detection rate of her is very low compared to the others.

Dong et al. [11] proposed an intrusion detection model based on information gain ratio and Bagging algorithm for detecting DoS attacks in a cluste-based WSNs. The authors used information gain ratio to reduce unnecessary features. The Bagging algorithm was used to construct an ensemble algorithm to train a set of C4.5 decisions trees in the aim of improving them. The proposed model was implemented by using both NSL-KDD and WSN-DS dataset separately to examine the performance of the model. This method provides enhanced performance than other methods.

Abdullah et al. [12] have studied a set of machine learning techniques for detecting DoS attacks with an IDS applied for WSNs. Support vector machine (SVM), Naïves Bayesian, Random Forest, and Decision Tree (j48) classifiers were implemented with the WEKA data mining tool using WSN-DS as a dataset. From the results of this study, the SVM classifier has the upper hand in detecting intrusions with a high detection rate compared to the other techniques.

Sindhu et al. [13] have constructed a new lightweight IDS aimed for detecting anomalies in WSNs based on DT classification algorithm in WSN. For the implementation the authors chose to use Kddcup'99 as a dataset for relevant data. The model is based on three steps, in the first step feature selection method was implemented to remove irrelevant features for better results. The important features then were used in a wrapper based feature selection algorithm to identify suitable subset. The last step was adapting the learning paradigm neurotree in IDS. The authors claim that applying the right features with neurotree is a promising strategy for intrusion detection. Indeed, the model presented higher detection accuracy.

Pachauri et al. [14] have examined machine learning techniques, classification and regressions algorithms on real medical dataset with their proposed framework to detect faults and anomalies. The framework combines random forests algorithm for classification jobs and additive regression techniques for prediction jobs for anomaly detection in medical WSNs. The authors declare that their approach gives more accurate results than other existing fault detection mechanisms and both these algorithms perform much better than other previous research techniques.

Cauteruccio et al. [15] proposed a novel approach for Short-long term anomaly detection in heterogeneous wireless sensor networks based on machine learning and multi-parameterized edit distance, their method is performed by applying the analysis of edge and cloud on real data, which has been developed inside residential building and then deformed with a set of fake impairments. The obtained results show that the proposed method can self-adapt to the
environment variations and correctly identify the anomalies.

Bosmana et al. [16] have proposed a new lightweight framework for online anomaly detection in IoT applications including WSNs based on ensembles of incremental learners. Their decentralised approach was able to perform better than each individual centralised offline learner alternatives to detect anomalies, even in environments with little a priori knowledge, finding that ensemble schemes are feasible for practical implementation. The implementation used various large synthetic and real-world datasets, the evaluation of the proposed model was based on the prediction accuracy and confusion matrix metrics.

Bosman et al. [17] have proposed a decentralized anomaly detection system for WSNs using unsupervised online learning approach. Central techniques have several drawbacks and for that an implementation with a range of real-world network deployments and data-sets were used to detect anomalies, also reducing energy and spectrum consumption by incorporating neighborhood information approach and using Recursive Least Squares (RSL) to learn linear models.

Rassam et al. [18] have introduced a variation of PCA called the One-Class Principal Component Classifier (OCPCC) for local and unsupervised anomaly detection, taking into consideration the energy consumption in WSN that uses the Candid Covariance free Incremental Principal Component Analysis (CCIPCA) algorithm to detect the intrusions as they occur. The implementation used GSB as a dataset and the approach is divided into two phases, the offline phase a PCA model is trained using normal data collected from each sensor to build the normal behavior model, the online detection phase when the sensor nodes classify every packet as either normal or abnormal according to the threshold specified in a global normal model (GNM). The normal PCA model is updated and retrained with new mean and standard deviation of the new data. The proposed model achieved 96% as Detection accuracy with 7.2% as False Detection Rate.

Martins et al. [19] have proposed an online anomaly detection using a Least Squares-Support Vector Machine algorithm (LSSVM), under the form of a Reproducing Kernel Hilbert Space (RKHS) with Radial Basis Function (RBF) kernel, along with a sliding window-based learning technique. The proposed model was tested on a dataset generated with a virtual system that was used to assess the performance of the proposed approach. Simulation results have shown the out-performance of the proposed approach.

Myint et al. [20] have proposed one classifier known as Incremental Learning Algorithm (ISVMM), which is based on a support vector machine with Mahalanobis distance [12]. In this, a prediction is done by using SVM and is going to reduce steps required for calculation and complexity of the algorithm. This is achieved via finding a support set, error set, remaining set and providing a hard and soft decision. Time is then saved for repeatedly training the dataset. The authors used for simulation KDD Cup99 as a dataset to check the performance of the system. the proposed ISVMM model can predict well on all of the 41 features without reducing the dimensionality of the dataset.

In this paper, we will use in our experiment a specialized dataset WSN-DS in order to classify four types of DoS attacks: Blackhole, Grayhole, Flooding, and Scheduling among normal network traffic. We will compare three feature selection methods with the online Passive-Aggressive classifier, and examine his performance with each method and find the pair that achieve better results. We will propose an intelligent, efficient, and learnable model using the online classifier Passive-Aggressive with applying feature reduction, and ensuring that the model is compatible with the characteristics of WSN.
3. Research Methodology

3.1. Leach protocol:

LEACH (Low Energy Adaptive Clustering Hierarchy) is one of the main proactive sensor network protocols, it is a self-organizing hierarchical routing protocol based on adaptive clustering used in RCSF to minimize the energy consumption of network elements in order to increase the lifetime of the latter [21–23]. Leach was proposed by Wendi B. Heinzelman of MIT [24]. LEACH assumes that Base Station (BS) is fixed and located far from the sensor nodes. In addition, all sensor nodes are homogeneous and have limited energy and memory. The sensors can communicate with each other and they can communicate directly with the BS. The main idea of the LEACH protocol is to organize the nodes into clusters to distribute the energy between all the nodes of the network. Thus, in each cluster, there is a master node called Cluster Head (CH) which gathers the data received from the sensors of its cluster and transmits it to the base station which allows to minimize consumption and reduce the amount of information sent at the base station.

![WSN network topology based on LEACH protocol.][10]

3.2. Feature Selection:

Some predictive model problems have a large number of variables that can slow the development and training of the models and require a large amount of system memory. Additionally, the performance of some models can degrade when including input variables that are not relevant to the target variable.

Feature selection methods in the WSN are data pre-processing methods that are intended to reduce the number of irrelevant input variables to those that are believed to be most related to the intrusion attack. Relevant features have decisive effects on the output of classification, such as increasing the efficiency of the IDS and reducing energy consumption. For this reason, we choose 3 feature selection methods that are known to give a great performance to obtain the effective one with our model.

Chi-squared:

The chisquared statistic is used to compute a score between the target and the numerical variable and only select the variable with the maximum chi-squared values. In feature selection,
chi-squared measures the independence of features with respect to the class. The initial beliefs in is that the feature and the class are independent before computing a score [25]. A score with high value means the existence of a high-dependent relationship.

$$X^2 = \frac{(Observed\ frequency - Expected\ frequency)^2}{Expected\ frequency}$$ (1)

Where:
- Observed frequency = Number of observations in class.
- Expected frequency = Number of expected observations of class if there was no relationship between the feature and target attribute.

**Information gain**

Information gain used in determining relevant features from a set of features. Before the start of the learning process it is used to rank and select the top features to reduce the feature size based on information theory. The greater the information gain, the more important the features are. Prior to ranking, the entropy value of the distribution is measured to determine the uncertainty of each feature according to their relevance in determining different class [26]. The entropy of the variable X is defined as follows:

$$H(X) = -\sum_{i=0}^{n} P(x_i) \log_2(P(x_i))$$ (2)

where $P(x_i)$ is the value of prior probabilities of X. The entropy of X after observing values of another variable Y is defined as:

$$H(X/Y) = -\sum_{j} P(y_j) \sum_{i} P(x_i|y_j) \log_2(P(x_i|y_j))$$ (3)

Where in Eq.3 $P(y_j)$ is the prior probability of the value $y_j$ of Y, and $P(x_i|y_j)$ is the posterior probability of X given Y. The information gain is defined as the amount by which the entropy of X decreases to reflects additional information about X provided by Y and is defines as:

$$IG(X|Y) = H(X) - H(X|Y)$$ (4)

According to this measure, if $IG(X/Y) > IG(Z/Y)$ then the feature Y and X are more correlated than feature Y and Z. The ranking used to select the most important features is calculated using the equation 4.

**Information gain ratio**

The purpose of information gain ratio is to improve the bias of information gain towards features with large diversity value [27].

$$GR(X) = \frac{IG(X)}{H(X)}$$ (5)

where GR(X) is the information gain ratio of feature X. Gain ratio takes number and size of branches into account when choosing an attribute and corrects the information gain by taking the intrinsic information of a split into account. Intrinsic information is the information about the class is disregarded.
3.3. **Online Machine Learning:**

Online learning (also known as incremental or out-of-core learning) [28] is a method of machine learning that builds a learnable model for effective classification in the real-time detection where the data is coming from multiple sensors. Avoiding the traditional machine learning techniques (also known as offline or batch learning) that require time and great computing to process the data, the model uses only previously provided data. The offline learning may require frequent model updates manually on newer data and then deploying the resulting model again every time the normal system behavior changes.

Incremental learning techniques allow the model to be updated after receiving new data and making the model learns over time, without requiring a large historic data-set to be kept in memory. The structure of incremental learning classifiers can detect novel intrusions and handle concept drift in a dynamic network that is changed over time.

3.4. **Online Passive-Aggressive Algorithm:**

Online Passive-Aggressive Algorithm (PA) is a family of online learning algorithms (for both classification and regression) proposed by Crammer et al. [29] it is similar to support vector machine classifier and can be considered as the online version of it. The idea is very simple and his performance has been proved to be superior to many other alternative methods like Online Perceptron and Margin-infused relaxed algorithm (MIRA) algorithm. The PA classifier learns from streaming data and try to find hyper-planes to separate the instance into halves.

**Algorithm 1** Passive-aggressive classifier

1: **Initialize:**

\[ w_t \leftarrow (0, \ldots, 0) \]

2: **for** \( t = 1, 2, \ldots \)** **do**

- Receive instance: \( x_t \in \mathbb{R}^n \)
- Predict: \( y_t \leftarrow \text{sign}(w_t . x_t) \)
- Observe correct label: \( y_t \in \{-1, +1\} \)
- Suffer loss: \( l_t \leftarrow \max \{0, 1 - y_t (w_t . x_t)\} \)
- Set: \( \tau \leftarrow l_t / \|x_t\|^2 \)
- Update: \( w_{t+1} \leftarrow w_t + \tau_t y_t x_t \)

3: **end for**

Where \( w_t \) is the weight of the vector on round \( t \), \( y_t \) is the signed margin. \( w_{t+1} \) is set to be the projection of \( w_t \) in the half-space of vectors that achieve a hinge-loss of zero. The algorithm is passive when a correct classification occurs having a hinge-loss as zero otherwise the classifier adjusts its weight vector for each misclassified training sample it receives. The PA classifier tries to get correct classification and updates the classification model. Online passive-aggressive classifier gives better results as its learning rate does not decrease with respect to time making him suitable solution for WSN.

WSN Intrusion detection model based on information gain ratio and online passive-aggressive algorithm, the shortened form is ID-GOPA. The main purpose of the proposed model, Figure 2, is to apply the study of the online classifier for the streaming data of the network. ID-GOPA inspects all events circulating in the network by observing abnormal activities and it consists of two phases: the offline and the online phase.
Figure 2. The structure of the proposed ID-GOPA model.

- In the offline phase (training dataset), the model is trained by the online classifier PA to be more familiar and more learnable for existing activities in the network flow, where the processed and labeled learning records are introduced for build a learnable model capable of being tested.
- In the online phase, using the trained model from the offline phase with the same prepossessing engine selecting only the relevant attribute based on information gain ratio algorithm and classifying every packet as either normal or attack in real-time detection.

4. Experiments and analysis

4.1. WSN-DS Dataset:

The experiment uses a simulated wireless sensor network-detection system (WSN-DS) dataset developed by Almomani et al. [10], and the network simulator NS-2 was used to simulate wireless sensor network environment based on the LEACH routing protocol to collect data from network and preprocessed to generate 23 features identifying the state of each sensor, and simulates four different types of Denial of Service (DoS) attacks: Blackhole, Grayhole, Flooding, and Scheduling, the simulation parameters are summarized in Table 1. Only 19 features including the class label were in the dataset file as showing in Table 2. This dataset was generated as an IDS dataset to apply machine learning techniques in order to detect and classify DoS attacks. The data distribution is shown in Figure 2.

The technical characteristics of the computer adopted in the implementation phase are:

- Central Processing Unit: Intel(R) Core(TM) i7-4610M CPU @ 3.00GHz 3.00GHz
- Random Access Memory: 8 GB
- Operating System: Windows 7 Pro 64-bit
Table 1. WSN Simulation parameters.

| Parameter                  | Value          |
|---------------------------|----------------|
| Number of nodes           | 100 nodes      |
| Number of clusters        | 5              |
| Network area              | 100m × 100m    |
| Sink Location             | (50,175)       |
| Size of packet header     | 25 bytes       |
| Size of data packet       | 500 bytes      |
| Routing protocol          | LEACH          |
| Simulation time           | 3600 s         |

Table 2. Features of the WSN-DS Dataset.

| Feature number | Symbol   | Feature name      | Description                                                      |
|----------------|----------|-------------------|------------------------------------------------------------------|
| 1              | id       | Node Id           | A unique ID number of the sensor node                             |
| 2              | Time     | Time              | The run-time of the node in the simulation                       |
| 3              | IS_CH    | Is CH             | Describes if the node is a CH or not                             |
| 4              | WHO_CH   | Who CH            | Cluster head ID                                                  |
| 5              | Dist_to_CH| Distance to CH   | Distance between node and CH                                     |
| 6              | ADV_S    | ADV CH sends      | Number of the advertise CH’s broadcast messages sent to nodes    |
| 7              | ADV_R    | ADV CH receives   | Number of advertise messages received by the nodes from CH       |
| 8              | JOIN_S   | Join request send | Number of join request messages sent by the nodes to the CH      |
| 9              | JOIN_R   | Join request receive | Number of join request messages received by CH from nodes  |
| 10             | SCH_S    | ADV SCH sends     | messages of TDMA schedule broadcast sent to the nodes          |
| 11             | SCH_R    | ADV SCH receives  | Number of scheduled messages received by the CH                  |
| 12             | Rank     | Rank              | Node order in TDMA scheduling                                    |
| 13             | DATA_S   | Data sent         | Number of data packets sent from the node to its CH             |
| 14             | DATA_R   | Data received     | Number of data packets received by the node from the CH         |
| 15             | Data_Sent_to_BS| Distance sent to BS | Number of data packets that are sent from node to the BS     |
| 16             | dist_CH_to_BS| Distance CH to BS | Distance between CH and BS                                       |
| 17             | send_code | Send code         | The sending code of the cluster                                  |
| 18             | Consumed_Energy | Energy consumption | Energy consumed                                                |
| 19             | Attack type | Attack type     | Type of attacks or normal traffic                                |

Table 3. The dataset separated into training and testing set.

| The Attack Type | Training Set(60%) | Testing Set(40%) |
|-----------------|-------------------|------------------|
| Normal          | 204174            | 135892           |
| Grayhole        | 8653              | 5943             |
| Blackhole       | 5999              | 4050             |
| Scheduling      | 4007              | 2631             |
| Flooding        | 1963              | 1349             |
| Sum             | 224796            | 149865           |

The dataset was split into training and testing sets with 60% of the data were used as the training data set and 40% of the data were used as the test data set. The number of observations in these two sets is presented in Table 3.
4.2. Performance evaluation:

The results of this study are evaluated according to four criteria, namely accuracy (ACC), precision (PR), f1-score (F), and recall (RE). All these criteria take a value between 0 and 1. When it approaches 1, the performance increases, while when it approaches 0, it decreases. These performance evaluation metrics are computed as:

- **Accuracy (Acc)**: It estimates the ratio of the correctly recognized records to the entire test dataset. Accuracy serves as a good measure for the test dataset that contains balanced classes and defined as follows:

  \[
  \text{Accuracy} = \frac{TP + TN}{TP + FP + FN + TN}
  \]  \hspace{1cm} (6)

- **Precision (PR)**: Or Positive Predictive value (PPV) presents the ratio of the correctly classified data as the attack to all data classified as the attack and it is defined as follows:

  \[
  \text{Precision} = \frac{TP}{TP + FP}
  \]  \hspace{1cm} (7)

- **Recall (RE)**: It is also called as True Positive Rate (TPR) or (Sensitivity), it estimates The ratio of data classified as an attack to all attack data:

  \[
  \text{Recall} = \frac{TP}{TP + FN}
  \]  \hspace{1cm} (8)

- **F1-Score (F)**: or F1-Measure represents the harmonic mean of the two matrices Precision and Recall. This concept is used to express the overall success:

  \[
  F1 - \text{Score} = \frac{2 \times PR \times RE}{PR + RE}
  \]  \hspace{1cm} (9)

The four values summarized below are used:

- True positive (TP) represents the number of correctly classified attack instances (correct detection).
- True negative (TN) represents the number of successfully classified normal data as being normal (correct rejection).
- False positive (FP) is the number of wrongly classified attack instances.
- False negative (FN) is the number of wrongly classified normal instances.
4.3. Feature selection:

In this study, feature selection methods chi-squared, information gain and information gain ratio are used with WSN-DS data for comparative analysis of each one using the online PA algorithm to verify the results of the selection. The selected features and performance are shown in Table 4.

Through the experiment using Acc as an evaluation index, it can be seen from Table 4 that the algorithm chi-squared and Information gain both of their Acc reached 90.68%. In the other hand when using the information gain ratio the Acc has gotten higher to 95.69% which means that the proposed WSN intrusion detection model has a better classification accuracy when choosing the information gain ratio as the attribute selection method. The selected feature set is S={3,5,6,7,8,9,10,11,12,13,15,16,17,18}.

| Feature selection method | Feature selection result | Irrelevant feature | Accuracy (%) |
|--------------------------|--------------------------|--------------------|--------------|
| Information gain ratio   | 3,5,6,7,8,9,10,11,12,13,15,16,17,18 | 1,2,4,14          | 95.69        |
| chi-squared              | 1,2,3,4,5,6,7,9,10,12,13,14,15,16 | 8,11,17,18        | 90.68        |
| Information gain         | 1,3,4,5,6,7,8,10,11,12,13,15,17,18 | 2,9,14,16         | 90.68        |

4.4. Simulation results and Discussion:

Table 5 presents the detection performance of the proposed WSN intrusion detection model for normal scenario and with the attacks, using WSN-DS dataset, such as Blackhole, Grayhole, Flooding, and Scheduling. The whole accuracy amount is 96%, as we analyze each class label to observe each individual performance, we see that the detection performance of normal cases is very high compared to abnormal cases with detection rate of 99%. And about the detection rate of Scheduling, Grayhole and Flooding attacks is 86%, 68% and 63%, respectively, on the other hand the Blackhole attack got the worst detection rate with a percentage of 46%.

Table 6 presents the detection performance of the proposed WSN intrusion detection model for normal scenario and with the attacks, using WSN-DS dataset, such as Blackhole, Grayhole, Flooding, and Scheduling. The whole accuracy amount is 96%, as we analyze each class label to observe each individual performance, we see that the detection performance of normal cases is very high compared to abnormal cases with detection rate of 99%. And about the detection rate of Scheduling, Grayhole and Flooding attacks is 86%, 68% and 63%, respectively, on the other hand the Blackhole attack got the worst detection rate with a percentage of 46%.

We have to take in consideration that the Passive-Aggressive classifier learns from streaming data, as the the classifier learns, he tries to train the model better and also the accuracy gets better over time/iterations. A general trend is that individual online learning classifiers are characterized by a reduced recall and from the results obtained high accuracy was achieved in the task of classifying four DoS attacks to determine whether the protocol in its normal mode or exposed to any type of attack.
Table 6. Online Passive Aggressive Results.

|         | PR  | RE  | F   |
|---------|-----|-----|-----|
| Normal  | 0.99| 0.99| 0.99|
| Grayhole| 0.52| 0.68| 0.59|
| Blackhole| 0.73| 0.46| 0.57|
| Scheduling| 1.00| 0.86| 0.93|
| Flooding | 0.93| 0.63| 0.75|
| Weighted avg. | 0.96 | 0.96 | 0.96 |
| Overall Accuracy | 0.96 |      |      |

4.5. Comparison with existing offline learning algorithms:

Table 7. Comparison of performance of different methods of WSN intrusion detection model.

|         | PR  | RE  | F   | Acc (%) |
|---------|-----|-----|-----|---------|
| SVM     | 0.88| 0.92| 0.90| 89%     |
| Naïve Bayes | 0.94| 0.85| 0.88| 94%     |
| Random Forest | 0.94| 0.85| 0.88| 94%     |
| Decision Tree | 0.94| 0.94| 0.93| 94%     |
| ID-GOPA     | 0.96| 0.96| 0.96| 96%     |

For the purpose of comparison, four algorithms of machine learning are considered, namely SVM, NB, RF, DT to compare our work with using the same dataset (WSN-DS) and the specific results of performance comparison were measured and compared using Recall, precision, F1-score and accuracy index. As can be seen from Table 7, the RE of the proposed method reaches 96%, which is higher than that of SVM, NB, DT, and RF. Among them, the Acc of SVM method is 89%, which is the smallest compared with the above methods. The mathematical reason behind the low accuracy is that SVM works better for small dataset and in our experimentation, we have used large dataset. Again, we have mentioned that the accuracy of Online PA classifier is high because it works better for large stream dataset and we have used large dataset for our experimentation in addition it gives better results, as it’s learning rate does not decrease with respect to time since most of the online algorithms their concepts might change through time.

5. Conclusion

Providing security services in WSN based on intrusion detection systems to identify attacks with high accuracy is a challenging task. In this paper we have presented an intelligent intrusion detection model based on incremental machine learning. The model determines the presence of an intrusion, and classifies the type of attack in real-time based on a cluster WSN network topology. The proposed model ID-GOPA efficiently detects intrusion, and avoids the resource waste. It used information gain ratio as a feature selection to reduce the parameters and processing load. Feature selection is an important factor which improves the performance of the model with the passive-aggressive algorithm as an incremental learning machine. The simulation results shows an overall accuracy of 96% which means our model is very accurate compared to...
offline models. Our model is applicable to any application which make it advantageous compared to existing models which are specific to their applications.

As future improvement work, we plan to go further by combining an ensemble of algorithms to detect anomalies. This would theoretically result in a better detection accuracy since there are more algorithms working together to overcome each other’s limitations.

References
[1] Yu Y, Krishnamachari B and Kumar V P 2006 Information processing and routing in wireless sensor networks (World Scientific)
[2] Ha R W K 2006
[3] Gungor V C, Lu B and Hancke G P 2010 IEEE transactions on industrial electronics 57 3557–3564
[4] Rassam M A, Maarof M and Zainal A 2012 American Journal of Applied Sciences 9 1636
[5] Marriwala N and Rathee P 2012 An approach to increase the wireless sensor network lifetime 2012 World Congress on Information and Communication Technologies (IEEE) pp 495–499
[6] Butun I, Morgera S D and Sanck R 2013 IEEE communications surveys & tutorials 16 266–282
[7] El Mourabit Y, Bouirden A, Toumanani A and Moussaid N 2015 International Journal of Advanced Computer Science and Applications 6 164–172
[8] Ping Y, Xinghao J, Yue W and Ning L 2008 Journal of systems engineering and electronics 19 851–859
[9] Anderson J P 1980 Technical Report, James P. Anderson Company
[10] Almomani I, Al-Kasasbeh B and Al-Akhras M 2016 Journal of Sensors
[11] Abdullah M A, Alsolami B M, Alyahya H M and Alotibi M H 2018 Journal of fundamental and Applied Sciences 10 298–303
[12] Sindhu S S S, Geetha S and Kannan A 2012 Expert Systems with applications 39 129–141
[13] Pachauri G and Sharma S 2015 Procedia Computer Science 70 325–333
[14] Cauteruccio F, Fortino G, Guerrieri A, Liotta A, Mocanu D C, Perra C, Terracina G and Vega M T 2019 Information Fusion 52 13–30
[15] Bosman H H, Iacca G, Tejada A, Wörtche H J and Liotta A 2015 Ad hoc networks 35 14–36
[16] Bosman H H, Iacca G, Tejada A, Wörtche H J and Liotta A 2017 Information Fusion 33 41–56
[17] Rassam M A, Maarof M A and Zainal A 2014 Knowledge-Based Systems 60 44–57
[18] Martins H, Palma L, Cardoso A and Gil P 2015 A support vector machine based technique for online detection of outliers in transient time series 2015 10th Asian Control Conference (ASCC) (IEEE) pp 1–6
[19] Myint H O and Meesad P 2009 Incremental learning algorithm based on support vector machine with mahalanobis distance (isvmm) for intrusion prevention 2009 6th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology vol 2 (IEEE) pp 630–633
[20] Heinzelman W R, Chandrakasan A and Balakrishnan H 2000 Energy-efficient communication protocol for wireless microsensor networks Proceedings of the 33rd annual Hawaii international conference on system sciences (IEEE) pp 10–pp
[21] Liu H, Li L and Jin S 2006 Cluster number variability problem in leach International Conference on Ubiquitous Intelligence and Computing (Springer) pp 429–437
[22] Heinzelman W B, Chandrakasan A P and Balakrishnan H 2002 IEEE Transactions on wireless communications 1 660–670
[23] Xu J, Jin N, Lou X, Peng T, Zhou Q and Chen Y 2012 Improvement of leach protocol for wsn 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery (IEEE) pp 2174–2177
[24] Devi K L, Subathra P and Kumar P 2015 Tweet sentiment classification using an ensemble of machine learning supervised classifiers employing statistical feature selection methods Proceedings of the Fifth International Conference on Fuzzy and Neuro Computing (FANCCO-2015) (Springer) pp 1–13
[25] Tesfahun A and Bhaskari D L 2013 Intrusion detection using random forests classifier with smote and feature reduction 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies (IEEE) pp 127–132
[26] Baig Z A, Sait S M and Shaheen A 2013 Engineering Applications of Artificial Intelligence 26 1731–1740
[27] Zheng J, Liu Z, Zeng Y, Cui L and Ji Z 2017 A survey on incremental learning Proceedings of the 5th International Conference on Computer, Automation and Power Electronics, Colombo, Sri Lanka pp 25–27
[28] Crammer K, Dekel O, Keshet J, Shalev-Shwartz S and Singer Y 2006 Journal of Machine Learning Research 7 551–585