Defence Against 802.11 DoS Attacks Using Artificial Immune System

M. Zubair Shafiq and Muddassar Farooq

College of Electrical & Mechanical Engineering
National University of Sciences & Technology
Rawalpindi, Pakistan
zubairshafiq@ieee.org, muddassar.farooq@udo.edu

Abstract. In this paper we present an Artificial Immune System (AIS) based security framework, which prevents a number of serious Denial of Service (DoS) attacks. The proposed security framework can counter de-authentication and disassociation attacks. The results of our experiments clearly demonstrate that the proposed framework approximately achieved 100% detection rate with negligible false positive rate. One can conclude from the ROC (Receiver Operating Characteristics) plots of our AIS that its performance approaches 'perfect classification point' at a suitable matching threshold value.

Keywords: 802.11, Network Intrusion Detection, Artificial Immune System.

1 Introduction

Artificial Immune Systems (AISs) are inspired from Biological Immune System (BIS) in vertebrates [1]. BIS protects the body of an organism from foreign antigens. BIS has the remarkable ability to distinguish *non-self* from *self*. AIS maps this feature of BIS to distinguish an anomalous behavior from a normal behavior. AIS learns the normal behavior of a system by tuning an appropriate group of *detectors*. These detectors are used to discriminate the *non-self* antigens from the *self* antigens. Antigens and detectors (antibodies) can be mapped to a n-dimensional real shape-space, where antigen and detector represent two points [1]. The detectors utilize the concept of affinity (affinity between antigen and detector is measured in terms of distance between these points) to differentiate non-self from self. During the initialization phase detectors are generated in a random fashion. However, they are later tuned to *self* using the process of negative selection [3]. The malicious nodes in communication networks can significantly disrupt the normal operations of the networks. AIS based frameworks are ideally suited for NID systems which differentiate the malicious behavior from the normal behavior in the network.

AIS based NIDs have been successfully deployed at the Network layer in wired networks [2,3]. But, to the best of our knowledge, little attention has been paid to the vulnerability analysis of wireless networks. The shared communication

L.N. de Castro, F.J. Von Zuben, and H. Knidel (Eds.): ICARIS 2007, LNCS 4628, pp. 95–106, 2007.

medium and the open connectivity policy of wireless networks introduce novel security threats that are not experienced in the wired networks. A number of serious security threats have been discovered at the MAC layer of 802.11b networks.

IEEE 802.11 has become the popular standard for wireless networks in recent years [5]. Most wireless standards deployed today use IEEE 802.11b standard and it is the oldest (launched in July 1999) [5]. With the increasing popularity and usage, several security loopholes and vulnerabilities have been discovered. IEEE 802.11b has been identified for vulnerabilities at Media Access Control (MAC) layer. WEP (Wired Equivalent Privacy) is a classical framework that is deployed at the MAC layer to provide security [5]. In this approach, MAC frame is encrypted using WEP algorithm. Open source tools are available that can break 802.11b WEP. The researchers have also proposed a number of other schemes such as WPA (WiFi Protected Access) and WPA2 (in 802.11i) to cater for security threats in 802.11. These schemes have also failed to provide a satisfactory security level [16,17].

AISs have been used for misbehavior detection in wireless networks [6,8,21]. But almost all these works have focused on routing misbehavior. In this paper we present our comprehensive AIS framework for intrusion detection at the MAC layer. This work is a cardinal step towards the development of a meta-NID based on AIS for misbehavior detection at multiple layers of the protocol stack.

The rest of the paper is organized as follows. In Section 2, we provide a brief introduction to 802.11b wireless networks and discuss different types of vulnerabilities that a malicious node can easily exploit to disrupt the network's operations. In Section 3, we provide a brief review of related work in which AIS has been utilized in NID. We then introduce our AIS based security framework for 802.11b networks in Section 4 and then discuss the experimental results in Section 5. Finally we conclude our work with an outlook to our future research.

2 802.11b Networks

Different wireless standards have emerged to cater for the rapid growth of wireless networks. But IEEE 802.11b is the most popular standard that is deployed in the real world. IEEE 802.11b covers the Media Access Control (MAC) and the physical layer [5].

2.1 Topologies of 802.11b Networks

MAC layer of 802.11b defines two access schemes:

Point Coordination Function (PCF). This scheme is also called infrastructured networks where the complete network is managed by an Access Point (AP). The AP acts as the coordinator in the network. The clients connect to the AP using an authentication and association mechanism.

Distributed Coordination Function (DCF). This scheme is also called ad-hoc networks which are without coordinator (an AP in case of PCF). In DCF, the clients communicate with each other through the shared channel. The clients, however, have to compete for getting access to the channel. This challenge is not present in PCF in which a station only transmits if it is scheduled a time slot by the AP [5].

2.2 Types of Frames

Three types of frames are exchanged by the communicating nodes at the MAC layer of an 80211b network.

1. Data Frames are used for data transmission.
2. Control Frames are used to control access to the shared medium.
3. Management Frames are only used to exchange management information and hence are not forwarded to the upper layers [5].

2.3 Vulnerabilities in 802.11b Networks

Several vulnerabilities of 802.11b Networks are reported by the authors in [16] which include *Passive Eavesdropping*, *Active Eavesdropping*, *Message Deletion*, *Malicious AP*, *Session Hijacking*, *Man-in-the-Middle* and *De-authentication & Disassociation* attacks.

A malicious node is able to successfully launch the attacks because 802.11b networks provide an attacker the ability to sniff and interpret wireless traffic and spoof the MAC addresses of the AP and the clients. IEEE 802.11b utilizes crypto-based protocols such as WEP and WPA for providing security at the MAC layer. But the authors of [17] have shown that these crypto based solutions are subject to vulnerabilities. As a result, they are unable to provide an adequate security level.

In this paper we have focused on two specific types of DoS attacks which are launched by manipulating *management frames*:

De-authentication Attacks. As already discussed, an attacker can spoof the MAC address of a victim client provided that it has the ability to sniff and interpret the wireless traffic. In de-authentication attacks, an attacker spoofs the MAC address of a victim client and then uses it to send de-authentication frames to the AP (see Figure 1). This attack can significantly degrade the performance of the communication channel between the client and the AP (DoS) because the client, once de-authenticated, must restart authentication/association process again.

A number of schemes have been proposed and implemented for detection and prevention of de-authentication attacks. SNORT uses a '*threshold value of the number of de-authentication frames per unit time*' as a metric for detecting malicious attacker [14]. This scheme applied to bio-inspired techniques, such as genetic programming, results in significantly less detection rates [9,10]. In [18], the authors have used the strategy of delaying the response to de-authentication and disassociation requests. The receiver of the de-authentication frames waits for data frames in the subsequent frames. Valid data frames after

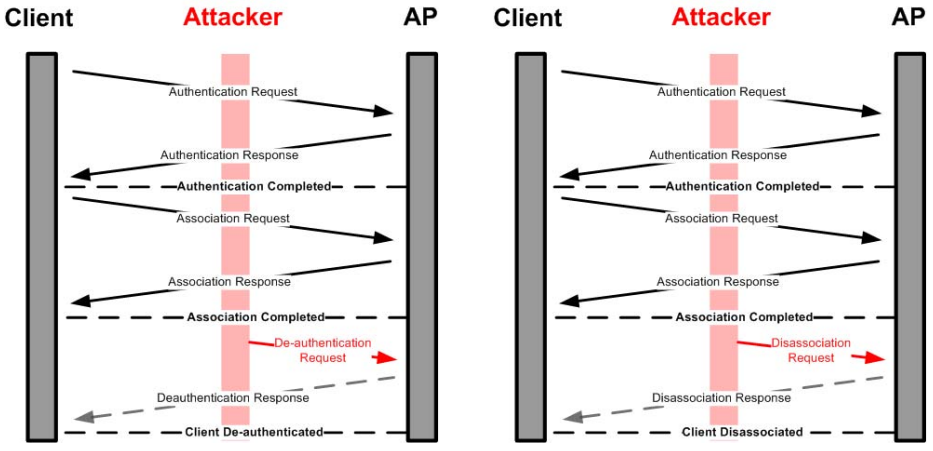

Fig. 1. De-authentication and Disassociation Attacks

the de-authentication frame is an indication of malicious de-authentication attack. This approach, however, results into a number of new vulnerabilities [19]. Another approach utilized the fact in 802.11b networks that the *Sequence Numbers* of the frames vary linearly in case of a normal activity. If an attacker launches the malicious de-authentication attack, then non-linear variations of large magnitudes are observed [6]. The variation in sequence numbers is an important parameter that can act as an indicator to detect de-authentication attack. Fuzzy rules in agent based schemes have also been utilized to detect these random variations in the sequence numbers [7]. In [10,11], the authors have used Genetic Programming to detect de-authentication attacks using such scheme.

Disassociation Attacks. The philosophy behind disassociation attacks is the same as in case of de-authentication attacks. An attacker spoofs the MAC address of a victim node, and then on its behalf sends the disassociation frames to the AP (see Figure 1). Disassociation attacks are less effective in reducing the performance of 802.11b networks because a victim node still remains authenticated with the AP. As a result, it only needs to restart the association process again. Nevertheless, disassociation attacks do cause the disruption in communication (DoS) between victim and AP.

3 AIS for Network Intrusion Detection

AISs have been used for network intrusion detection. The authors in [3] utilized the concepts of AIS such as clonal selection and negative selection for network intrusion detection. Hofmeyr et. al. presented a framework for AIS called *ARTIS* [2]. This framework was specialized for network intrusion detection in Light Weight Intrusion Detection Systems (*LISYS*). LISYS (for wired networks) operated at the Network layer of the OSI Stack [4].

In [6], the authors used a hybrid approach involving AIS for misbehavior detection in wireless ad-hoc networks. Their work is focused on detecting routing misbehavior in DSR (Dynamic Source Routing) due to malware or compromised nodes. In [8], the authors have used AIS exclusively to cater for similar routing misbehavior. In [20], the authors have employed AIS for securing a nature inspired routing protocol, Beehive. Recently they have also proposed an AIS based security framework for a nature inspired wireless ad hoc routing protocol, BeeAdHoc [21]. These works have set the ground for the use of AIS for misbehavior detection in wireless networks.

4 AIS Framework

Our AIS framework consists of two phases: *learning/training* and *detection phase*. During learning/training phase AIS tunes/tolerizes the detectors (antibodies) to the normal behavior of the network utilizing negative selection (*extended thymus action*) [22,23]. This learning/tuning phase takes approximately 30 seconds. During this phase, it is assumed that the system is under normal operating conditions (traffic is training traffic) and any type of anomalous behavior is not experienced during this phase. After learning phase, AIS enters into the detection phase in which it also counters the malicious traffic. During this phase the system detects the malicious traffic and takes countermeasures to neutralize its impact.

Table 1. AIS mapping to 802.11b-MAC

AIS	AIS for 802.11b-MAC
Self-Set	Training traffic set
Non-self Set	Test traffic set
Antigen-1	Antigen consisting of fields from de-authentication frame
Antigen-2	Antigen consisting of fields from disassociation frame
Antibody-1	Detector for de-authentication attacks
Antibody-2	Detector for disassociation attacks
Matching Technique	Euclidean distance matching

As already mentioned in the previous section, we utilized the same scheme that is based on the observation that the variation in sequences numbers in frames is significantly large in an attack scenario. The AIS mapping used in our AIS model for 802.11b networks is given in Table 1. A MAC frame is mapped on to one of the two types of antigens: type-1 consists of the fields extracted from the de-authentication frame and type-2 consists of the fields taken from the disassociation frame. The Euclidean distance matching technique is used to match antigens to antibodies (detectors). The formula for Euclidean distance is given below [1]:

$$D = \sqrt{\sum_{i=1}^{L} (Ab_i - Ag_i)^2}$$

We have defined two types of antibodies, type-1 and type-2, to cater for two types of attacks. The type-1 detectors are utilized to counter de-authentication attacks whereas type-2 detectors are used to counter disassociation attacks. Their *epitope model* is essentially the same but type-1 and type-2 detectors are tuned using separate sets of training traffic.

Figures 2 and 3 show the *MAC frame format* and *frame control* field respectively. The sub-fields which are used to vulnerability analysis are:

Type - 00 indicates that it is a *management* frame (2 bits)
Subtype - 1100 indicates that the management frame is a *de-authentication* frame, and 1010 indicates that the management frame is *disassociation* frame (4 bits)
toDS - 0 for management and control frames (1 bit)
fromDS - 0 for management and control frames (1 bit)
Sequence Control - subfield *sequence number* (12 bits)

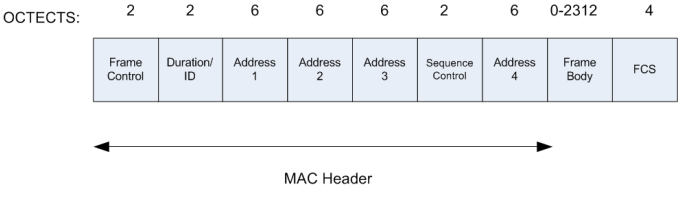

Fig. 2. MAC frame format [5]

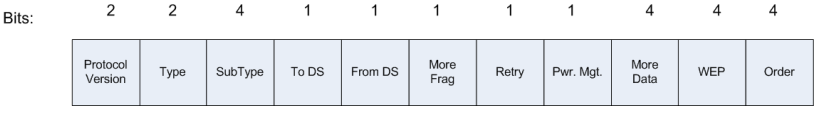

Fig. 3. Frame Control Field [5]

Figure 4 shows the antigen model for our AIS to counter attacks in 802.11b networks. First four fields of the antigen ensure that the appropriate management frame, de-authentication in case of type-1 antigen and disassociation in case of type-2 antigen, is encoded as an antigen. 12 bit *sequence control* field contains the sequence number field of 802.11b MAC frame. The detectors model the average difference in the sequence numbers for every client. It is worth mentioning that difference in the sequence numbers is 1 only in the case when consecutive frames reach the AP without any drops. In case of a lossy environment, the difference in the sequence number even for a client operating under normal conditions will be more than one. There the system needs to learn a threshold value under which the network operation are considered normal. If the distance between the antigen and the detector (antibody) is greater than this threshold value, then a successful match is made. As a result, this match will detect the malicious activity.

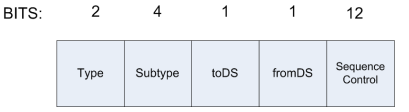

Fig. 4. Antigen Model

5 Results

5.1 Attack Scenario

De-authentication attack (Type-1). Consider the attack scenario, in which 5 clients are authenticated and associated to the Access Point (AP) (see Figure 5). The attacker node spoofs the MAC address of the victim node (node-2) and starts sending the de-authentication frames to the AP with random frequencies. AP will receive the de-authentication frame, and will consider this to be from the victim node. As a result, the connection of the victim node will be invalidated by the AP. In order to communicate again with the AP, node-2 will again have to undergo authentication and association phases (see Figure 1). Hence, the communication between the victim node and AP will be disrupted that might result into poor data transfer rates between the nodes. The level of disruption depends on the frequency of malicious de-authentication frames. In the most severe form of the attack, the victim node will never be able to reach the data transmission phase because as soon as it re-authenticates, next malicious de-authentication frame arrives. The victim node will again be de-authenticated and this malicious cycle repeats itself again. Hence, there is a need to identify and discard the malicious de-authentication frames from the attacker node at the AP. Our AIS will discriminate between the legal and malicious de-authentication frames on the basis of the difference in the sequence numbers of consecutive frames in case of attack.

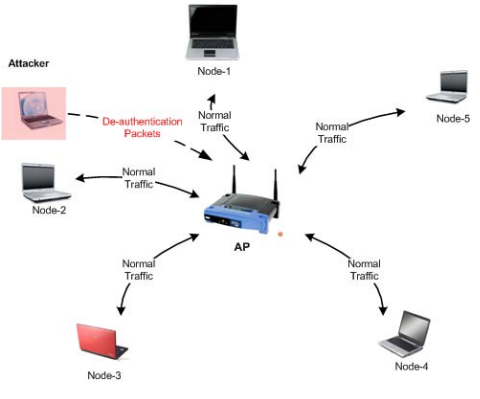

Fig. 5. Attack 1: De-authentication Attack

Disassociation attack (Type-2). Consider the similar attack scenario as shown in Figure 5. The attack node spoofs the MAC address of the victim node (node-2) and starts sending the disassociation frames to AP at random frequencies. AP will disassociate the victim client. In order to communicate victim client would have to undergo association process again, even if it remains authenticated. The reconnection overhead in this case is lesser than the de-authentication attacks as the victim client only has to undergo the association process before being able to enter data sending phase (see Figure 1). Still, disassociation attacks can cause significant disruption and therefore need to be countered. Our AIS will distinguish between legal and malicious disassociation frames on the basis of the difference in sequence numbers of consecutive frames in case of the attack.

5.2 Dataset Collection

The data-sets (both training and testing) were collected using the tools that are available on the internet such as Ethereal [12] and SMAC 2.0 [13]. Similar tools have also been used in [7] to collect the real traffic. As discussed earlier, the important thing to note in the attack part of testing data-sets is the difference in the sequence numbers when the the attack is launched.

The data-sets which are representatives of the captured traffic were processed by the proposed AIS. AIS requires the training data-set, which is free of attacks, to capture the notion of 'normal'. This training data-set is used to tolerize detectors to normal (*self*) so that they should not detect self-antigens which can result in high number of false alarms. AIS is then exposed to test data-set for detection of malicious de-authentication frames. Using these data-sets, we tested our AIS based NID system. Each run started with a different seed that is used to generate initial detector population randomly. The reported results are an average of the results obtained from 10 independent runs.

5.3 Performance Metrics

Figure 6 shows the 2x2 confusion matrix for the binary classifiers. Four possible outcomes of a classifier are True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN). The metrics considered for the evaluation

	P	N
Y	True Positives	False Positives
N	False Negatives	True Negatives

Fig. 6. 2x2 ROC Confusion Matrix (Redrawn from [15])

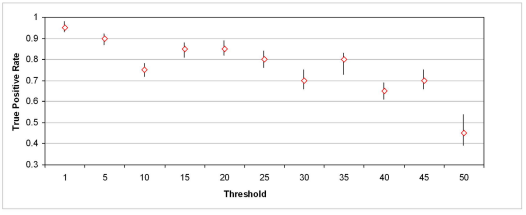

Fig. 7. True Positive Rate for testing data-set (type-1)

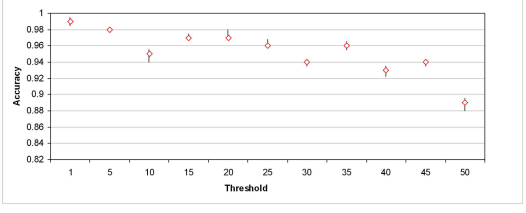

Fig. 8. Accuracy for testing data-set (type-1)

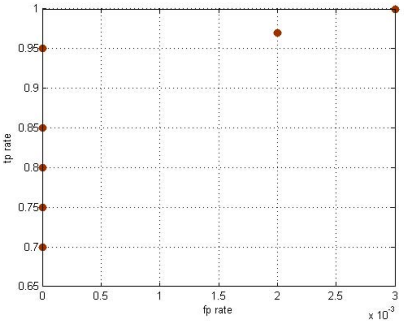

Fig. 9. The performance of our AIS system in the ROC space (type-1)

of AIS are false positive rate *(fp rate)*, true positive rate *(tp rate)* and *accuracy*. These metrics are defined as,

$$tp\ rate = \frac{TP}{P} \qquad fp\ rate = \frac{FP}{N} \qquad accuracy = \frac{TP+TN}{P+N}$$

5.4 Discussion on Results

De-authentication attack. An important parameter of an AIS is a threshold for the match between an antigen and an antibody (detector). We made an interesting observation when we analyzed the effect of varying matching threshold values on the value of false positive rate. We noticed that even for low values

of matching thresholds the value of false positive rate was significantly small (as low as 0.001%). Figures 7 and 8 show the plots for *true positive rate* and *accuracy* while varying matching *threshold* value. If we map the values of true positive rate and false positive rate for the type-1 attacks to Receiver Operating Characteristics (ROC) space (see Figure 9) then the performance of our AIS based system approaches the performance of *perfect classification point* [15]. The point at the top-right corner in Figure 9 where system approaches 100% true positive rate is at the threshold value of 4. Therefore, optimal threshold value for matching type-1 antigens and antibodies (detectors) is set to 4.

Disassociation attack. A low value of false positive rate can also be seen for disassociation attacks. This is essentially due to the similar nature of challenges

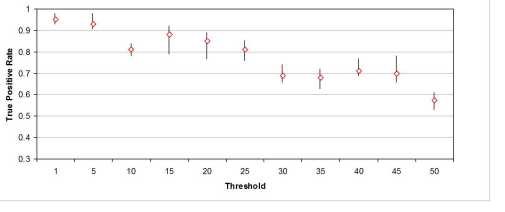

Fig. 10. True Positive Rate for testing data-set (type-2)

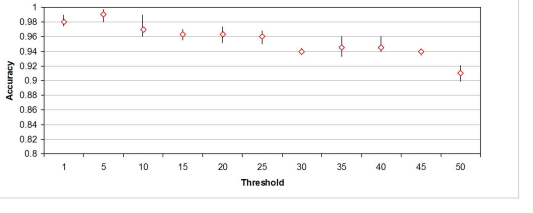

Fig. 11. Accuracy for testing data-set (type-2)

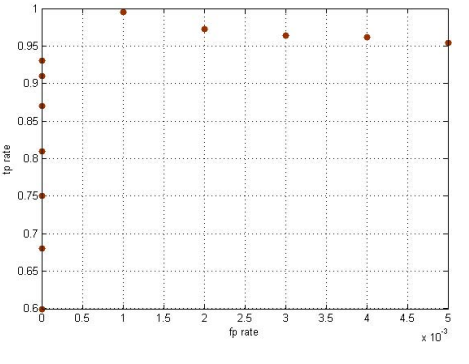

Fig. 12. The performance of our AIS system in the ROC space (type-2)

in both types of attacks. Figure 10 and 11 show the plots for *tp rate* and *accuracy* while varying the value of matching *threshold*. Figure 12 shows the ROC plot for type-2 attack. One can again see that our AIS based system has the performance of a perfect classifier even for type-2 attacks. The optimal matching threshold value for type-2 attacks was found to be 3.

6 Conclusion and Future Work

We have presented a security framework on the basis of principles of AIS for prevention of DoS attacks at the MAC layer. We focused on two specific attacks: de-authentication and disassociation. The results of extensive evaluation of our AIS show that our security framework is able to counter both types of attacks successfully and it has significantly small value of false positive rate. The memory overhead of our AIS based security framework is 3 bytes per detector that is significantly small. Our future objective is to develop a meta-security framework on the basis of AIS for misbehavior detection and prevention in wireless networks at multiple layers.

References

1. de Castro, L.N., Timmis, J.: Artificial Immune Systems: A New Computational Intelligence Approach. Springer, London (2002)
2. Hofmeyr, S.A., Forrest, S.: Architecture for an Artificial Immune System. Evoloutionary Computation Journal, 443–473 (2000)
3. Kim, J., Bentley, P.J.: Investigating the Roles of Negative Selection in an AIS for NID. IEEE Transactions of Evolutionary Computing, Special Issue on AIS (2001)
4. ISO Standard 7498-1:1994, `standards.iso.org/iso/`
5. ANSI/IEEE Std 802.11, 1999 edn. (R2003), `standards.ieee.org/getieee802/802.11.html`
6. Balachandran, S., Dasgupta, D., Wang, L.: A Hybrid Approach for Misbehavior Detection in Wireless Ad-Hoc Networks. Published in Symposium on Information Assurance, New York (June 14-15, 2006)
7. Kaniganti, M.: An Agent-Based Intrusion Detection System for Wireless LANs, Masters Thesis, Advisor: Dr. Dipankar Dasgupta, The University of Memphis (December 2003)
8. Sarafijanovic, S., Le Boudec, J.-Y.: An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors. In: 3rd International Conference on Artificial Immune Systems, pp. 342–356 (2004)
9. LaRoche, P., Zincir-Heywood, A.N.: 802.11 De-authentication Attack Detection using Genetic Programming. In: Collet, P., Tomassini, M., Ebner, M., Gustafson, S., Ekárt, A. (eds.) EuroGP 2006. LNCS, vol. 3905, Springer, Heidelberg (2006)
10. LaRoche, P., Zincir-Heywood, A.N.: 802.11 Network Intrusion Detection using Genetic Programming. In: GECCO, Workshop Program (2005)
11. LaRoche, P., Zincir-Heywood, A.N.: Genetic Programming Based WiFi Data Link Layer Attack Detection. In: IEEE 4th Annual Communication Networks and Services Research Conference (2006)

12. Ethreal: www.ethereal.com/
13. SMAC: www.klcconsulting.net/smac/
14. Snort- the de facto standard for Intrusion detection/prevention: www.snort.org
15. Fawcett, T.: ROC Graphs Notes and Practical Considerations for Researchers, HP Laboratories (March 16, 2004)
16. He, C., Mitchel, J.C: Security Analysis and Improvements for IEEE 802.11i, Network and Distributed System. In: Security Symposium Conference Proceedings (2005)
17. Arbaugh, W.A., Shankar, N., Wang, J.: Your 802.11 Network has no Clothes. In: Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, pp. 131–144. IEEE Computer Society Press, Los Alamitos (2001)
18. Bellardo, J., Savage, S.: 802.11 Denial-of-Service attacks: real vulnerabilities and practical solutions. In: Proceedings of the USENIX Security Symposium, pp. 15–28 (2003)
19. Lee, Y.-S., Chien, H.-T., Tsai, W.-N.: Using Random Bit Auhentication to Defend IEEE 802.11 DoS Attacks. ICS, Taiwan (2006)
20. Wedde, H.F., Timm, C., Farooq, M.: Beehiveais: A simple, efficient, scalable and secure routing framework inspired by artificial immune systems. In: PPSN, pp. 623–632 (2006)
21. Mazhar, N., Farooq, M.: BeeAIS: Artificial Immune System Security for Nature Inspired, MANET Routing Protocol, BeeAdHoc. In: ICARIS-2007, Brazil (in Press)
22. Shafiq, M.Z., Kiani, M., Hashmi, B., Farooq, M.: Extended Thymus Action for Reducing False-Positives in AIS based Network Intrusion Detection Systems. In: GECCO-2007, London (in Press)
23. Shafiq, M.Z., Kiani, M., Hashmi, B., Farooq, M.: Extended Thymus Action for Improving the response of AIS based NID against Malicious Traffic. In: CEC-2007, Singapore (in Press)