Research Paper

Volume : 2 | Issue : 10 | October 2013 • ISSN No 2277 - 8179

Proposal to WNIDS Wireless Network Intrusion Detection System

Computer Science

KEYWORDS : WLAN, IDS, SVM, ANN and ID3

Dr. Saad K. Majeed	Computer Sciences/ University of Technology/ Baghdad-Iraq
Dr. Soukaena H. Hashem	Computer Sciences/ University of Technology/ Baghdad-Iraq
Ikhlas K. Gbashi	Computer Sciences/ University of Technology/ Baghdad-Iraq

ABSTRACT

Although of the widespread use of the WLANs, it is still vulnerable for the availability security issues. This research presents a proposal Wireless Network Intrusion Detection System (WNIDS) which is use misuse and anomaly techniques in intrusion detection. The proposal depend on Data mining is a DM-based WNIDS since mining provide iterative process so if results are not satisfied with optimal solution, the mining steps will continue to be carried out until mining results are corresponding intention results. For training and testing of WNIDS in our experiment, we used collected dataset called it Wdataset, the collection done on an organized WLAN 802.11 consist of 5 machines. The collection of data involved frames from all types (normal and the four known intrusions and unknown intrusion).

The collected connections contain features those appear directly in the header of 802.11 frames and we added one more feature (casting) since it is critical in distinguish among intrusions. These connections are labeled as either normal or attack type, many of these features are irrelative in classification process. Here we propose Support Vector Machine SVM classifier as feature extraction to reduce no. of features to avoid time consuming in training and real-time detecting. SVM introduce 8 features as subset of correlated intrinsic features present the basic point in classification. The sets of features that have been resulted from SVM and the all features set will be the feeding of WNIDS.

The results obtained from WNIDS showing that accuracy rate of ANN and ID3 classifiers are both higher with SVM (8) features than set of all features. And absolutely, ANN accuracy is higher than ID3 with both sets of features.

1. Introduction

WLANs suffer from a lot of vulnerabilities, some of these vulnerabilities inherited from the usual wired networks and some are new due to the broadcast connection medium. These vulnerabilities include confidentiality, integrity and availability vulnerabilities. Through the WLAN evolution, many security improvements have been added to the IEEE 802.11 standards such as: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and IEEE 802.11i (WPA2). These techniques can only protect data frames to satisfy the confidentiality and the integrity security issues. The management and control frames still unprotected [1].

Several vulnerabilities exist at the link layer level of the802.11 protocol. Many 802.11-specificattacks were analyzed and demonstrated to present a real threat to network availability. Most of the attacks on WLAN are; ***Deauthentication attack,*** where the attacker fakes a deauthentication frame as if it hadoriginated from the base station (Access Point). Up on reception, the station disconnects and tries to reconnect to the base station again. This process is repeated indefinitely to keep the station disconnected from the base station. The attacker can also set the receiving address to the broadcast address to target all stations associated with the victim base station. However, we noticed that some wireless network cards ignore this type of deauthentication frame. ***ChopChop attack,*** where the attacker intercepts an encrypted frame and uses the Access Point to guess the clear text. The attack is performed as follows: The intercepted encrypted frame is chopped from the last byte. Then, the attacker builds a new frame 1 byte smaller than the original frame. In order to set the right value for the 32 bit longCRC32 checksum named ICV, the attacker makes a guess on the last clear byte. To validate the guess he/she made, the attacker will send the new frame to the base station using a multicast receive address. If the frame is not valid (i.e., the guess is wrong), then the frame is silently discarded by the access point. The frame with the right guess will be relayed back to the network. The hacker can then validate the guess he/she made. The operation is repeated until all bytes of the clear frame are discovered. ***Fragmentation attack,*** where the attacker sends a frame as a successive set of fragments. The access point will assemble them into a new frame and send it back to the wireless network. Since the attacker knows the clear text of the frame, he can recover the key stream used to encrypt the frame. This process is repeated until he/she gets a 1,500 byte long key stream. The attacker can use the key stream to encrypt new frames or decrypt a frame that uses the same three byte initialization vector IV. The process can be repeated until the attacker builds a rainbow key stream table of all possible IVs. Such a table requires 23 GB of memory. ***Duration attack,*** where the attacker exploit a vulnerability in the virtual carrier-sense mechanism and sends a frame with the NAV field set to a high value (32 ms). This will prevent any station from using the shared medium before the NAV timer reaches zero. Before expiration of the timer, the attacker sends another frame. By repeating this process, the attacker can deny access to the wireless network. [2].

Intrusion is the result of flaws in the design and Implementation of computer systems, operating systems, applications, and communication protocols. The vulnerabilities of wireless networks are the subject of new types of attacks which range from the passive eavesdropping to more devastating attacks such as denial of service .These vulnerabilities are a result of the nature of the transmission media. Intrusion detection system IDS is a process of identifying and responding to malicious activity targeted at computing and networking resources. A wireless IDS is unique in that it detects attacks against the 802.11 frame at layer two of the wireless network. There are three different types of 802.11 MAC frames; data, control, and management. The Objective of this project is to design a self learning system that will reduce the numbers of features and that will accurately determine the attacks at the Data Link Layer [3].

IDS can be classified according to IDS's environment as: a network-based IDS (NIDS) that is a dedicated computer, or special hardware platform, with detection software installed that captures packets in a promiscuous mode, or as a host-based IDS (HIDS) that monitors the resource usage of the operating system (OS) and the network. HIDS can only monitor the resource usage of the applications and not the applications themselves. Intrusion detection techniques are classified into two broad categories: misuse detection and anomaly detection. Misuse detection works by searching for the traces or patterns of well-known attacks. Clearly, only known attacks that leave characteristic traces can be detected that way. Anomaly detection, on the other hand, uses a model of normal user or system behavior and ages significant deviations from this model as potentially malicious. This model of normal user or system behavior is com-

monly known as the user or system profile. Strength of anomaly detection is its ability to detect previously unknown attacks [4, 5, 6].

2. Related Works

In [3] Baig M. N. et al., present model for feature selection uses the information gain ratio measure as a means to compute the relevance of each feature and the k-means classifier to select the optimal set of MAC layer features that can improve the accuracy of intrusion detection systems while reducing the learning time of their learning algorithm. The optimization of the feature set for wireless intrusion detection systems on the performance and learning time of different types of classifiers based on neural networks. Experimental results with three types of neural network architectures clearly show that the optimization of a wireless feature set has a significant impact on the Efficiency and accuracy of the intrusion detection system. ***In [7] Neelakantan N. P. et al.***, present that 802.11 network, the features used for training and testing the intrusion detection systems consist of basic information related to the TCP/IP header, with no considerable attention to the features associated with lower level protocol frames. The resulting detectors were efficient and accurate in detecting network attacks at the network and transport layers, but unfortunately, not capable of detecting 802.11-specific attacks such as deauthentication attacks or MAC layer DoS attack. ***In [8] Al-Janabi S. T. et al.,*** they tend to develop an anomaly based intrusion detection system (IDS) that can promptly detect and classify various attacks. Anomaly-based IDSs need to be able to learn the dynamically changing behavior of users or systems. they are experimenting with packet behavior as parameters in anomaly intrusion detection. There are several methods to assist IDSs to learn system's behavior. Their proposed IDS use a back propagation artificial neural network (ANN) to learn system's behavior. They have used the KDD'99 data set in our experiments and the obtained results satisfy the work objective. ***In [9] Haldar N. A. et al.,*** they present an intrusion detection system which exploits pattern recognition techniques to model the usage patterns of authenticated users and uses it to detect intrusions in wireless networks. The key idea behind the proposed intrusion detection system is the identification of discriminative features from users activity data and use them to identify intrusions in wireless networks. The detection module uses PCA technique to accumulate interested statistical variables and compares them with the thresholds derived from users activities data. ***In [10] Gupta V. et al.,*** analyze attacks that deny channel access by causing pockets of congestion in mobile ad hoc networks. Such attacks would essentially prevent one or more nodes from accessing or providing specific services. In particular, we focus on the properties of the popular medium access control (MAC) protocol, the IEEE 802.11x MAC protocol, which enable such attacks. They consider various traffic patterns that an intelligent attacker(s) might generate in order to cause denial of service. They show that conventional methods used in wire-line networks will not be able to help in prevention or detection of such attacks. Our analysis and simulations show that providing MAC layer fairness alleviates the effects of such attacks. ***In [11] Lakhina S. et al,*** present a new hybrid algorithm PCANNA (principal component analysis neural network algorithm) is used to reduce the number of computer resources, both memory and CPU time required to detect attack. The PCA (principal component analysis) transform used to reduce the feature and trained neural network is used to identify the any kinds of new attacks. Test and comparison are done on NSL-KDD dataset. It is a new version of KDDcup99 and has some advantages over KDDcup99, the experiments with NSL-KDD data demonstrate that our proposed model gives better and robust representation of data as it was able to reduce features resulting in a 80.4% data reduction, approximately 40% reduction in training time and 70% reduction in testing time is achieved. ***In [12] Peddabachigaria S. et al.,*** presents two hybrid approaches for modeling IDS. Decision trees (DT) and support vector machines (SVM) are combined as a hierarchical hybrid intelligent system model (DT–SVM) and an ensemble approach combining the base classifiers. The hybrid intrusion detection model combines the individual base classifiers and other hybrid machine learning paradigms to maximize detection accuracy and minimize computational complexity. Empirical results illustrate that the proposed hybrid systems provide more accurate intrusion detection systems. ***In [13] Depren O. et al.,*** propose a novel Intrusion Detection System (IDS) architecture utilizing both anomaly and misuse detection approaches. This hybrid Intrusion Detection System architecture consists of an anomaly detection module, a misuse detection module and a decision support system combining the results of these two detection modules. The proposed anomaly detection module uses a Self-Organizing Map (SOM) structure to model normal behavior. Deviation from the normal behavior is classified as an attack. The proposed misuse detection module uses J.48 decision tree algorithm to classify various types of attacks. The principle interest of this work is to benchmark the performance of the proposed hybrid IDS architecture by using KDD Cup 99 Data Set, the benchmark dataset used by IDS researchers.

3. Analyzing Critical Points in Current Wireless IDS

The major limitations with the current Wireless Intrusion Detection Systems are:

1. There is no available standard dataset for wireless intrusion detection as in wire networks, where KDD'99 presents the benchmark dataset for training and testing.
2. Noise limits intrusion detection systems effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.
3. It is very possible for the number of real attacks to be far below the false-alarm rate. Real attacks are often so far below the false-alarm rate that they are often missed and ignored.
4. Many attacks are prepared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to new strategies of attacks.

4. The Proposed Model of WNIDS

The proposed WNIDS is a DM-based IDS in which both the misuse and anomaly detection techniques depended in the detection of intrusion, where each record in a constructed dataset is labeled as "normal" or "intrusion (specify class of intrusion)" and a learning algorithm is trained over the labeled dataset. Misuse technique is able to automatically retrain ID models on different input data that include new types of attacks, as long as they have been labeled appropriately. While anomaly technique should first learn the characteristics of normal activities and abnormal activities of the system, and then the IDS detect traffic that deviate from normal activities.

For training and testing of the proposed WNIDS a constructed dataset, named "*Wdataset*", will be used. *Wdataset* dataset composed of features derived from the header of the WLAN 802.11 frame in data link layer. The design and the implementation of the proposed WNIDS, as depicted with diagram in figure (1), will be according to the following consequence steps these are;

1. Prepare WLAN 802.11 Network and Collect the Wdataset
2. Feature selection,
3. Classifiers building, and
4. Classification (testing).

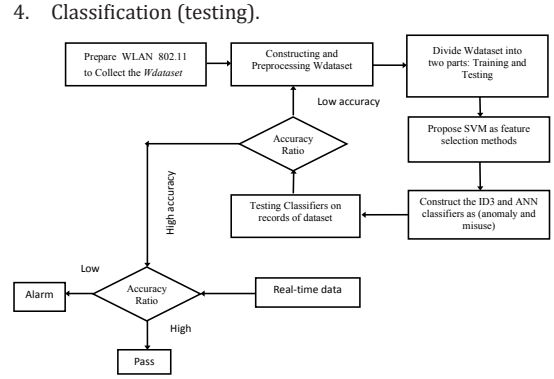

Figure 1 Diagram of the proposed WNIDS

Volume : 2 | Issue : 10 | October 2013 • ISSN No 2277 - 8179

4.1 Prepare WLAN 802.11 Network and Collect the Wdataset

The data will use to train and test the classifiers were collected from a wireless local area network. The local network is composed of 5 wireless stations and two one access points. One machine is used to generate normal traffic of HTTP and FTP. The second, third and fourth machines transmit simultaneously data originating from 4 types of WLAN attacks. The fifth station is used to collect and record both types of traffic (normal and intrusive (type of intrusion). The attacks will use to test proposed WNIDS are the 4 types of WLAN attacks (de-authentication, chopchop, fragmentation and duration). There is no real WLAN traffic dataset which can be considered as benchmark to be used in this area of researches. Here select and construct features from MAC layer (Data link layer). Figure (2) shows the contents of the MAC Data in IEEE 802.11. All these information can be used to construct features.

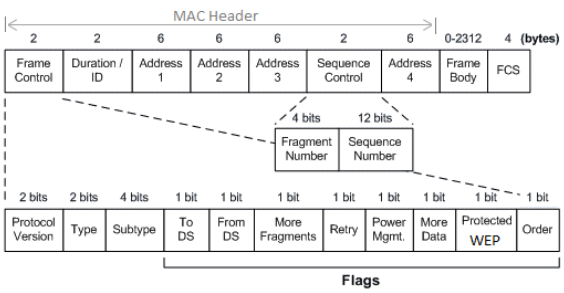

Figure (2): Frame WLAN 802.11with details.

To collect WLAN traffics from the constructed WLAN 802.11 we use Wireshark tool. We collect 2000 frames. From each frame we extract the following features 16 features the 15 features are clearly found in the header and we add one more feature not found explicitly in frame this is the last one (casting type);

- Protocol version, two bits indicate which version of the 802.11 MAC is contained in the rest of the frame.
- Type; indicate the type of the frame (Mgmt, Ctrl, Data).
- Subtype, indicate the Subtype of the frame.
- To DS, indicate if a frame is destined to the Distribution System.
- From DS, indicate if a frame is non final fragment or not.
- More Fragmentation, indicate whether a frame is non final fragment or not.
- Retry, indicate if the frame is retransmitted frame.
- Power Management, indicate whether the station is active or in Power Saving Mode.
- More Data, indicate whether an access point has buffered frames for a dozing station.
- Protected Wep, indicate if the frame is processed by the WEP protocol.
- Order, indicate if the "strict ordering" delivery is employed.
- Duration, The number of microseconds the medium is expected to be busy.
- RA, the MAC address of the receiving station.
- TA, the MAC address of the transmitting station.
- MA, depending on the values of To DS and From DS fields, this addresses can be the MAC address of the sending, Destination or Base Station.
- FCS, frame Check Sequence, which contains a 32 bit CRC.
- Casting type, Unicast Multicast Broadcast.

The data collected were grouped in two sets: training and testing sets. The first set is used to reach the optimal classifiers. The training set contains the input with its desired output. Testing dataset are necessary to avoid the effect of over fitting, it should be able to predict the output of each entry of the testing data set.

4.2. Feature selection

Feature Selection, also known as "subset selection" or "variable selection", is a common pre-processing step used in data mining because it treat huge no. of data with many attributes, where a subset of the features available from the original data are selected for subsequent application of a learning algorithm. Feature selection is the most critical step in building intrusion detection models since it tend to reduce, if possible, number of features and select the most intrinsic of these features in the classification decision, and hence to minimize the computation time of implementing the classification algorithms and so of the proposed system. Feature selection was proven to have a significant impact on the performance of the classifiers, since it can reduce the building and testing time of a classifier by 50 percent, that according many of experiments and studies.

Support Vector Machine Classifier SVM used as classification task usually includes with training and testing data which consist of some data examples. Each example in the training set contains one base values and several attributes. The goal of SVM is to introduce a model which predicts base value of data example in the testing set which is given only the attributes. Classification in SVM is Supervised Learning. Known typecast help indicate whether the system is performing in a right way or not. This information points to a coveted response, validating the precise of the system, or be used to help the system learn to do correctly.

In our proposal we use SVM classifier as approach for feature selection since it is a useful technique for data classification because it determines the critical point (attributes or variables) to distinct two classes. Here in our proposal we apply SVM five times on training dataset these are;

1. SVM to distinguish normal from general unknown intrusion traffic.
2. SVM to distinguish normal from deauthentication intrusion traffic.
3. SVM to distinguish normal from chopchop intrusion traffic.
4. SVM to distinguish normal from fragmentation intrusion traffic.
5. SVM to distinguish normal from duration intrusion traffic.

Then union the support features for each SVM, and from applying SVM as in algorithm (1), five times we find SVMs subset.

Algorithm (1): Feature Selection-SVM

Input: Wdataset for training and testing.

Output: Results of intrinsic features come from union of applying SVM for five times to distinguish among normal, four known intrusion and unknown intrusion.

Steps:

1. Initialize all points in training dataset as (Xi, Yj) where X is a vector of data x1, ……, xn and Y is vector of classes.
2. Initialize vector of weight W.
3. Distribute all points (x, y) and extract the hyper plane separator.
4. If the hyper plane give optimal separation then depend hyper plane as classifier model to classify testing dataset and go End
5. Else must do the following steps
6. $\Phi(w) = \frac{1}{2} w^t w$ Maximize the hyper plan using equation of Getting Maximum Margin = MM = 2 / ||w||. …….. (1)
7. For minimum using equation same as maximizing ……. (2)
8. Initialize Lagrange multiplier αi vector α1…αn using equation

   Q(α) =Σαi - ½ΣΣαiαjyiyjxiTxj …….. (3)
7. Apply classification function using equation f(x) = ΣαiyixiTx + b …….. (4)

8. Determine the support vectors xi with non-zero α_i (support vectors are the points determine the area of hyper plan)

9. Depend the hyperplan resulted after determining support vectors as the classifier model to classify testing dataset. That mean take the features present the supports depended as classifier to be the intrinsic features of distinguish between two classes.

10. End

4.3. Suggested ID3 and ANN Classifiers

After the intrinsic features had been selected, the two popular DM classification algorithms: ID3 from Decision Tree field and ANN from soft computing field, used in the design of the proposed WNIDS.

A "*Decision Tree classifier*" is one of the most widely used supervised learning methods used for data exploration. It is easy to interpret and can be re-represented as *If-then-else* rules. This classifier works well on noisy data. With ID3 classifier, a decision tree has been constructed starting with *training dataset* as the *"root node*" of the tree, then split it into several sub-datasets nodes according to the feature with the *"highest GR"* value and the columns with this feature in each of these nodes will be removed, and the split process will be repeated with these new nodes. Before deciding to split each new constructed node, computing:

- the "number of classes" in it,
- its "initial entropy",
- specify the "selected and used features",
- and, the "InfoGain" and "GR" of each feature in the node.

The splitting continues until either all records in the node are labeled with the same class or there is no feature to split the node according to feature's values. After splitting stage has been stopped, a set of "*top-down"* paths will be constructed from the root node of the tree to each leaf node in it. A path consists of a series of feature-value pairs ending with a class label. This set of paths examined to discover and delete the duplicated once. Then these paths converted to "*if-then-else"* rules (i.e. classification rules) which will be used then to classify records of the *testing dataset*. Algorithm (2) explains ID3 algorithm with Intrusion detection learned on collected Wdataset dataset.

Algorithm (2): *Suggested-ID3*

Input: A dataset (Wdataset) of training examples, *S,* and testing.

Output: A decision tree (classifier model).

Steps:

1. Create the root node containing the entire set S
2. If all examples are positive, or negative, then stop: decision tree has one node. Otherwise (the general case).
3. Select feature that has the largest GR value
4. For each value from the domain of feature :
5. add a new branch corresponding to this best feature value, and a new node, which stores all the examples that have value for feature
6. If the node stores examples belonging to one class only, then it becomes a leaf node, otherwise below this node add a new subtree, and go to step 3
7. End

An artificial neural network is a system simulating work of the neurons in the human brain. The neuron consists of some inputs emulating dendrites of the biological neuron, a summation module, an activation function and one output emulating an axon of the biological neuron. The importance of a particular input can be intensified by the weights that simulate biological neuron's synapses. Then, the input signals are multiplied by the values of weights and next the results are added in the summation block. The sum is sent to the activation block where it is processed by the activation function. Thus, we obtain neuron's answer to the input signals "x". Here will use in more conventional MLP (Multi Layer Perceptron) approach as misuse detection techniques to identify class of intrusion traffics (these are detected intrusion in the first level classifier and sent to the second level to determine it is class). Algorithm (3) explains ANN algorithm with Intrusion detection learned on Wdataset dataset.

Algorithm (3): Suggested-ANN

Input: Wdataset for training and testing.

Output: Optimal ANN (classifier model).

Steps:

1. Main Assumption for the Training Process of MLP:
- Learning method: Quasi Newton BFGS and Levenberg-Marquardt
- Number of Epochs: 1000.
- MSE (Mean Square error): 0.01.
- Learning rate: 0,9.
- Activation function: log-signoid.
- Number of neurons in the Input layer: (41 or according no. of SVM set).
- Number of neurons in the hidden layer: (21 for 41 input neurons and with no. of SVM set equal to half of this no.).
- Number of neurons in the output layer: (6 cause no. of intrusions classes are 4, unknown intrusion and the normal class).
- Update of weights – batch mode (after presentation of the entire training data set).

2. Train and Test on Wdataset to construct final ANN model for WNIDS.
3. End.

Discussion and Experiments

The proposal has been implemented on the following platform: Windows 7 Ultimate Service Pack1 and 64-bit OS, 32GB RAM, and Intel® Core (TM) 3 Duo CPU with 2.00GHz; and by using Visual Basic.Net programming language and SQL.

We collect 2000 frames using wireshark tools to construct, from these frames we construct Wdataset which conducted by selecting 1250 (1000 for training and 250) for testing) frame with optimal features' values (no missing values, no noisy and no redundant) and then distribut the data collected to training and testing and specify no. of frames for normal and each attacks in both training and testing as in table (1).

Table (1): No. of Records selected from Wdataset for Training and Testing

No. of Records/Type of Records	Training	Testing
Deauthentication	220	40
Chopchop	180	50
Duration	200	50
Fragmentation	150	40
Normal	250	70

Both of ID3 and ANN classifiers will be used 2 times with each of these 2 sets of features to design the proposed classifiers; all 44 features of *training dataset* and subset of features in according to the result of SVM method. Thus, four classifiers will be obtained: two ID3 classifiers and two ANN classifiers. Then the classification of the *testing dataset*'s records will be done with each one of these classifiers, and a comparison among their classification results will be done in order to specify the most accurate classifier among them.

Now before explaining results will present the voted 8 features as the best set of features that maximizes the distinguish of the SVM among normal, known four intrusion and unknown intrusions, these features are { Type, Subtype, To DS, More Fragmentation, Retry, Protected Wep, Duration, Casting type}.

Training which consist of two classifiers (ID3 and ANN) on *Training dataset* has been done with two sets of features (*All_Features*, *SVM_Features)*, so the proposed system has been experimented (i.e., trained and tested) for two times to each set of features to assess the accuracy of the classifiers and select the one of best and higher accuracy of detection. We performed three different experiments and selected a subset of eight features that indicates better performance as compared to others. Our aim is to select minimum features that produce optimal results in accuracy. This definitely impact on overall performance of the system. The features are reduced to 8 from the 41 raw features set. The above experiments show that optimal features increased accuracy, reduced training and computational overheads and simplified the architecture of intrusion analysis engine.

Results of three conducted experiments (Exp1, Exp2, Exp3), which producing the most accurate results, have been presented in this section. Four classification models have been constructed in each of these three experiments.

Next these models have been applied on the same *Testing dataset*, which has been constructed during Exp1, to assess the validation and accuracy of these constructed models on the same testing dataset. The classification results of testing are either **TP** (intrusion), **TN** (normal), false positive (**FP**) (misclassified as intrusion), false negative (**FN**) (misclassified as normal), **Unknown** (new user behavior or new attack). From classification results we calculate the detection rate (**DR**) of IDS is the ratio between the number of TP and the total number of intrusion patterns presented in the testing dataset. It has been calculated using

$$DR = \frac{TP}{TP+FN+Unknown2} * 100\% \quad \text{.....(5)}$$

, and the false alarm rate (FAR) of an IDS is the ratio between number of "normal" patterns classified as attacks (FP) and the total number of "normal" patterns presented in the testing dataset. It has been computed using

$$FAR = \frac{FP}{TN+FP+Unknown1} * 100\% \quad \text{.....(6)}$$

Values for both of DR and FAR for each classifier in the three experiments have been illustrated in table (2).

Table (2): DRs and FARs of both of them ID3 and ANN Classifiers

ID3 Classifier				ANN Classifier			
Feature Selection Measure	Experiment No.	DR	FAR	Feature Selection Measure	Experiment No.	DR	FAR
SVM	1	0.996	0.02	SVM	1	0.999	0.01
	2	0.997	0.02		2	0.999	0.01
	3	0.996	0.02		3	0.999	0.01
ALL	1	0.994	0.02	ALL	1	0.995	0.04
	2	0.993	0.03		2	0.995	0.03
	3	0.993	0.07		3	0.995	0.03

DR are higher with ANN classifiers higher than with ID3 classifiers and FAR often ranging between (0 - 0.07) with ID3 where is much less in ANN classifiers. It is very clear from these that ANN classifiers are better than ID3 classifiers. Selection of the best classification model would be done significantly according to its classification accuracy, which is introduced as the ratio between the number of the correctly classified patterns (TP, TN) and the total number of patterns of the testing dataset. The ***accuracy (Accu)*** of each classifier has been calculated using

$$Accu = \frac{TP+TN}{TP+FP+TN+FN+unknown} * 100\% \quad \text{..... (7)}$$

Table (3) summarizes *Accu* of both ID3 and ANN classifiers with *SVM_F and ALL_F* in the three experiments. According to these results, the classifiers ID3 and ANN were more accurate with *SVM_F Accu*.

Table (3): Accuracy of ID3 and ANN Classifiers

Classifier	Experiment No.	SVM_F	ALL_F
ANN	1	0.999	0.996
	2	0.999	0.996
	3	0.999	0.997
ID3	1	0.997	0.994
	2	0.998	0.995
	3	0.998	0.995

6. Conclusion

Feature selection is an important task of network intrusion detection. Using SVM as a feature selection approach, intrusions are detected with less error rate and high accuracy. Usage of ANN for intrusion detection introduces high accuracy than with ID3 as in tables (2 and 3). Where notice the higher rates of detection and very less rates of false alarms especially with SVM set of features with both classifier ID3 and ANN. The added feature (casting) which is not found directly in frame header was important variable in classification, so we think if there is an additional process to the frame to extract more feature may affect in increasing the performance.

REFERENCE

1. Barhoo T. S. and ElShami E., "Detecting WLANs' DoS Attacks Using Backpropagate Neural Network", Journal of Al Azhar University-Gaza (Natural Sciences), 2011, 13 : 83-92, | http://www.alazhar.edu.ps/journal123/natural_Sciences.asp?typeno=1 | 2. Tulasi R. L. and Ravikanth M., "Impact Of Feature Reduction On The Efficiency Of Wireless Intrusion Detection Systems", International Journal Of Computer Trends And Technology- July To Aug Issue 2011, Issn: 2231-2803 Http://Www.Internationaljournalssrg.Org Page 171. | 3. Baig M. N. and Kumar K. K. , "Intrusion Detection in Wireless Networks Using Selected Features", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, 1887-1893. | 4. Lalli and Palanisamy, "Modernized Intrusion Detection Using Enhanced Apriori Algorithm", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 5, No. 2, April 2013, [IVSL]. | 5. Rehman R. U., "Intrusion Detection Systems with Snort: Advanced IDS Techniques with Snort, Apache, MySQL, PHP, and ACID", Pearson Education, Inc. Publishing as Prentice Hall PTR, 2003. | 6. Garuba M., Liu C., Fraites D., "Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems", IEEE Computer Society, Fifth International Conference on Information Technology, pp. 592-598, 2008. | 7. Neelakantan N. P., Nagesh C. and Tech M.., "Role of Feature Selection in Intrusion Detection Systems for 802.11 Networks", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Volume-1, Issue-1, 2011. | 8. Al-Janabi S. T., and Saeed H. A., "A Neural Network Based Anomaly Intrusion Detection System", IEEE Computer Society, 2011 Developments in E-systems Engineering, pp. 221-226. | 9. Haldar N. A., Abulaish M. and Pasha S. A., "An Activity Pattern Based Wireless Intrusion Detection System", IEEE Computer Society, 2012 Ninth International Conference on Information Technology- New Generations, pp. 846-847. | 10. Gupta V., Krishnamurthy S., and Faloutsos M., " Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks", This material is based upon work supported by the National Science Foundation under Grant No. 9985195, DARPA award N660001-00-18936 | 11. Lakhina S., Joseph S. and verma B., "Feature Reduction using Principal Component Analysis for Effective Anomaly–Based Intrusion Detection on NSL-KDD", Shilpa Lakhina et. al. / International Journal of Engineering Science and Technology Vol. 2(6), 2010, 1790-1799. | 12. Peddabachigaria S., Abraham A., Grosanc C., and Thomas o., "Modeling intrusion detection system using hybrid intelligent systems", Journal of Network and Computer Applications, 1084-8045/$ - see front matter r 2005 Published by Elsevier Ltd. doi:10.1016/j.jnca.2005.06.003. | 13. Depren O., Topallar M., Anarim E., and Ciliz M. K. , "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks", Expert Systems with Applications 29 (2005) 713–722 0957-4174/$ - see front matter q 2005 Elsevier Ltd. All rights reserved. doi:10.1016/j.eswa.2005.05.002 |