NOVEL NEUROCOMPUTING-BASED SCHEME TO AUTHENTICATE WLAN USERS EMPLOYING DISTANCE PROXIMITY THRESHOLD

Tarik Guelzim and Mohammad S. Obaidat
Computer Science Department, Monmouth University, West Long Branch, NJ 07764, U.S.A.

Keyword: Security of WLANs, Authentication, Distance, Proximity, Neural Networks, Performance Evaluation.

Abstract: The IEEE 802.11 standard is considered one of the most popular and profitable network topology in use today. As with the growth of every other technology, the scalability of Wireless Local Area Networks (WLANs) comes with the burden of ensuring the integrity, confidentiality and trust in the network. By integrity we need to develop a mechanism by which only authorized users can gain access to the network resources. Confidentiality implies that every data transmitted by each user stays known only to the communication parties. The above two characteristics can then enforce a trust environment in which all wireless nodes and users are authorized and secure. In this paper, we propose a scheme to authenticate and authorize 802.11 wireless nodes within a network. Our proposed scheme relies on neural networks decision engine that restricts network access to mobile nodes whose physical location is within a threshold distance from the wireless access point or the controller of the network. We present a detailed description of the work done as well as a performance analysis of this scheme.

1 INTRODUCTION

The popularity of mobile computing and mobile devices such as PDAs, laptops, notebooks and alike have raised security issues on wireless networks. These latter advancements urged to define mechanisms by which we can restrict network access. Luckily, this issue was solved since the inception of the 802.11 protocol using various methods such as public key cryptographic algorithms, passwords, access cards, ticket servers and others. Nevertheless, these solutions do not give the flexibility needed or desired by hotspots and public Internet zones for example. Because of the embedded cost of setting up such authentication systems as well as the ownership cost of maintaining such infrastructure, business owners in most cases opt out to not use any of the above mentioned security features and offer an unsecure connection channel to their free wireless zone users. Although this decision is solely based on financial basis, the security of the users as well as the confidentiality of the data they access or transmit is open to malicious users without any protection. A good solution to resolve this issue must be scalable, meaning that its performance is not affected in case the network shrinks or grows in size. Cost efficient in this context means that it can be implemented with minor changes to the current infrastructure in terms of hardware and/or software. Transparent, meaning that deploying this solution will not require users to install or upgrade any of their devices in order to access the network. Lastly, it must put into perspective the quality of service (QoS) of the wireless network and not introduce any major overhead that deteriorates and affects user experience. In our proposed scheme, we tackled all of these issues and created an authentication and authorization system that can be suitable for deployment in any public wireless zone. Location is one of the contextual variables that are most important in the design of context aware computing (Obaidat and Boudriga, 2007, Nicopolitidis, 2003, Dey, 2001). Applications require this type of data in order to provide accurate data in both form and content. For example, based on a node's location within a museum a system might be able to provide content in different languages based a room's theme. It can also provide content once it senses that a user is physically present within a room. One of the

Guelzim T. and S. Obaidat M. (2008).
NOVEL NEUROCOMPUTING-BASED SCHEME TO AUTHENTICATE WLAN USERS EMPLOYING DISTANCE PROXIMITY THRESHOLD.
In *Proceedings of the International Conference on Security and Cryptography*, pages 145-153
DOI: 10.5220/0001929901450153

earliest systems that dealt with location aware wireless applications was the active badge system. This method required users to wear a badge that emits signals to a centralized grid of sensors which in turns report to a master server to perform further analysis of location data (Want et al., 1992). Another ubiquitous system is the Global Positioning System (GPS) through which mobile users can estimate their location with great accuracy. Nevertheless, GPS does not function well within indoor environments because the signal reception is very low. The cricket system described in (Priyantha, 2000) defined a new context aware solution based on ultrasound pulses in order to estimate the distance between a transmitter and a received.

All of the previous solutions work with respect to the environment they are deployed in, the only drawback they present is the necessity for extra hardware to be installed and the fact that they do not target wireless LAN infrastructures. A first attempt at this was presented by (Bahl, and Padmanabhan, 2000); this system, RADAR, uses 802.11 Wireless LAN (WLAN) along with a statistical model based on the nearest neighbor clustering algorithm. The main idea is that the location of the user can be determined if we send an ultrasound signal to the receiver and upon reception of that signal we can calculate the flying time of that signal, thus determining its location. The experiment also fixed the grid size to the same size in order to have all cells with the same characteristics. From the view point of performance analysis and accuracy of the localization method, this scheme showed that the simulation results were far from close to the analytical cases that were conducted in reality using the same method. In (Seshadri, 2005), the authors used a probabilistic method to estimate user location. The experiment in (Jan and Lee, 2003) described a fingerprinting technique that reduces the efforts in building a map table by defining any wireless node in terms of at most two APs power readings. Another localization scheme was proposed by (Pandey et al., 2006) aimed at providing a location determination technique that is easy to deploy. Their work also uses triangulation technique that records the signal strength from three AP previously fixed at a specific location. Another scheme of location positioning was presented in (Mundt, 2006) using a collaborative sensing. We can classify location based techniques into two sets: a deterministic technique and a probabilistic technique. The deterministic technique tries to represent the signal as a scalar value and estimate the location of the system based on that value while the probabilistic techniques are more accurate as they store information about the location of the user and use probability to approximate that location. In this paper, we present a novel access control approach that uses a neural network engine to predict the location of WLAN users that are either requesting to join the network or a resource in it. We also show how this scheme can be used a QoS mechanism to optimize network sharing and load balancing.

2 MOTIVES

In this section, we define usage and necessity scenarios in which each participating party, client and server has a requirement in order to demonstrate the practicality and feasibility of our proposed work.

2.1 Scenario 1: Hotspot Wireless Internet

In this first scenario we consider two parties: a user who wants to use the already existing free and public wireless network while on the source's premises and a controlling authority (CA) who wants to offer this free service to only those clients that are trying to connect from within its business area.

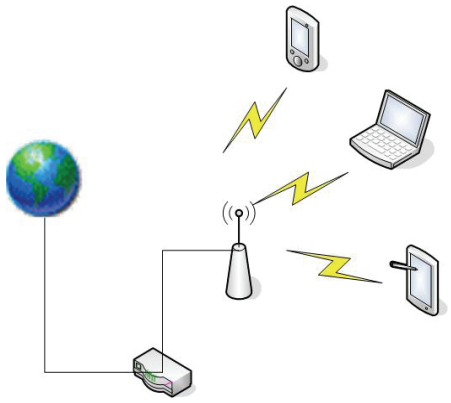

Figure 1: Coffee shop Hotspot WLAN infrastructure.

We emphasis on the fact that the CA wants to offer the free service to its clients only, although this can still be implemented using an Authorization, Authentication and Accounting server (AAA) such as FreeRadius for example, it does not offer the flexibility required by such a dynamic environment

where in the case of a coffee shop, customers come in, check their emails and leave as quickly as possible. Using such a server would be overkill. Instead, we need a solution that will ensure that only the customers of that hotspot zone can receive access to the system and that this functionality is accomplished transparently to both server and client i.e. no password or subscription is needed to do it.

2.2 Scenario 2: Network Resource Sharing in an 802.11 Wireless Network

In this second scenario, we consider a network setup in which we have a public wireless file server that serves files to its clients. Under normal circumstances, this scenario does not prove any deployment difficulties, however, if we have a larger number of users that are trying to retrieve data at the same time, we can clearly see that we might need to add mirror servers to the current setup in order to distribute the load on the single server.

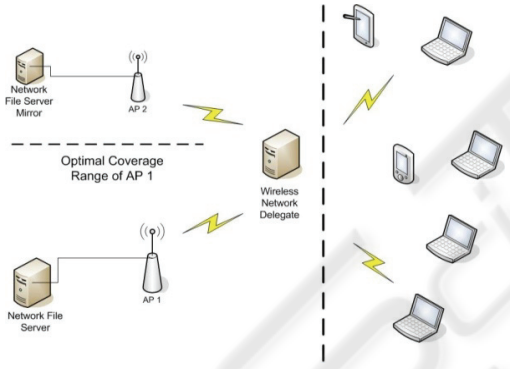

Figure 2: Optimization of network resources sharing based on physical proximity.

In the above WLAN setup, we route all requests to a wireless network delegate that determines, transparently, which mirror to assign to which user based on a heuristic model. Our model, in this case, is to infer the user's location, and assign the mirror server that is, physically, close to it.

2.3 Scenario 3: Authorization to Access Files and/or Resources Remotely

Often in big environments, users are given the right to access corporate data remotely. This can pose a serious threat if security measures are breached. One way to strengthen the security is to use some mechanism by which we can add a challenge to a user in addition to the already used public key schemes (PK) and cryptographic techniques. Using our work, for example, we can restrict access to resources to only those users that are within a physical threshold area. To make this clearer, we can restrict usage of the network to only those users that are within 'x' meters of the source where 0<x<maximum threshold.

The previous three scenarios were usage cases in which the proposed work in this paper is suitable for. In all three cases we need a mechanism by which we can authenticate and authorize usage of network resources based on the physical location of the user. Users that are within the permitted distance from the network are granted access and those that are outside are denied it.

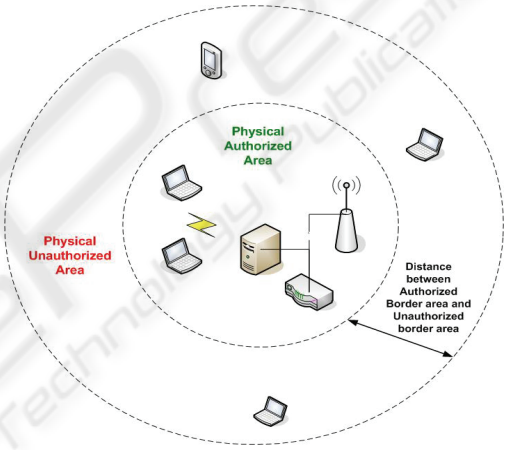

Figure 3: 802.11 Network security based on distance threshold authorization proximity scheme.

3 PROPOSED SCHEME

In this paper, we propose a scheme with the goal to add another authentication and authorization mode to the existing 802.11 networks based on physical proximity threshold. Our scheme relies on neurocomputing to learn cluster and make decisions on whether the user, device or node that is requesting to connect to the system is able to authenticate to the network given its physical proximity from the access authority controller based on the threshold distance that is defined by the implementation. As mentioned earlier, we created a network topology to match a generic common infrastructure in which there exists an access point and wireless nodes connecting to it with range. NS2 simulation package was used to conduct the analysis.

3.1 Access Point

We took a bottom up approach when designing our network topology. As in any wireless infrastructure, we started by defining the properties of the access point. This latter is an 802.11 compatible router that can serve up to 64 wireless nodes. We opted for the Two Ray Ground radio propagation model, which is used to mimic the free propagation model in real deployments. Access points must contain a buffer to process the received packets. In our experiments, we defined a buffer size of 2MB using a priority queue in which packets that are received first are processed first unless their priority flag states otherwise. The use of priority queues was picked because in wireless security, it is usually the case that certain packets such as management packets are processed first because they might include information that might affect the overall flow of the operation of the network. For example, an access point must process disassociation packets first because disconnecting a malicious node as soon as possible might have a big impact on the compromised network. The AP also transmits the electromagnetic signal using an Omni-antenna. We have chosen this antenna type to match the current mode in most commercial router devices. The AP also handles routing using the Direct Sequence Distance Vector (DSDV) algorithm. As in most 802.11 networks, the Z-order of the access point is not taken into consideration because it is usually installed in the same level as the WN. This is not true in other types of wireless networks such as GSM for example where the base station BS is usually installed at a high altitude to cover a larger cell area as well as to prevent issues such as line of site (LOS) problems.

3.2 Mobile Wireless Nodes

In our network simulation, we defined mobile wireless nodes that access the network resources via the access point defined above. These nodes are generated randomly using a scenario script and move throughout the network perimeter defined previously. The mobile nodes use the same physical characteristics as the AP i.e. the antenna and transmission types. In order to make the simulated network identical to wireless local area network in real conditions, we defined the access point as well as the wireless nodes in the same subnet. This last condition is very important because we are trying to simulate an environment in which the mobile nodes are requesting access directly from the AP in the same network. This implies that putting them on a separate subnet forces the handshake packets to travel across a wired backbone, thus, the packet energy cannot be relied on because its physical characteristics altered too much. The wireless node movement within the simulated grid is random; i.e. all nodes start at a random position and they all move in different but continuous directions. By continuous direction we imply that there is no jump over or cuts in the path because doing so is inconsistent with real human movements. As in the case of the AP, the wireless nodes are positioned in the same Z-order as the AP, i.e. on the same level. To get the simulation to run at a high degree of realism, we observed how nodes move in the students' area of our University and recorded the way they moved in terms of x and y coordinates. After recording such data, we reproduced WN movement accordingly. Before we delve into the experiment, let us recap what we are trying to accomplish. We are trying to correlate the wireless user's distance from the access point and granting access to use the WLAN. This is a new level of security, because even if the user, whether malicious or not, tries to access to system, he must prove that he is physically located where he claims to be. This scheme can be used alone or in combination with other well known security schemes to protect sensitive information and data that can for example be accessed from within the company's authorized perimeter only and remotely through a network.

In order to accomplish this goal without incurring any change to the existing infrastructure, we use the power of the received packets to approximate the location of the transmitter. The approximation process as we will detail later, is done using a neural network system to learn and cluster the input data.

3.3 Grid Definition

To simulate our topology, we defined a 670 by 670 grid where we position our access point as well as the mobile nodes. The figure bellow depicts the grid topology that we used in our simulation.

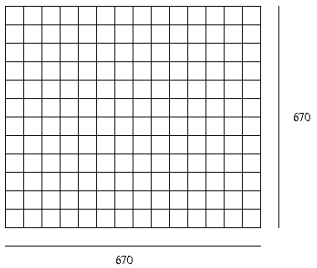

Figure 4: Simulated Grid Topology.

The above is the grid topology we simulated. We have chosen such a big dimension because we also wanted to account for cases in which we know that the transmitted signal is not reachable and where malicious users can use high gain antennas to receive the AP signal and use the same antennas to transmit their location.

3.4 Handshake Implementation

This is an important factor in training our neural net to recognize false packets. Since this is an authentication mechanism in wireless networks, we are only interested in the packets sent in the handshake phase. The following figure depicts how we simulated this process using our network simulation.

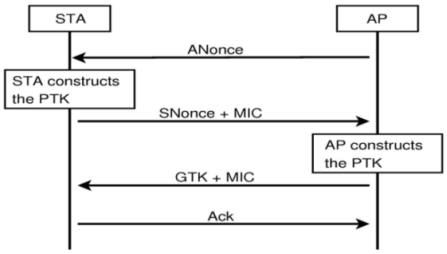

Figure 5: 802.11 Four -Way Handshake.

The 4-Way handshake, as summarized in Figure 5, requires that the AP determines that it is talking to an authorized mobile node, and the mobile node must also ensure that it is communicating with an authorized AP and not a 'Rogue' device. Rogue devices are illegal devices that are placed into the network for malicious use such as diverting traffic or flooding the network with packets that lead to Denial of Service (DoS) attacks and other attacks.

3.5 Neural Network Classifier

Training a Neural Network is a core component in our work because it enables us to extract patterns from the data collected from the simulation and learn how mobile nodes roam inside the grid as well as how they interact with the rest of the system. The neural net enables us also to approximate and predict the pre-assumed location of the mobile nodes in the system even though if there is a new or an irregular pattern is presented for the first time to the system. Training a neural network is not as trivial task. Some experimentation has to be done with different configurations and learning schemes until we find a network whose output is as close as possible to the presented data. We varied the structure of the hidden layer, including adding new hidden layers. When the NN is presented with the input data, the hidden layer as well as the output layers must have an activation function that forces the corresponding neurons to fire a value that is bounded by the domain of the activation function. We experimented with both the TanH function as well as the sigmoid function, as we will explain later. The sigmoid function performed better than the hyperbolic Tangent one. As for the training of the NN, we used the Back Propagation algorithm (BP). Our general NN template consists of an input layer with two inputs; the first input is the received power per packet and the second input is the average power received from the sending location. We have two hidden layer each of 8 neurons. The hidden layers have a sigmoid activation function that outputs in the range -1 to +1. The hidden layer is attached to two output neurons. The first neuron indicates a received power within the authorized zone, while the second neuron indicates a received power that is in the unauthorized zone. Training the new configuration was accomplished on the same hardware platform as well as the same data sets of 5000 power readings. For each training run, we run the network for 1000 iterations; however, we varied the learning rate by a decrement and/or increment of 0.1 each time until we obtained a network that has the characteristics of the data presented.

4 PERFORMANCE EVALUATION

4.1 Simulation Parameters

In order to get reliable results we ran the simulation for twenty five (25) minutes in which random nodes were generated inside the grid and were not destroyed until the simulation ended. Using this scheme, we generated 80,000 packets for a total traffic of 120MB.

Table 2: Simulated Scenario.

Simulation Run Time	25 minutes
Number of Nodes	670
Packets Generated	80,000
Traffic Generated	≈ 120 MB

As noted above, we tried to generate as much data as possible because training our Neural Network

engine is a two phase process, a learning phase and a validation phase. The next section will detail how this process works.

4.2 Analysis of the Signal Strength Data

As mentioned above, we ran the simulation for 25 minutes and produced 80,000 received signal strength indicator (RSSI) reads, which is, in telecommunications, a measurement of the power in the received radio signal. That data was split into two parts. The first part is used for training the neural network and the second part is used for testing. We have to ensure that the input data to the neural network is valid. As mentioned above we used the received packet power and the average power for a particular distance as input to the neural network. The simulation uses a "Two Ray Propagation Model" to simulate the properties of the transmitted signal. We compared the output power of the simulation to Fris analytic formula which indicates how data fits the propagation models of modern routers. Fris formula, $\mathbf{P=kr^{-n}}$, expresses the received power as inversely proportional to the distance. In our case, free space, the term n is equal to 2, and hence the power is said to be inversely proportional to the square root of the distance.

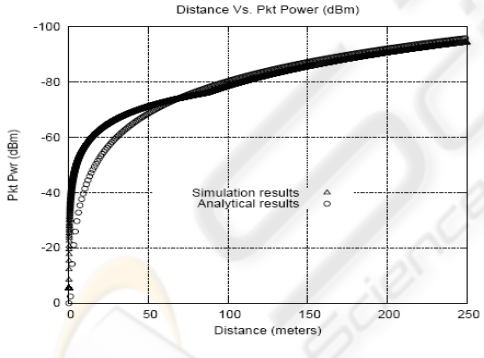

Figure 6: Comparison of distance V.s. power for both simulation and experimental results.

In a normal setup, we expect the received power to decrease as the distance increases from the source. The experimental results follow Fris model and as we can see it preserves this property. The simulation results are the data obtained by running the simulation via NS2. Depending on the deployment of the system, ranges from 0 to 50 meters might represent a deployment in a small office home office (SOHO) setup in which the physical area (diameter) from the source node i.e. router is of that range. As the range starts to grow, we indicate that the deployed system is of a wider physical area such as corporate or university campuses.

4.3 Neural Network Configurations Performance

As mentioned earlier, a neural network that performs well in terms of correctly mapping the packet power to the correct location is essential for the performance of our system. For that reason, we experimented and trained different NN paradigms and compared their performance in terms of predicting the location of wireless nodes.

The above graph shows five NN paradigms with different learning rates and activation functions. Based on the results we obtained the first type, which is based on a linear model, failed to map every packet power introduced to it. The other two paradigms used a sigmoid activation function in which the NN with the LR=0.4 has a very high success rate for distances 2 meters away from the source and above. However it has almost 98% failing rate for distances less than 2 meters. On the other hand, the NN paradigm with an LR=0.3 has a more balanced distributed error across all distances. For example, it can approximate the location of 90% of users within 2 meters, 79% of users less than 1 meter, and 97% of the entire wireless user population within 10 meters. This is very good performance for our application since in the scenarios we mentioned in section 2, 10 meters is a good resolution.

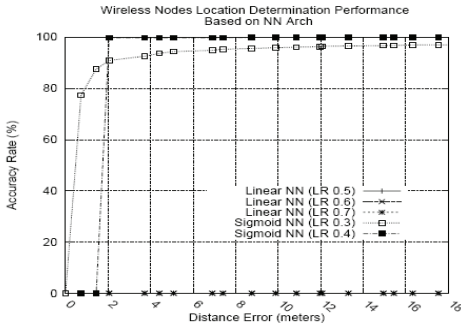

Figure 7: CDF of error in wireless node prediction.

4.4 WLAN Authentication Performance using our Scheme

In the following sections, we considered the setup to be a SOHO layout such as a department floor or a coffee shop place.

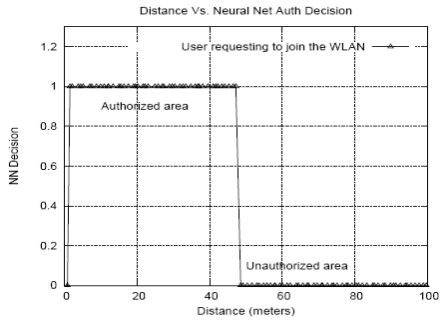

Figure 8: Users requesting to join the network and online Neural Net authentication decision.

In the above experiment, we defined the threshold for the authorized region to be 50 meters while any request from a farther distance is considered to be in the unauthorized zone. The above graph also shows initial results of the decision made by the neural network. We expected the network to output a value close to one indicating a successful authentication and a value close to zero indicating an unsuccessful one. Figure 8 gives a clearer picture on this authentication process.

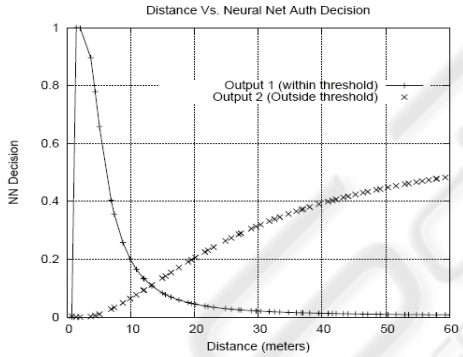

Figure 9: Users requesting to join the network and online Neural Net authentication decision based on approximated distance.

Figure 9 shows an online view of authentication decisions made by the neural network as the wireless nodes request the authentication from it. The increasing curve corresponds to the users in the prohibited region that are trying to authenticate while the decreasing curve corresponds to the users in the authorized region that are requesting to authenticate. We tested the system with 670 users requesting to authenticate at different times of the day. As we are going to explain later we were successful in authenticating users rightfully 95% of the time. The error is depicted in the leftmost section of the authorized curve. We expected all requesting users in that section of the graph to have a value equals to 1. What we obtained was a value of zero (0). Thirty out of the six hundred users (30 out of 670) were not authorized even though they were in the authorized section. This translates into 5% error margin (30/670). We refer to this as type I error or false rejection of authorized users.

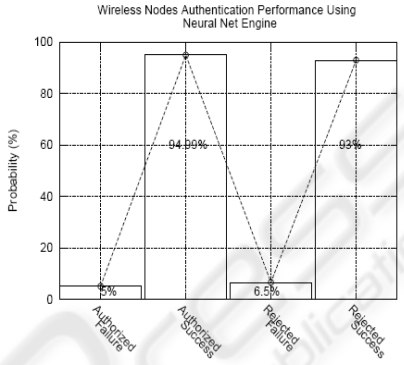

Figure 10: System Performance.

As explained before, we ran the test on the system to check its performance with respect to successfully authenticating users and denying unauthorized ones from connecting to the network.

We input 670 authentication requests to the system and we calculated the following errors.

Authorized failure (type 1): This is the indication of how many users who were inside the authorized zone of the network and were denied access by the system.

Rejected failure (type 2): This is the indication of how many users were outside the authorized zone and were granted access to the system.

The authorized failure was, as indicated previously, 5% since 33 users out of the 670 were denied access. The unauthorized failure was 6.5% where 43 out of the 670 were granted access while requesting to authenticate from the unauthorized zone. The Success rate, responding correctly to authentication requests, was 94.99%, and denying illegal users was 93%.

In order to evaluate the performance of our system fully, we compared the neural network location estimation based technique with other systems and in terms of probability of success vs. distance error. The following are the results we obtained:

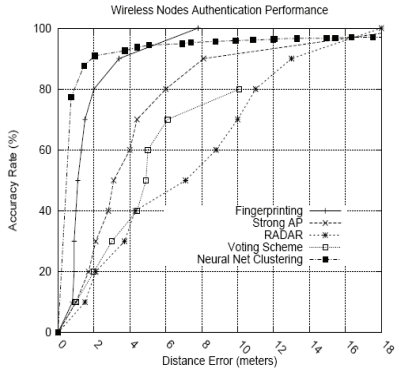

Figure 11: Accuracy rate comparison with different location methods.

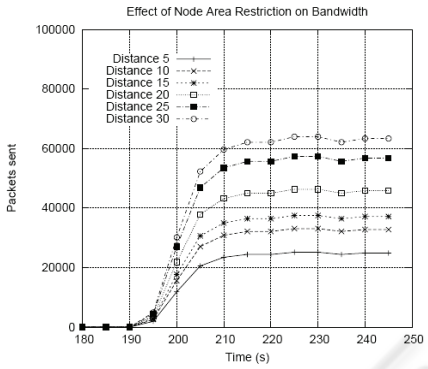

Figure 12: Effect of Node Area Restriction on Bandwidth.

Figure 11 indicates how our system performs with respect to three other techniques. The first technique, fingerprinting, is a method by which the wireless node is given a "fingerprint" based on the physical location within vicinity. This technique gives good performance for short distances and can identify all nodes in an 8 meter radius. The next technique is the strong AP. This latter uses multiple access points to probe the wireless node which in turns takes the highest signal to estimate its position. This technique is not suitable for our application because of the cost setting up the infrastructure. Our technique, neural net clustering, on the other hand, proved to be very efficient in terms of resources as well as the performance. As the above results show, we are able to estimate 92% of the users within 2 meter error margin vs. 4.2 meters for the Strong AP technique and 16 meters for fingerprinting and radar techniques respectively. A two meter resolution is more than suitable for our security application and in terms of authentication as well as authorization of wireless users.

In the following section, we ran an experiment to see how the neural network authentication scheme can be used to optimize the bandwidth of the underlying network.

4.5 Neural Network Authentication as a Bandwidth Preserving Scheme

In this experiment, we used our NN authentication scheme to study its effect on the WLAN bandwidth. We measured the network bandwidth in terms of packets sent across the network. As we can see from Figure 12, we restrict network access to areas of smaller radius using the NN, network traffic can be reduced. This seems logical; however, our proposed technique makes it possible to implement it in environments where we want to force a load balance between multiple access points. In Figure 12, we started by restricting network access to users within 30 meters. In this scenario, we generated about 60,000 packets. In each run, we made the authorized zone radius, i.e. threshold, smaller by a factor of 5 meters. Following this method, we generated 55,000, 43,000 and 38,000 packets for 25, 20 and 15 meters, respectively. The trend we noticed is that the bandwidth used can be restricted by making the authorized zone smaller in area. In scenarios where we have multiple access points, this proposed scheme may be used to force wireless users to connect to resources that are closer to them in terms of distance and thus we can distribute network load across the network.

5 CONCLUSIONS

In this paper, we presented a novel approach that uses neurocomputing to authenticate users in a wireless local area network. This technique uses distance proximity from the access point to restrict access to the network. We explained some scenarios in which our scheme can be applicable such as in coffee hotspots, forcing enterprise access security policies or in network traffic load balancing as examples. In terms of performance metrics, we measured two types of errors. The first error is the is the probability of rejecting authorized users while the second error is the probability of authenticating (accepting) unauthorized users. The former error rate was 5% and the latter is 6.5%. Our clustering scheme using NN showed performance higher than that for other methods that were described with success rate of 95% versus 87% and 30% for the fingerprinting and strong AP, respectively. We also

extended this work to see its impact on the bandwidth of the network. We noticed that it is possible to use it as a QoS technique in order to balance the network load in case we need to add another AP to the system.

REFERENCES

M. S. Obaidat and N. Boudriga," Security of e-Systems and Computer Networks," Cambridge University Press, 2007.

P. Nicopolitidis, M. S. Obaidat, G. Papdimitriou, and A. S. Pomportsis," Wireless Networks," John Wiley & Sons, 2003.

A.K. Dey, "Understanding and Using Context In Personal and Ubiquitous Computing", *ACM Transactions on Information Systems,* vol. 5, pp. 4-7, Feb. 2001 .

R. Want, A. Hopper, V. Falcao, and J. Gibbons. "The active badge location system", *ACM Transactions on Information Systems.* Vol. 10, pp. 91-102, Jan. 1992.

N.B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System", *ACM Int'l Conf. Mobile Computing and Networking"*, pp. 32-43, Aug. 2000.

Bahl, P. and V.N. Padmanabhan, "An in-building RF-Based Location and Tracking System", *IEEE INFOCOM*, Vol. 1, pp. 775-785, Mar. 2000.

V. Seshadri, G.V. Zaruba, and M. Huber, "A Bayesian Sampling Approach to In-door Localization of Wireless Devices Using Received Signal Strength Indication", *IEEE International Conference on Pervasive Computing and Communications*. pp. 75-84, Mar. 2005.

R.H. Jan and Y.R. Lee, "An Indoor Geolocation System for Wireless LANs", *IEEE International Conference on Paralled Processing Workshops*, p. 29, Oct. 2003.

S. Pandey, F. Anjum, B. Kim, and P Agrawal, "A Low-Cost Robust Localization Scheme for WLAN", *ACM International workshop on wireless internet,* Vol 220, p. 17 2006.

T. Mundt. "Two Methods of Authenticated Positioning", *ACM International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, pp. 25-32, Oct. 2006.