An Analysis of a Signature-based Approach for an Intrusion Detection System in a Wireless Body Area Network (WBAN) using Data Mining Techniques

---

A Master's Project Report presented to
Department of Network and Computer Security

In Partial Fulfillment of the Requirements for the

Master of Science Degree

State University of New York Polytechnic Institute

By

Serene Elisabeth Medina, medinas@sunypoly.edu
SUNY Polytechnic Institute, Graduate Student
New York, United States

Under the supervision of
Dr. Hisham Kholidy, hisham.kholidy@ sunypoly.edu
Department of Network and Computer Security

Table of Contents

Abstract

Wireless Body Area Networks (WBANs) use biosensors worn on, or in the human body, which collect and monitor a patient's medical condition. WBANs have become increasingly more beneficial in the medical field by lowering healthcare cost and providing more useful information that medical professionals can use for a more accurate, and faster diagnosis. Due to the fact that the data collected from a WBAN is transmitted over a wireless network, there are several security concerns involved. This research looks at the various attacks, and concerns involved with WBANs. A real physiological dataset, consisting of ECG signals obtained from a 25-year-old male, was used in this research to test accuracy of various decision tree classifiers. The Weka software was used to analysis the accuracy and detection rate results of this dataset in its original form, versus a reduced dataset consisting of less, more important attributes. The results concluded that the use of decision tree classifiers using data mining, is an efficient way to test the increased accuracy on a real dataset obtained from a WBAN once it has been altered. The original dataset produced results where the ROC curve ranged from 0.313 (31%) to 0.68 (68%), meaning their accuracy is not very high and the detection rate is low. Once an attribute selection feature was used on the dataset, the newly reduced set showed ROC curves ranging from 0.68 (68%) to 0.969 (97%) amongst the three classes. As a result, decision tree models were much more accurate with a higher detection rate when used on a real dataset that was reduced to function better as a detector for a WBAN.

Keywords—wireless body area network; intrusion detection system; anomaly detection; datamining; NSL-KDD (key words)

1. Introduction

1.1 Background of WBANs

A wireless body area network (WBAN), also known as a body sensor network (BSN), consists of a network containing a set of biosensor nodes that collect and transmit data to a wireless local area network (WLAN), or a personal device known as a personal digital assistant (PDA) [14]. There are many uses to a wireless body area network, but they are particularly popular within the medical field, being used as medical devices to monitor a patient's condition. In this case, they are referred to as Medical Body Area Networks (MBAN). A MBAN remotely monitors various signals of a human body such as physiological signals including heart rate, skin temperature, and electrocardiogram, as well as various activities including sleeping and running [1].

A WBAN can be positioned on a patient's body or implanted in the body to provide a continuous flow of information, such as a real time health monitoring of the patients. WBANs help medical professionals treat patients accordingly [1]. A WBAN's sensors can be used in two different ways known as wearable WBANs and implantable WBANs. Wearable WBANs are worn with the sensors placed directly on the body, or at a close distance to the body, for a short period of time. Various examples of wearable WBANs include respiration monitors, blood pressure monitors, pacemakers, and insulin sensors [23]. On the other hand, implantable WBANs consist of sensors that are implanted deep into the body. For example, implantable sensors can be placed in the body near the heart, spinal cord, or brain [2]. An endoscope capsule and a cardiac recorder are a couple examples of implantable WBANs.

Data that is collected by the body sensors is wirelessly transmitted to an external unit that processes the information, which is then sent over via Wi-Fi or Ethernet to a specific server, or another device [2]. An example of how a body area network works is shown in Figure 1. The sensor nodes are placed on, or within the patient's body, where the data that is gathered is wirelessly transmitted via a device. This data is sent over the Internet to a server, which can then be used by medical professionals (Figure 1).

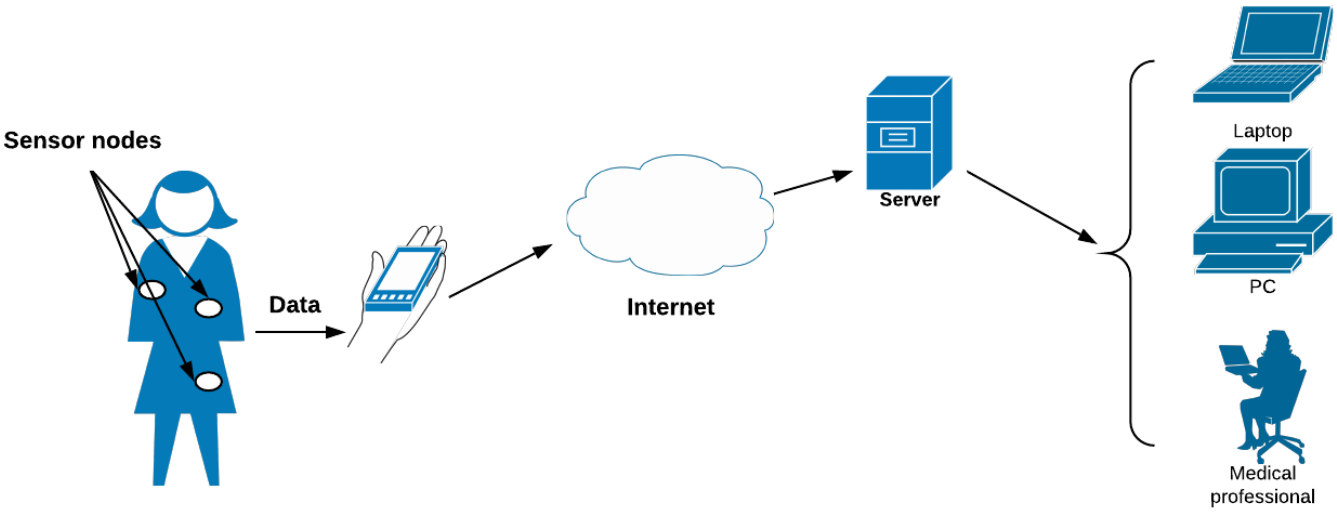


Figure 1: Wireless Body Area Network (WBAN) diagram

There are several security challenges and issues in relation to WBANs. Mainly, the security architecture of a WBAN can be challenging to successfully implement due to the fact that there are various security and performance requirements that also must be met. These security requirements include confidentiality, integrity, authentication, and availability [5, 47]. Data obtained from a WBAN must be secured with all these requirements in order to prevent security attacks from occurring on the collected date via a wireless network [47].

1.2 IEEE 802.15.6

Wireless body area networks transmit private information wirelessly through a network. A big threat to transmitting information in this way is wireless access points being accessed by an unauthorized user [5,13]. WBANs are often used in the medical field for health applications, therefore making sure the networks are secure is important. WBANs must be able to support security protocols so that communication within the network is secure [20]. The IEEE 802.15.6 standard was created for wireless body area networks in 2012 [5].

IEEE 802.15.6 supports secure and unsecure communication in body area networks [13]. It uses three different security levels as a way to secure communication amongst BANs. The levels are referred to as level 0, level 1, and level 2. Level 0, unsecured communication, is known as providing the least amount of security in IEEE 802.15.6. [13]. There is no security mechanism used in this level for the data that is transmitted. There is no authentication, integrity, or confidentiality for the data transmitted. The next level, level 1, is for authentication only. This means this level consists of average security, and messages that are transmitted using this level are secure. Although messages are considered to be secure, they are not encrypted, and it does not provide any type of protection in terms of privacy or confidentiality [13]. Level 1 does provide integrity and authentication. The final level, level 2, is for authentication and encryption, which is the highest security level. In IEEE 802.15.6, level 2 provides the most secure communication by encrypting and using secure authentication. This level of the 802.15.6 standard provides integrity, authentication, privacy protection, and confidentiality [13].

In a medical body area network, during communication, when a sensor node is going to join the network, or leave the network, it should pick one of the security levels in order to ensure

the communication is going to be secure [13]. A sensor node should also see what the requirement is for authentication throughout the transmission.

1.3 Security Attacks

A WBAN's data is transmitted wirelessly, meaning there are various security concerns involved. A patient's private data from a WBAN is highly confidential and must be protected from potential security attacks [2]. In order to preserve the confidentiality of a patient's information via a WBAN, efficient security measures must be implemented. Security issues in regard to WBANs are very important because it can be highly destructive to an individual. If an attack is successfully performed, a patient's medical records or sensitive information can be compromised [5]. There are a numerous amount of threats and attacks that can occur on a WBAN, which can be dangerous and can create an opportunity for a variety of threats and attacks performed on through the network. Based off a research report by Kompara and Holbl titled "Survey on security in intra-body area network communication," the authors describe the attacks that can be performed on a WBAN. I will briefly summarize a few important attacks:

Man in the middle attack (MITM) [4,9]: This type of attack involves an attacker having the ability to eavesdrop and/or intercept messages between a user and an application. A MITM attack acts as a normal exchange between the two parties, while the third party is secretly intercepting the messages between them [7]. This attack can be extremely dangerous because an attacker can manipulate the exchanged data between the two communicating parties [4]. Figure 2 displays a figure of how a Man in the middle attack works [9]. Machine A is communicating with Machine

B but is unaware of the Attacker Machine intercepting and listening in on their conversation (Figure 2).

Figure 2: MITM Attack [9]

Eavesdropping Attack [4]: A WBAN transmits data wirelessly, meaning it can be much easier for an attacker to spy on any information being exchanged on the network. This type of attack has to do with data being collected from the attacker by listening in on the exchange of data. In the medical field, BANs exchange a large amount of highly sensitive information, meaning it is very important that this type of attack is prevented.

One way that an eavesdropping attack can be prevented is through the use of encryption. If the data is encrypted throughout the exchange, with the use of changing keys, this type of attack can be prevented from occurring [4]. Although Figure 2 specifically shows a MITM attack, an eavesdropping attack is similar because it is a type of MITM attack. An attacker machine is listening in on the conversation between Machine A and Machine B (Figure 2) [9].

Node-compromising attack [4,10]: This type of attack is considered to be very serious in regard to wireless body sensor networks. It works as a three-stage attack: capturing sensor nodes, redeployment of the sensor nodes, and those sensor nodes launching the attack [10]. A node-

compromising attack allows an attacker to be able to extract data from a node that has been compromised and use it as a way to gain access into the network [4]. A way to help prevent this type of attack is to ensure that they keys are refreshed on a regular basis, and that keys are revoked once they are used.

Denial of Service Attack (DOS) [4,34]: To perform this type of attack, an attacker floods a network with malicious traffic until the intended target is no longer able to respond and the network ultimately crashes [8]. This happens because the machine being attacked cannot handle the amount of traffic coming in. Once this happens, the users of the network are unable to access their devices or the other parts of the network. If this type of attack occurs, then the availability of information in regard to a WBAN is disrupted [4].

Probing Attack [34]: This type of attack is when attacker probes, or scans a network in order to collect information. They collect information on the different vulnerabilities within the network to later use to exploit them and attack the system.

Remote to Local Attack (R2L) [34]: This type of attack is exactly how it sounds; an attacker sends malicious data to a victim machine and gains local access to it in order to exploit its vulnerabilities.

User to Root Attack (U2R) [34]: This is when an attacker attempts to gain access to a victim's machine to become the root user and have the highest amount of privileges.

1.4 Security Requirements

Considering all of the various security threats involved with WBANs, in order for them to perform at their highest efficiency, there are certain security requirements involved [24]. A few of these requirements are based off of the CIA triad. The CIA triad is a security model that is broken down into three categories: confidentiality, integrity, and availability [6]. WBANs transmit a patient's sensitive data and medical records through a wireless network, therefore the information is at high risk. Here are a few of the security requirements with WBANs:

Confidentiality & Privacy [5,24]: Sensitive data, especially a patient's medical records, are very important to keep private from those who should not have access to it. WBANs transmit this type of important data through a wireless network, meaning if there is an insecure network involved, a person might be able to gain access to the data without the victim being aware can occur. These types of attacks include an eavesdrop attack or a man in the middle attack (Figure 2). Information that is being transmitted via a WBAN should be encrypted during storage and when it is transmitted in order to preserve data confidentiality.

Integrity [5]: Data that is collected from a WBAN needs to be secure so it cannot be modified or deleted by a third party [6]. If someone who is authenticated to access the data changes it some way, the change should be able to be reversed [5]. Maintaining the integrity of a person's sensitive data is an important WBAN requirement because, if anyone was able to alter the data in any way, it could lead to something negative happening to the patient, such as a misdiagnosis or the medical professional providing them with the wrong type of treatment [24].

Authentication [5, 24]: A medical patient who is using a WBAN would not want their personal, sensitive information to be seen by anyone other than themselves and medical professionals. Therefore, it is important to make sure that only authenticated users are able to access the network, and prevent any malicious attacks from occurring.

Availability [5]: It is important for the collected information from a patient to always be available to the medical professionals. The data from a wearable or implantable WBAN should be protected, but be available when needed by those authenticated to access it [6]. In the case of WBANs, it also is important for the data to adjust to a particular time and location regarding a patient's needs [5].

2. State of the art

2.1 Intrusion Detection Systems (IDS)

A wireless body area network (WBAN) transmits data over a network through the use of sensor nodes. One of the ways to provide security to WBANs to defend against malicious attacks is to monitor the sensor nodes, and the network, using an Intrusion Detection System (IDS) [24]. An IDS is commonly used to detect malicious activity in the network before it does any real harm to the network [25]. Due to the limited resources of WBAN's such as power, memory and even bandwidth, there are not many security tools implemented to provide efficient security [26]. An Intrusion Detection System is often used as a second defense mechanism with WBANs because they are able to detect known and unknown attacks on the network [26].

In order to implement an efficient IDS, there are certain goals that need to be considered. An IDS must be able to detect or identify an incoming attack after it has been attempted, and then

set off an alarm to let the "owner" of the WBAN, and the network, know that an attack is about to occur. This ensures that whoever owns the WBAN is able to prevent the attack from successfully attacking the network [26]. There are two types of Intrusion Detection architectures and those include: host based, and network based. According to [26], an IDS that is host-based determines suspicious behavior and attacks from a specified host. The malicious behavior is determined based off of raw files of information that was collected at that specified node. Considering it is designed to monitor only a specific host, that is why it is unable to look at the network for suspicious behavior/incoming attacks [26]. Due to the fact that HIDS are unable to detect attacks within the network, the use of a NIDS is much more useful in terms of efficiently securing an WBAN [26]. This type of IDS differs from a host-based because it looks at the entire network, where it then captures network packets [26]. Variant types of IDSs introduced in [52-86] that uses recent machine learning approaches to classify, detect, and protect against attacks in different domains such as cloud computing and SCADA systems. We will adjust some of these approaches to work in the WBAN.

2.2 Intrusion Detection Based on Data Mining

Over the years there has been limited research on intrusion detection systems (IDS) because of the requirements involved, especially in terms of designing for a WBAN. However, there has been an increase in recent years of the number of implementations of IDSs by different researchers. These implementations of IDSs are designed using a variety of techniques and Signature-based detection methods [32]. According to [32], Signature-based detection for an IDS is designed to learn the normal and abnormal behaviors of a wireless body area network, which the intrusion system can detect malicious activity that differs from the normal. Signature-based

detection is trained and used to detect unknown attacks that have never affected the WBAN before. It has various advantages and disadvantages to its use. One disadvantage of using Signature-based detection it is unable to detect insider attacks. However, an advantage to using such techniques is, it is able to detect malicious attacks that the system has not seen before [32].

This research focuses on the use of a signature-based detection method, data mining. Data mining is one of the various technologies used for intrusion detection [32] because it can process a sizeable amount of data, and it can detect information without needing additional input from the user. Weka, a software that consists of numerous tools and algorithms for performing data mining [32], will be used as a part of this research. This software includes a variety of classification algorithms and visualization techniques to be used to determine accuracy on a dataset where information was collected from a WBAN. An effective, and commonly used classification method is known as decision trees. A decision tree includes three different parts: a root node, internal nodes and a leaf node [43]. Examples include a J48 tree, a Random Forest tree (RF), and a Random Tree (RT), all of which will be used in this research to measure accuracy on a dataset. These decision tree classifiers are described below:

J48 [41, 42]:

The full name of the J48 classifier in Weka is known as "weka.classifiers.trees.J48". The J48 classifier is based off of the C4.5 decision tree algorithm, which can build a pruned or unpruned decision tree. A common modeling error, known as overfitting, has to do with a decision tree classifying all of the data correctly in a dataset, but not necessarily being a "good classifier" if the accuracy is not maintained on new training sets. In other words, it is generating results that are meaningless. The use of the J48 decision tree classifier helps prevent this error

from occurring by having the option to prune the decision tree. To "prune" a tree means to grow a much larger tree, and then reduce it by discarding parts of it to prevent the tree from becoming too large. By doing this, the accuracy of the data will be much higher and more efficient [43].

Random Forest (RF) [41, 49]:

This classifier has to do with creating a forest of random trees. In other words, it creates a set of various decision trees that are selected at random from subsets of the provided dataset. It uses the trees it creates to decide on the final class. When using the Random Forest model for classification purposes, the tree with the most "votes" is the decided tree.

Random Tree (RT) [41, 45]:

This is considered to be a supervised, learning classifier [45]. It can be used as both a classification and regression technique. According to a source, a Random Tree classifier works by taking the input features, classifying them with all of the other trees included in the "forest," and then the results are labels that got the most votes [45].

3. Proposed contribution

3.1 Methodology

The proposed methodology for this research is shown in Figure 3. Beginning with a training dataset as the first step, will be referred to as the "Original dataset" throughout this paper. The second step is to reduce the dataset using Weka, to remove any redundant attributes that are possibly lowering the accuracy, which will be called the "Reduced Dataset." Weka is able to perform various classification, regression, and visualization techniques. This research will

consist of using classification and visualization techniques to show the improvement and accuracy of detection.

The dataset that will be used in this research is the "Motion Artifact Contaminated ECG Database" [38, 39], also known as the "StandWalkJump" dataset [40], is a dataset consisting of real physiological data. This dataset was published in 2015, and includes ECG signals obtained from a 25-year-old male wearing a WBAN placed on his body. The WBAN collected information from the man performing the activities of standing, jumping, and walking [38]. The data was collected by placing a patch that included 4 pairs of electrodes on to the body of the male, which recorded ECG signals. The data was collected at a sampling rate of 500 Hz [38] with a 16-bit resolution.

The original dataset includes 12 instances and 2501 attributes. The second step of the methodology requires taking this dataset and reducing it using an attribute selection technique to eliminate redundant, useless attributes. In this research, the AttributeSelection filter is chosen, which selects specific attributes. This filter is considered to be flexible in terms of allowing different search and evaluators to be used with it. To reduce the original dataset with this filter, an evaluator needs to be chosen to determine how the attributes will be evaluated and chosen. In this case, the CfsSubetEval evaluator will be used, which works by evaluating the worth of attributes in a subset [41]. Lastly, the search method that will be used with this filter is the BestFirst method, which performs a best first search on the entire dataset. According to Weka, it defines this search method as searching "the space of attribute subsets by greedy hillclimbing augmented with a backtracking facility." The Best First method can either start its searching with an empty or full set, and move forward or backwards from there [41]. Table 1 displays detailed descriptions of the filter, evaluator, and search method, provided by Weka (Table 1)

[41]. After the dataset has been reduced, it is left with 12 instances still, and 35 attributes, significantly lowering the data that will be used.

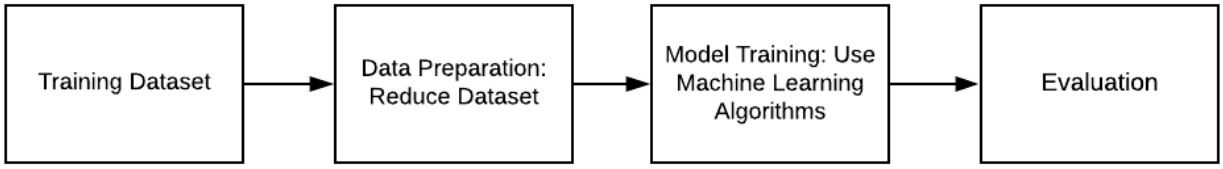


Figure 3: Proposed Methodology

		Description
Filter	AttributeSelection	A supervised attribute filter that can be used to select attributes
Evaluator	CfsSubetEval	Evaluates the worth of a subset of attributes by considering the individual predictive ability of each feature along with the degree of redundancy between them.
Search Method	BestFirst	Searches the space of attribute subsets by greedy hillclimbing augmented with a backtracking facility.

Table 1: Feature Selection Technique [41]

Once the 35 "best" attributes have been selected, the third step is to use the reduced dataset on a couple of the decision tree classification algorithms in Weka to see the improved classification accuracy on the dataset. The classification techniques and their descriptions [36] that will be used are displayed in Table 2. These include the decision trees: J48, Random Forest, and Random Tree. The ending results will be evaluated by examining the building model times, the TP rate, the FP Rate, and the ROC area.

Model	Description
J48	For generating a pruned or unpruned decision tree using the C4.5 algorithm. Increases better performance.
Random Forest (RF)	Builds a forest of different decision trees.
Random Tree (RT)	Constructs a tree that considers K randomly chosen attributes at each node. No pruning.

Table 2: Classification Decision Trees & Descriptions

The proposed methodology for this research (Figure 3) is to improve the detection technique used on WBANS, and to show the increase in accuracy and detection rate by using a real physiological dataset, reducing it to its most important attributes, and testing it on various decision tree classifiers. Once the results are obtained, the true positive rate (TPR) will be closely analyzed to determine if the specific classifier is accurate r to use for correct detections. The higher the TPR, the better it is at detection, therefore less false alarms. The other number that will be examined is the false positive rate (FPR). The FPR should be lower in relation to the TPR, so the threshold will be higher as well, for a more accurate classifier. The measurements and metrics provided by Weka, that are used in Figures 4–9, are described in Table 3 and 4 [51].

Measurement	Definition
TP Rate	TP / (TP + FN) True positives / (true positives + false negatives)
FP Rate	FP / (FP + TN) False positives / (false positives + true negatives)
Precision	TP / (TP + FP) True positives / (true positives + false positives)
Recall	TP / (TP + FN) True positives / (true positives + false negatives)

Table 3: Accuracy Measurements & Definitions

Metric	Definition
TP (True positive)	Correctly labeled as positives
TN (True negative)	Negatives correctly labeled as negatives
FN (False negative)	Positive examples incorrectly labeled as negative
FP (False positive)	Negative examples incorrectly labeled as positive

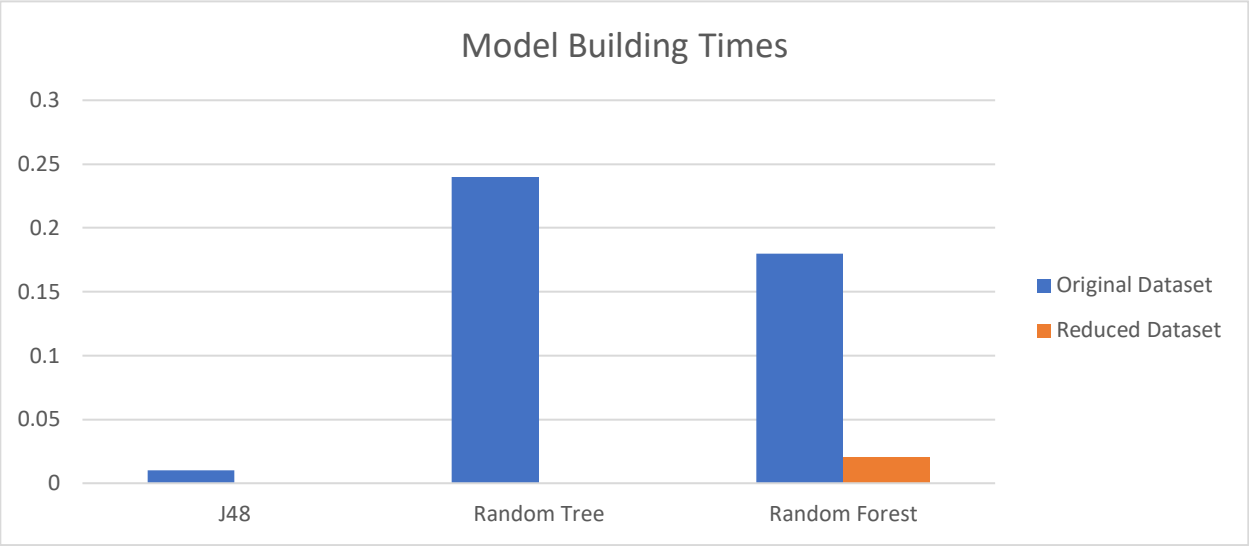
Table 4: Metrics & Definitions

4. Experiment Analysis

The original ECG signals dataset consists of 12 instances and 2501 attributes. The attributes are labeled as "Channels" for the signals that were recorded. For this research, the dataset was used in Weka and tested on three different decision tree classifiers. These classifiers were the J48, RandomTree, and RandomForest. The models that were built with these classifiers were based off of a 4-fold cross-validation. Cross-validation is a technique that is used to divide a dataset into a specified number of pieces [46], which in this case 4 was chosen in order to increase accuracy. The dataset was then reduced with the use of the Attribute Selection filter, the CfsSubetEval evaluator and BestFirst search method to eliminate any redundant attributes that were decreasing the accuracy of the dataset. Once that filter was applied to the dataset, the number of attributes decreased to 35. This newly reduced dataset was also tested with a 4-fold cross-validation and with the same three classifiers that were listed previously.

The original dataset was reduced after removing a significant number of attributes, therefore the time to build the models decreased with the reduced dataset as well. These time results are shown in Graph 1, where the blue displays the building times in seconds of the

original dataset, and the orange are the times of the reduced dataset models. The names of the classifiers are shown on the X-axis, with J48 and Random Tree at 0 seconds for the reduced dataset. (Graph 1). Even though both datasets built their models at a high speed, the reduced dataset was still faster.



Graph 1: Model Building Times

After the decision tree models were built in Weka, a "Detailed Accuracy by Class" section was displayed which showed the accuracy results. The results of the original dataset models are displayed in Figures 4, 5, 6. The three classes of standing, walking and jumping each display separate results, as well as a weighted average of the three. The measurements included in these results that are the most important to examine are the true positive (TP) rate, the false positive (FP) rate, and the AU (Area Under the Curve) ROC (Receiver Operating Characteristics) curve.

The first decision tree model built was the J48, based off of the original dataset is shown in Figure 4. According to Figure 4, for each of the three classes, the TP rate ranged from 0.333 (jumping) to 0.500 for both of the other classes. The FP rate was also considerably low ranging

from 0.125 to 0.625. Similar results occurred for the other two classifier models in Figures 5 and 6. With all 3 of these decision tree models tested on the original dataset, and showing a low TPR and FPR, the accuracy and detection rate is low.

```
=== Detailed Accuracy By Class ===

               TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
               0.500    0.125    0.667      0.500    0.571      0.408    0.688     0.500     standing
               0.000    0.250    0.000      0.000    0.000      -0.316   0.375     0.333     walking
               0.500    0.625    0.286      0.500    0.364      -0.120   0.438     0.310     jumping
Weighted Avg.  0.333    0.333    0.317      0.333    0.312      -0.009   0.500     0.381
```

Figure 4: J48 Results - Original Dataset

```
=== Detailed Accuracy By Class ===

               TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
               0.500    0.375    0.400      0.500    0.444      0.120    0.344     0.335     standing
               0.000    0.250    0.000      0.000    0.000      -0.316   0.391     0.329     walking
               0.250    0.500    0.200      0.250    0.222      -0.239   0.375     0.377     jumping
Weighted Avg.  0.250    0.375    0.200      0.250    0.222      -0.145   0.370     0.347
```

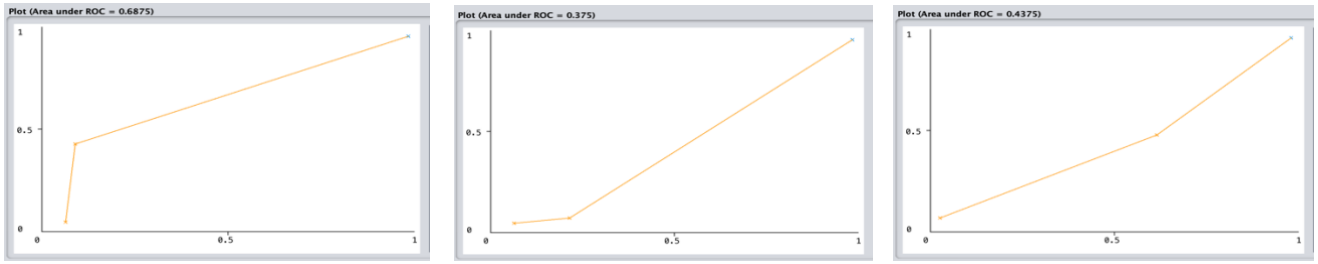
Figure 5: Random Forest Results - Original Dataset

```
=== Detailed Accuracy By Class ===

               TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
               0.250    0.500    0.200      0.250    0.222      -0.239   0.375     0.300     standing
               0.000    0.375    0.000      0.000    0.000      -0.408   0.313     0.333     walking
               0.500    0.250    0.500      0.500    0.500      0.250    0.625     0.417     jumping
Weighted Avg.  0.250    0.375    0.233      0.250    0.241      -0.132   0.438     0.350
```

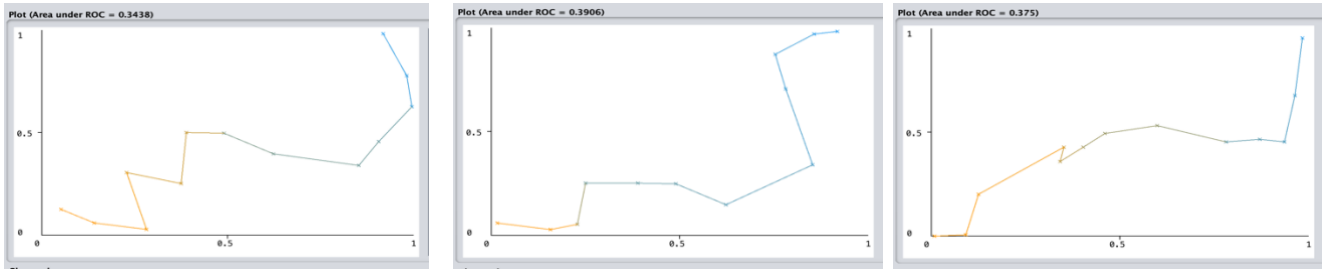
Figure 4: Random Tree Results - Original Dataset6

The ROC curve, also known as the threshold curve in Weka, is one of the most important measurements to examine in order to accurately evaluate the performance of the classification models tested in this research [46]. This curve is determined by placing the FPR on the x-axis and the TPR on the y-axis. The higher the area under the curve is, the higher the accuracy and detection rate. In order to visualize the results for the ROC curves, the models for J48, Random

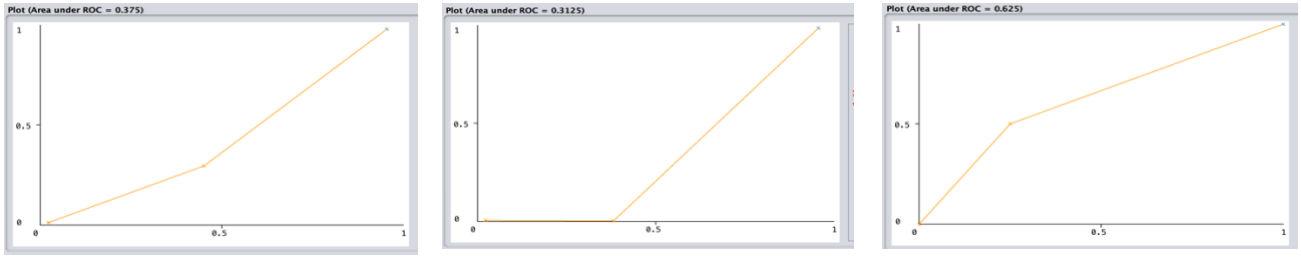
Forest, and Random Tree classifiers, based off of the original data, are displayed in graphs 2, 3, 4, respectively. For each graph set, from left to right they are displayed for each of the three classes results: standing, walking, and jumping (Graphs 2, 3, 4). By looking at these graphs, the ROC curves range from 0.313 (31%) to 0.68 (68%), meaning their accuracy is not very high and the detection rate is low. However, this can be improved once the dataset eliminates any redundant attributes.



Graph 4: J48 – Standing, Walking, Jumping (Original Data)



Graph 4: Random Forest – Standing, Walking, Jumping (Original Data)



Graph 4: Random Tree – Standing, Walking, Jumping (Original Data)

In order to show that these decision tree classifiers are good classifiers to use and obtain a high accuracy on a real physiological dataset, the results of the reduced dataset are examined as well. The results of the reduced dataset are displayed in Figures 7, 8, and 9 below. Each of the classifiers resulted in TP rates above 0.60 (60%), and a few of them are at 1.00 (100%), meaning they have achieved a high detection rate.

```
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                0.750    0.125    0.750      0.750    0.750      0.625    0.813     0.646     standing
                0.500    0.125    0.667      0.500    0.571      0.408    0.688     0.500     walking
                0.750    0.250    0.600      0.750    0.667      0.478    0.750     0.533     jumping
Weighted Avg.   0.667    0.167    0.672      0.667    0.663      0.504    0.750     0.560
```

Figure 7: J48 Results - Reduced Dataset

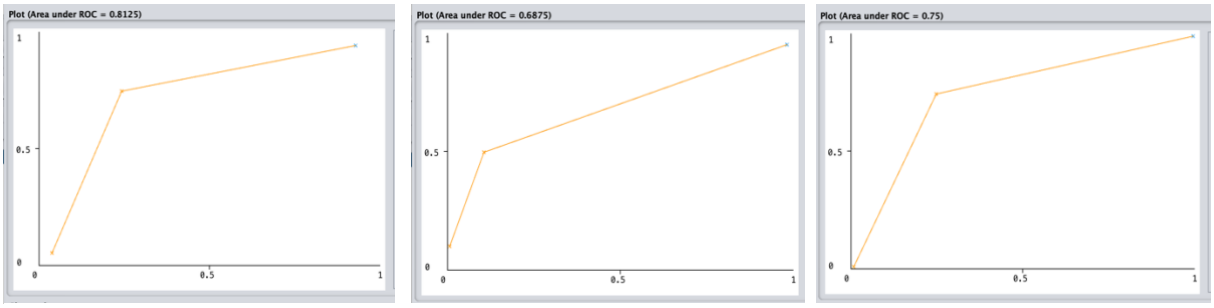
```
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                0.750    0.125    0.750      0.750    0.750      0.625    0.844     0.813     standing
                0.500    0.000    1.000      0.500    0.667      0.632    0.969     0.950     walking
                1.000    0.250    0.667      1.000    0.800      0.707    0.938     0.888     jumping
Weighted Avg.   0.750    0.125    0.806      0.750    0.739      0.655    0.917     0.883
```

Figure 7: Random Forest Results - Reduced Dataset

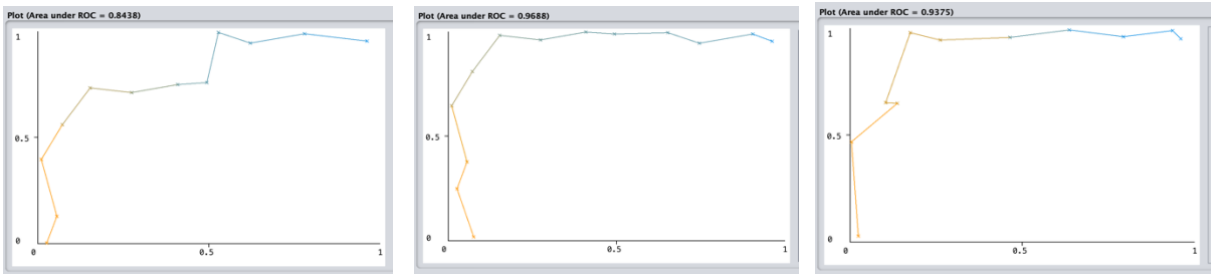
```
=== Detailed Accuracy By Class ===

                TP Rate  FP Rate  Precision  Recall   F-Measure  MCC      ROC Area  PRC Area  Class
                0.750    0.125    0.750      0.750    0.750      0.625    0.813     0.646     standing
                0.750    0.125    0.750      0.750    0.750      0.625    0.813     0.646     walking
                0.750    0.125    0.750      0.750    0.750      0.625    0.813     0.646     jumping
Weighted Avg.   0.750    0.125    0.750      0.750    0.750      0.625    0.813     0.646
```

Figure 7: Random Tree Results - Reduced Dataset

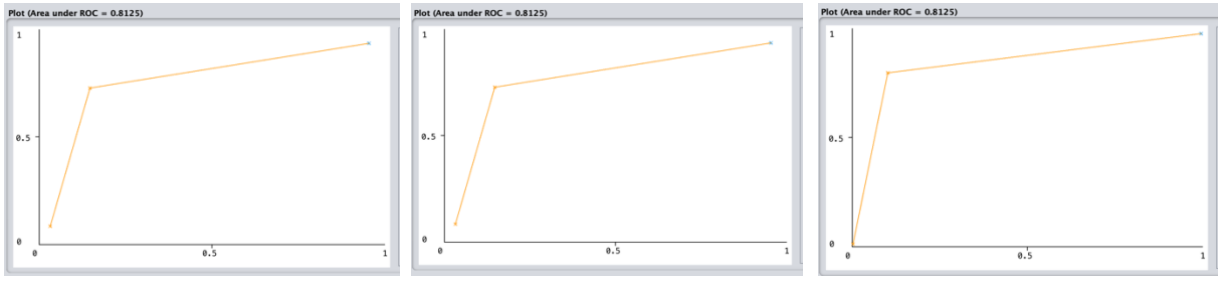
The visual results of the area under ROC curves for the reduced data are displayed in graphs 5, 6, and 7. In comparison to the graph sets of 2, 3, and 4, the results for the reduced dataset are increasingly more accurate. The area under the ROC curve are much higher and closer to 100%, ranging from 0.68 (68%) to 0.969 (97%) amongst the three classes. The accuracy of these models is much higher, and so is the detection rate. This means the data has a high detection rate after filtering out the redundant attributes, and using various decision tree classifiers to test the data on. From looking at these three graphs based off and their ROC curves, it can be concluded that they are not as accurate nor efficient as when the data has been reduced. The closer the ROC curve is to 1.0, the more accurate and efficient the classifier is.



Graph 7: J48 – Standing, Walking, Jumping (Reduced Data)



Graph 7: Random Forest – Standing, Walking, Jumping (Reduced Data)



Graph 7: Random Tree – Standing, Walking, Jumping (Reduced Data)

5. Conclusion

Wireless Body Area Networks (WBANs) gather and monitor physiological information from a patient's body through the use of biosensors [14]. The data that is collected from these sensors is transmitted wirelessly to a WLAN or PDA, which is then used by medical professionals to accurately treat patients. There are many advantages to WBANs, such as reduced hospital costs, better quality of life for a patient, data is collected over a longer period of time, etc. Despite these advantages, there are many security concerns in regard to WBANs. These concerns include protecting confidentiality and privacy; integrity and authentication; and availability of the data that is transmitted wirelessly. A solution is the utilization of an Intrusion Detection System (IDS). In this research, several data mining algorithms and classifiers were tested on a real physiological dataset obtained from a WBAN to test its accuracy and detection rate. To show the increased accuracy of various classification models, the Weka software was used. The results showed that in order to classify and detect accurate information from a dataset, certain attributes must be removed and then examined in order to increase performance and accuracy.

.

6. References

[1] Gupta, S., Mukherjee, T., & Venkatasubramanian, K. (2013). Body area networks safety, security, and sustainability. Cambridge: Cambridge University Press.

[2] Sylla, I. T. (2011, September 26). The wireless body area network: What engineers need to know. Electronic Engineering Times, 35–40.

[3] Kwak, K. S., Ullah, S. S., & Ullah, N. S. (2011). An Overview of IEEE 802.15.6 Standard.

[4] Kompara, M., & Hölbl, M. (2018). Survey on security in intra-body area network communication. Ad Hoc Networks, 70, 23–43. https://doi.org/10.1016/j.adhoc.2017.11.006

[5] Ibrahim, M., Kumari, S., Das, A., Wazid, M., & Odelu, V. (2016). Secure anonymous mutual authentication for star two-tier wireless body area networks. *Computer Methods and Programs in Biomedicine*, *135*, 37–50. https://doi.org/10.1016/j.cmpb.2016.07.022

[6] Forcepoint. (2019, October 30). What is the CIA Triad? Retrieved from https://www.forcepoint.com/cyber-edu/cia-triad

[7] Imperva. (n.d.). What is MITM (Man in the Middle) Attack: Imperva. Retrieved from https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/.

[8] Understanding Denial-of-Service Attacks: CISA. (n.d.). Retrieved from https://www.us-cert.gov/ncas/tips/ST04-015.

[9] Calvert, C., Khoshgoftaar, T. M., Najafabadi, M. M., & Kemp, C. (2017). A Procedure for Collecting and Labeling Man-in-the-Middle Attack Traffic. International Journal of Reliability, Quality & Safety Engineering, 24(1), 1. https://doi-org.sunypoly.idm.oclc.org/10.1142/S0218539317500024

[10] Lin, X. (2009). CAT: Building Couples to Early Detect Node Compromise Attack in Wireless Sensor Networks. GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference. doi:10.1109/glocom.2009.5425922

[11] Deepak, K., & Babu, A. (2016). Enhancing Reliability of IEEE 802.15.6 Wireless Body Area Networks in Scheduled Access Mode and Error Prone Channels.(Author abstract). 89(1), 93–118. https://doi.org/10.1007/s11277-016-3254-4

[12] Usman, Muhammad & Asghar, Muhammad Rizwan & Ansari, Imran & Qaraqe, Marwa. (2018). Security in Wireless Body Area Networks: From In-Body to Off-Body Communications. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2873825.

[13] Salehi, S. A., Razzaque, M. A., Tomeo-Reyes, I., & Hussain, N. (2016). IEEE 802.15.6 standard in wireless body area networks from a healthcare point of view. 2016 22nd Asia-Pacific Conference on Communications (APCC). doi:10.1109/apcc.2016.7581523

[14] GroundAI. (2016, November 25). Investigating Low Level Protocols for Wireless Body Sensor Networks. Retrieved from https://www.groundai.com/project/investigating-low-level-protocols-for-wireless-body-sensor-networks/1.

[15] Deepak, K., & Babu, A. (2016). Energy consumption analysis of modulation schemes in IEEE 802.15.6-based wireless body area networks. EURASIP Journal on Wireless Communications and Networking, 2016(1), 1–14. https://doi.org/10.1186/s13638-016-0682-5

[16] Ullah, S., Mohaisen, M., & Alnuem, M. (2013). [Review of A Review of IEEE 802.15.6 MAC, PHY, and Security Specifications]. International Journal of Distributed Sensor Networks, 9(4), 12. https://doi.org/10.1155/2013/950704

[17] Cerny, M., & Penhaker, M. (2011). Wireless Body Sensor Network in Health Maintenance Systems. Elektronika Ir Elektrotechnika, 115(9), 113–116. https://doi.org/10.5755/j01.eee.115.9.762

[18] Li, C., Lee, C., & Weng, C. (2016). A Secure Cloud-Assisted Wireless Body Area Network in Mobile Emergency Medical Care System.(Report). 40(5), 117. https://doi.org/10.1007/s10916-016-0474-9

[19] Sylla, I. (2011). The wireless body area network: What engineers need to know. Electronic Engineering Times, (1608), 35–36,38,40. Retrieved from http://search.proquest.com/docview/896955824/

[20] Zhou, J., Cao, Z., Dong, X., Xiong, N., & Vasilakos, A. (2015). 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Information Sciences, 314, 255–276. https://doi.org/10.1016/j.ins.2014.09.003

[21] Ullah, S., Imran, M., & Alnuem, M. (2014). A Hybrid and Secure Priority-Guaranteed MAC Protocol for Wireless Body Area Network.International Journal of Distributed Sensor Networks, 10(2), 7. https://doi.org/10.1155/2014/481761

[22] Mitchell, B. (2019, July 17). The Future of Computer Networks and Your Body. Retrieved from https://www.lifewire.com/introduction-to-body-area-networks-817364#:~:targetText=The term body area networks,) and/or the Internet.

[23] Watkins, L., & Aggarwal, S. (n.d.). Tattle Tale Security: An Intrusion Detection System for Medical Body Area Networks (Mban).

[24] Thamilarasu, G. (2016). IDetect: an intelligent intrusion detection system for wireless body area networks (1/2, Vol. 11). Bothell, WA: Int. J. Security and Networks.

[25] Odesile, A., & Thamilarasu, G. (2017). Distributed Intrusion Detection Using Mobile Agents in Wireless Body Area Networks.

[26] Vasileios , A. (2019). Datasets for Intrusion Detection for Wireless Body Area Networks. http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/11888/Asimakopoulos_mte1605.pdf?sequence=1&isAllowed=y

[27] Li, M., & Lou, W. (2010). Data Security And Privacy In Wireless Body Area Networks. IEEE Wireless Communications. https://ubisec.cse.buffalo.edu/files/10.1.1.465.9743.pdf

[28] L. N. Tidjon, M. Frappier and A. Mammar, "Intrusion Detection Systems: A Cross-Domain Overview," in IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3639-3681, Fourthquarter 2019, doi: 10.1109/COMST.2019.2922584.

[29] R. Thomas and D. Pavithran, "A Survey of Intrusion Detection Models based on NSL-KDD Data Set," 2018 Fifth HCT Information Technology Trends (ITT), Dubai, United Arab Emirates, 2018, pp. 286-291, doi: 10.1109/CTIT.2018.8649498.

[30] H. Chauhan, V. Kumar, S. Pundir and E. S. Pilli, "A Comparative Study of Classification Techniques for Intrusion Detection," 2013 International Symposium on Computational and Business Intelligence, New Delhi, 2013, pp. 40-43, doi: 10.1109/ISCBI.2013.16.

[31] H. Chauhan, V. Kumar, S. Pundir and E. S. Pilli, "A Comparative Study of Classification Techniques for Intrusion Detection," 2013 International Symposium on Computational and Business Intelligence, New Delhi, 2013, pp. 40-43, doi: 10.1109/ISCBI.2013.16.

[32] Mohammad, M. N. (n.d.). A Novel Intrusion Detection System by using Intelligent Data Mining in Weka Environment.

[33] Bhuyan, M. (2013). Network Anomaly Detection: Methods, Systems and Tools.

[34] Thomas , R., & Pavithran , D. (2018). A Survey of Intrusion Detection Models based on Nsl-Kdd Data Set (tech.).

[35] Saporito, G. (2019, November 1). A Deeper Dive into the NSL-KDD Data Set. Medium. https://towardsdatascience.com/a-deeper-dive-into-the-nsl-kdd-data-set-15c753364657.

[36] Hossain , M. Erformance Analysis of Anomaly Based Network Intrusion Detection Systems (tech.). Performance Analysis of Anomaly Based Network Intrusion Detection Systems .

[37] Brownlee, J. (2020, February 6). *How to Calculate Precision, Recall, and F-Measure for Imbalanced Classification*. Machine Learning Mastery. https://machinelearningmastery.com/precision-recall-and-f-measure-for-imbalanced-classification/.

[38] V. Behravan, N. E. Glover, R. Farry, P. Y. Chiang and M. Shoaib, "Rate-adaptive compressed-sensing and sparsity variance of biomedical signals," *2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, Cambridge, MA, 2015, pp. 1-6. doi: 10.1109/BSN.2015.7299419

[39] Goldberger, A., Amaral, L., Glass, L., Hausdorff, J., Ivanov, P. C., Mark, R., ... & Stanley, H. E. (2000). PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. Circulation [Online]. 101 (23), pp. e215–e220.

[40] Time Series Classification. http://www.timeseriesclassification.com/description.php?Dataset=StandWalkJump.

[41] WEKA. Weka 3 - Data Mining with Open Source Machine Learning Software in Java. https://www.cs.waikato.ac.nz/ml/weka/.

[42] Salzberg, S.L. C4.5: Programs for Machine Learning by J. Ross Quinlan. Morgan Kaufmann Publishers, Inc., 1993. *Mach Learn* **16,** 235–240 (1994). https://doi.org/10.1007/BF00993309

[43] Patel, N., & Upadhyay, S. (2012). Study of Various Decision Tree Pruning Methods with their Empirical Comparison in Weka (tech.). Study of Various Decision Tree Pruning Methods with their Empirical Comparison in WEKA (Vol. 60). International Journal of Computer Applications.

[44] Othman M.F., Yau T.M.S. (2007) Comparison of Different Classification Techniques Using WEKA for Breast Cancer. In: Ibrahim F., Osman N.A.A., Usman J., Kadri N.A. (eds) 3rd Kuala Lumpur International Conference on Biomedical Engineering 2006. IFMBE Proceedings, vol 15. Springer, Berlin, Heidelberg

[45] FutureLearn. *Cross-validation - Data Mining with Weka*. FutureLearn. https://www.futurelearn.com/courses/data-mining-with-weka/0/steps/25384.

[46] Narkhede, S. (2019, May 26). Understanding AUC - ROC Curve. Medium. https://towardsdatascience.com/understanding-auc-roc-curve-68b2303cc9c5.

[47] Asam, M., & Jamal, T. Security Issues in WBANs (tech.). Security Issues in WBANs. https://arxiv.org/pdf/1911.04330.pdf

[48] Amrehn, Mario & Mualla, Firas & Angelopoulou, Elli & Steidl, Stefan & Maier, Andreas. (2018). The Random Forest Classifier in WEKA: Discussion and New Developments for Imbalanced Data.

[49] Chakure, A. (2020, May 26). *Random Forest Classification and its implementation*. Medium. https://towardsdatascience.com/random-forest-classification-and-its-implementation-d5d840dbead0.

[50] *Motion Artifact Contaminated ECG Database*. Motion Artifact Contaminated ECG Database v1.0.0. (2015, December 18). https://physionet.org/content/macecgdb/1.0.0/.

[51] Davis, J., & Goadrich, M. The Relationship Between Precision-Recall and Roc Curves (rep.). The Relationship Between Precision-Recall and ROC Curves.

[52] Kholidy, HA, Fabrizio Baiardi, Salim Hariri: 'DDSGA: A Data-Driven Semi-Global Alignment Approach for Detecting Masquerade Attacks'. The IEEE Transaction on Dependable and Secure Computing, 10.1109/TDSC.2014.2327966, pp:164–178, June 2015.

[53] Kholidy, HA, Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset For Cloud Computing and Masquerade Attacks ", in the 9th Int. Conf. on Information Technology: New Generations ITNG 2012, April 16-18, Las Vegas, Nevada, USA. http://www.di.unipi.it/~hkholidy/projects/cidd/

[54] Kholidy, HA, Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", in the 9th Int. Conf. on Information Technology: New Generations ITNG 2012, April 16-18, Las Vegas, Nevada, USA. http://www.di.unipi.it/~hkholidy/projects/cids/

[55] Kholidy, HA, Baiardi, F., Hariri, S., et al.: ‘A hierarchical cloud intrusion detection system: design and evaluation’, Int. J. Cloud Comput., Serv. Archit. (IJCCSA), 2012, 2, pp. 1–24.

[56] Kholidy, HA, “PH.D. Thesis: Cloud Computing Security, An Intrusion Detection System for Cloud Computing Systems”. https://pdfs.semanticscholar.org/cf8a/14dc638480dbc5304824dd99a631d917d3fe.pdf

[57] Kholidy, HA, “Autonomous mitigation of cyber risks in the Cyber–Physical Systems”, Future Generation Computer Systems, Volume 115, 2021, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.09.002. http://www.sciencedirect.com/science/article/pii/S0167739X19320680

[58] Kholidy, HA, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system", in Journal of Computing, Springer, DOI: 10.1007/s00607-016-0495-8, June 2016.

[59] Kholidy, HA, Abdelkarim Erradi, “A Cost-Aware Model for Risk Mitigation in Cloud Computing SystemsSuccessful accepted in 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November, 2015.

[60] Kholidy, HA, Ali Tekeoglu, Stefano Lannucci, Shamik Sengupta, Qian Chen, Sherif Abdelwahed, John Hamilton, “Attacks Detection in SCADA Systems Using an Improved Non-Nested Generalized Exemplars Algorithm", the 12th IEEE International Conference on Computer Engineering and Systems (ICCES 2017), December 19-20, 2017.

[61] Qian Chen, Kholidy, HA, Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the International Conference on Future Network Systems and Security (FNSS 2017), Gainesville, Florida, USA, 31 August 2017. Conference publisher: Springer. “Industrial control system (ics) cyberattack datasets, http://www.ece.uah.edu/~thm0009/icsdatasets/ PowerSystem_Dataset_README.pdf

[62] Kholidy, HA, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, “A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014.

[63] Kholidy, HA, “Detecting impersonation attacks in cloud computing environments using a centric user profiling approach”, Future Generation Computer Systems, Volume 115, issue 17,

Decmenr 13, 2020, Pages 171-187, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.12 , https://www.sciencedirect.com/science/article/abs/pii/S0167739X20330715

[64] Kholidy, HA, Hala Hassan, Amany Sarhan, Abdelkarim Erradi, Sherif Abdelwahed, *"QoS Optimization for Cloud Service Composition Based on Economic Model"*, Book Chapter in the Internet of Things. User-Centric IoT, Volume 150 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering pp 355-366, June 2015. Publisher: Springer International Publishing.

[65] Kholidy, H.A.,, Fabrizio Baiardi, Salim Hariri, Esraa M. ElHariri, Ahmed M. Youssouf, and Sahar A. Shehata, *"A Hierarchical Cloud Intrusion Detection System: Design and Evaluation",* in International Journal on Cloud Computing: Services and Architecture (IJCCSA), November 2012.

[66] Kholidy, HA, Alghathbar Khaled s., "*Adapting and accelerating the Stream Cipher Algorithm RC4 using Ultra Gridsec and HIMAN and use it to secure HIMAN Data*", Journal of Information Assurance and Security (JIAS), vol. 4 (2009)/ issue 4, pp 274-283, 2009.

[67] Samar SH. Haytamy, Kholidy, HA, Fatma A. Omara, "*ICSD: Integrated Cloud Services Dataset*", Springer, Lecture Note in Computer Science, ISBN 978-3-319-94471-5, https://doi.org/10.1007/978-3-319-94472-2. 14th World Congress on Services, pp18-30. Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA.

[68] Kholidy, HA, Ali Tekeoglu, Stefano Iannucci, Shamik Sengupta, Qian Chen, Sherif Abdelwahed, John Hamilton, "Attacks Detection in SCADA Systems Using an Improved Non-Nested Generalized Exemplars Algorithm", the 12th IEEE International Conference on Computer Engineering and Systems (ICCES 2017), December 19-20, 2017.

[69] Stefano Iannucci, Kholidy, HA, Amrita Dhakar Ghimire, Rui Jia, Sherif Abdelwahed, Ioana Banicescu, "A Comparison of Graph-Based Synthetic Data Generators for Benchmarking Next-Generation Intrusion Detection Systems", IEEE Cluster 2017, Sept 5 2017, Hawaii, USA. Conference Publisher: IEEE.

[70] Qian Chen, Kholidy, HA., Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the International Conference on Future Network Systems and Security (FNSS 2017), Gainesville, Florida, USA, 31 August 2017. Conference Publisher: Springer.

[71] Kholidy, HA, Abdelkarim Erradi, “A Cost-Aware Model for Risk Mitigation in Cloud Computing Systems”, accepted in 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November 2015.

[72] Kholidy, HA, Abdelkarim Erradi, Sherif Abdelwahed, “Attack Prediction Models for Cloud Intrusion Detection Systems”, in the International Conference on Artificial Intelligence, Modelling and Simulation (AIMS2014), Madrid, Spain, November 2014. Publisher: IEEE.

[73] Kholidy, HA, Ahmed M. Yousouf, Abdelkarim Erradi, Hisham A. Ali, Sherif Abdelwahed, "A Finite Context Intrusion Prediction Model for Cloud Systems with a Probabilistic Suffix Tree", in the 8th European Modelling Symposium on Mathematical Modelling and Computer Simulation, Pisa, Italy, October 2014. Conference Publisher: IEEE

[74] Kholidy, HA, Abdelkarim Erradi, Sherif Abdelwahed, “Online Risk Assessment and Prediction Models For Autonomic Cloud Intrusion Prevention Systems”, in the “11th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Doha, Qatar, November 2014. Conference Publisher: IEEE.

[75] Kholidy, HA, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, “A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014. Conference Publisher: IEEE.

[76] Kholidy, HA, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, “A Hierarchical, Autonomous, and Forecasting Cloud IDS”, the 5th IEEE International Conference on Modeling, Identification and Control (ICMIC2013), Cairo, Aug31-Sept 1-2, 2013.

[77] Kholidy, HA, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, “HA-CIDS: A Hierarchical and Autonomous IDS for Cloud Environments”, Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN) Madrid, Spain, June 2013. Conference Publisher: IEEE.

[78] Kholidy, HA, Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks", the 9th IEEE International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.

[79] Kholidy, HA, Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", The 9th International Conf. on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012. Conference Publisher: IEEE.

[80] Kholidy, HA, Chatterjee N., "Towards Developing an Arabic Word Alignment Annotation Tool with Some Arabic Alignment Guidelines", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 778-783, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010. Conference Publisher: IEEE

[81] Kholidy, HA, "A Study for Access Control Flow Analysis With a Proposed Job Analyzer Component based on Stack Inspection Methodology", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 1442-1447, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010. Conference Publisher: IEEE

[82] Kholidy, HA, "HIMAN-GP: A Grid Engine Portal for controlling access to HIMAN Grid Middleware with performance evaluation using processes algebra", The 2nd IEEE International Conference on Computer Technology and Development ICCTD, pp 163-168, Cairo, 2010.

[83] Kholidy, HA, Khaled S. Algathber, "A New Accelerated RC4 Scheme using "Ultra Gridsec" and "HIMAN", 5th Int. Conference on Information Assurance and Security, Aug 2009, China. Conference Publisher: IEEE

[84] Kholidy, HA, A. Azab, S. Deif, "Enhanced ULTRA GRIDSEC: Enhancing High-Performance Symmetric Key Cryptography Schema Using Pure Peer-to-Peer Computational Grid Middleware (HIMAN)", IEEE-ICPCA (the 3rd Int. Conf. on Pervasive Computing and Applications, 06-08 Oct 2008.

[85] A. Azab, Kholidy, HA, "An Adaptive Decentralized Scheduling Mechanism for Peer-to-Peer Desktop Grids", International Conference on Computer Engineering & Systems Nov 2008.

[86] Mostafa-Sami M., Safia H D., Kholidy, HA, "ULTRAGRIDSEC: Peer-to-Peer Computational Grid Middleware Security Using High-Performance Symmetric Key Cryptography" in IEEE-ITNG (5th Int. Conf. On Information Technology-New Generations), LasVegas, Nevada, USA, 7-9 April 2008.