In order to study the impact of the optimized set of features on both the learning phase and accuracy of the ANN networks, we have tested these attributes on three types of ANN architectures.

3 H U F H S W U R Q

Perceptron is the simplest form of a neural network. It's used for classification of linearly separable problems. It consists of a single neuron with adjustable weights of the synapses. Even though the intrusion detection problem is not linearly separable, we use the perceptron architecture as reference to measure the performance of the other two types of classifiers.

0 X O W L O D\HU EDFN SURSDJDWLRQ S%W D Q

The multilayer back propagation perceptions architecture is an organization of neurons in n successive layers (n > ¼ 3). The synapses link the neurons of a layer to all neurons of the following layer. Note that we use one hidden layer composed of eight neurons.

TABLE 4
Distribution of Collected Data

	Learning	Validation	Test
Normal	6000	4000	5000
De-authentication	900	600	800
Duration	900	600	800
Fragmentation	900	600	800
Chopchop	900	600	800
Total	9600	6400	8200

8.3 Hybrid Multilayer Perceptrons

The Hybrid Multilayer Perceptrons architecture is the superposition of perceptron with multilayer ackpropagation perceptrons networks. This type of network is capable of identifying linear and nonlinear correlation between the input and output vectors [19]. We used this type of architecture with eight neurons in the hidden layer. Transfer function of all neurons is the sigmoid function. The initial weights of the synapses are randomly chosen between the interval [_0:5, 0:5].

9 DATA SET

The data we used to train and test the classifiers were collected from a wireless local area network. The local network was composed of three wireless stations and one access point. One machine was used to generate normal traffic (HTTP, FTP). The second machine simultaneously transmitted data originating from four types of attacks. The last station was used to collect and record both types of traffic (normal and intrusive

The data collected were grouped in three sets (Table 4): learning, validation, and testing sets. The first set is used to reach the optimal weight of each synapse. The learning set contains the input with its desired output. By iterating on this data set, the neural network classifier dynamically adjusts the weights of the synapses to minimize the error rate between the output of the network and the desired output.

Fig. 3. Learning time (in seconds) for the three types of neural networks using 8 and 38 features.

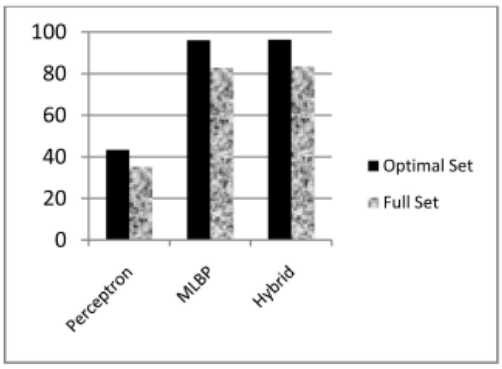

Fig. 4. Detection Rate percentage of the three types of neural networks using 8 and 38 features.

The following table shows the distribution of the data collected for each attack and the number of frames in each data set.

10 EXPERIMENTAL RESULTS

Experimental results were obtained using Neuro Solutions software [20]. The three types of classifiers were trained using the complete set of features (38 features), which are the full set of MAC header attributes, and the reduced set of features (eight features). We evaluated the performance of the classifiers based on the learning time and accuracy of the resulting classifiers. Experimental results clearly demonstrate that the performance of the classifiers trained with the reduced set of features is higher than the performance of the classifiers trained with the full set of features

As shown by the previous graph, the learning time is reduced by an average of 66 percent for the three types of classifiers.

The performance of the three classifiers is improved by an average of 15 percent when they are tested using the reduced set of features. Fig. 5 and Fig. 6 show the experimental results of false positives and false negatives. The false positives rate is the percentage of frames containing normal traffic classified as

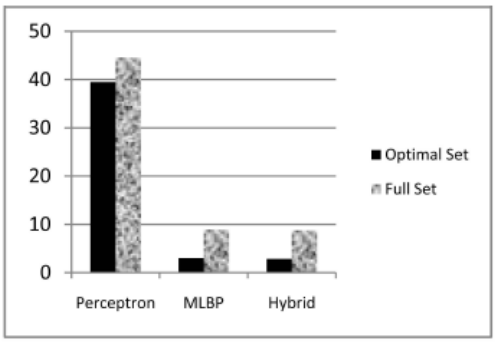

Fig. 5. False Positives Rate (%) for the three types of neural networks using 8 and 38 features.

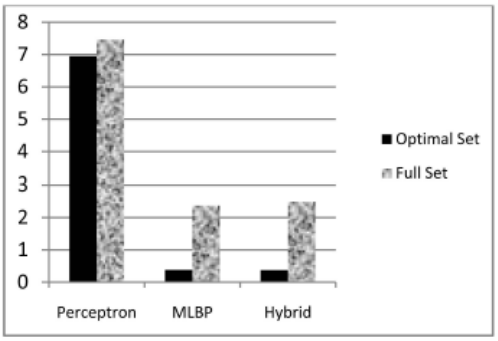

Fig. 6. False Negatives Rate (%) for the three types of neural networks using 8 and 38 features.

intrusive frames. Likewise, the false negatives rate is thepercentage of frames generated from wireless attacks which are classified as normal traffic.

The false positives rate is reduced by an average of 28 percent when the reduced set of features is used. If the perceptron classifier is excluded, the combined false positives rate of the MLBP and Hybrid classifiers is reduced by 67 percent. As shown in Fig. 6, the combined false negatives rate of the MLBP and Hybrid classifiers is reduced by 84 percent.

11 CONCLUSIONS and FUTURE WORK

In this paper, we have presented a novel approach to select the best features for detecting intrusions in 802.11- based networks. Our approach is based on a hybrid approach which combines the filter and wrapper models for selecting relevant features. We were able to reduce the number of features from 38 to 8. We have also studied the impact of feature selection on the performance of different classifiers based on neural networks. Learning time of the classifiers is reduced to 33 percent with the reduced set of features, while the accuracy of detection is improved by 15 percent. In future work, we are planning to do a comparative study of the impact of the reduced feature set on the performance of classifiers-based ANNs, in comparison with other computational models such as the ones based on SVMs, MARSs, and LGPs.

REFERENCES

[1] A. Boukerche, R.B. Machado, K.R.L. Juca´ , J.B.M. Sobral, and M.S.M.A. Notare, “An Agent Based and Biological Inspired Real- Time Intrusion Detection and Security Model for Computer Network Operations,” Computer Comm., vol. 30, no. 13, pp. 2649- 2660, Sept. 2007.
[2] A. Boukerche, K.R.L. Juc, J.B. Sobral, and M.S.M.A. Notare, “An Artificial Immune Based Intrusion Detection Model for Computer and Telecommunication Systems,” Parallel Computing, vol. 30, nos. 5/6, pp. 629-646, 2004.
[3] A. Boukerche and M.S.M.A. Notare, “Behavior-Based Intrusion Detection in Mobile Phone Systems,” J. Parallel and Distributed Computing, vol. 62, no. 9, pp. 1476-1490, 2002.
[4] Y. Chen, Y. Li, X. Cheng, and L. Guo, “Survey and Taxonomy of Feature Selection Algorithms in Intrusion Detection System,” Proc. Conf. Information Security and Cryptology (Inscrypt), 2006.
[5] H. Liu and H. Motoda, Feature Selection for Knowledge Discovery and Data Mining. Kluwer Academic, 1998.
[6] http://kdd.ics.uci.edu/databases/kddcup99/task.html, 2010.
[7] A.H. Sung and S. Mukkamala, “The Feature Selection and Intrusion Detection Problems,” Proc. Ninth Asian Computing Science Conf., 2004.
[8] A.H. Sung and S. Mukkamala, “Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks,” Proc. Symp. Applications and the Internet (SAINT ’03), Jan. 2003.
[9] G. Stein, B. Chen, A.S. Wu, and K.A. Hua, “Decision Tree Classifier for Network Intrusion Detection with GA-Based Feature Selection,” Proc. 43rd ACM Southeast Regional Conf.—Volume 2, Mar. 2005.
[10] A. Hofmann, T. Horeis, and B. Sick, “Feature Selection for Intrusion Detection: An Evolutionary Wrapper Approach,” Proc. IEEE Int’l Joint Conf. Neural Networks, July 2004.
[11] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proc. USENIX Security Symp., pp. 15-28, 2003.
[12] http://www.aircrack-ng.org/, 2010.
[13] Y.-H. Liu, D.-X. Tian, and D. Wei, “A Wireless Intrusion Detection Method Based on Neural Network,” Proc. Second IASTED Int’l Conf. Advances in Computer Science and Technology, Jan. 2006.
[14] T.M. Khoshgoftaar, S.V. Nath, S. Zhong, and N. Seliya, “Intrusion Detection inWireless Networks Using Clustering Techniques with Expert Analysis,” Proc. Fourth Int’l Conf. Machine Learning and Applications, Dec. 2005.
[15] S. Zhong, T.M. Khoshgoftaar, and S.V. Nath, “A Clustering Approach to Wireless Network Intrusion Detection,” Proc. 17th IEEE Int’l Conf. Tools with Artificial Intelligence (ICTAI ’05), Nov. 2005.