A Performance Comparison of User and Access Point based Artificial Immune Systems for intrusion detection on a Wireless Local Area Network

Erhan AKBAL[†] and Burhan ERGEN[††]

[†]Dept of Informatics, University of Firat, Elazig, Turkey,
[††]Dept of Computer Engineering, Faculty of Engineering, University of Firat, Elazig Turkey

Summary
Rapidly increasing wireless network systems and growing up of the mobile applications is raised threatening component for the security. The firewalls, virus software and protecting software is not capable to protect the network for a long time, because the use and misbehavior is continuously increasing and the network operates may be late to take precautions. This study aims to detect and protect the networks by using an Artificial Immune System (AIS) while removing the insufficient other protective approaches. The presented approach is not always requiring an operator interfere while keeping the high performance of the Wireless Local Area Network (WLAN) and network equipment. In presented study, the access point based AIS is realized on the contrary to classical methods detecting the intrusion on all node. It is observed the proposed method exhibit the higher performance than classical method.
Key words:
Artificial Immune System, Intrusion Detection, Wireless Network Security

1. Introduction

Widely usage of computer network has been yields the developing and widely usage of WLAN. In WLAN, it is supported two-way wide band communication using wireless electromagnetic waves, infrared, and bluetooth instead of fiber optic or copper cable in a bounded area like a building or a campus.

The security is an important problem in WLAN because there is not connection point. In this paper, it is presented an investigation and implementation of AIS on a wireless system, which is recently take place in many area and applications. Natural immune system (NIS) in human body is very complex and it is still a research subject [1], [3].

Traditional accepted opinion is that the priority duty of the immune system is to distinguish the self and non-self behaviors. There is plenty of study in literature to determine this situation. In same manner, there are divergences about the danger sensors. The NIS can not guarantee the complete solutions.[4] When the operation of intrusion detection is realized, two things should be considered. One of them is to obtain fast and reliable result, and the other is performance of computer and network should not be decreased.
In this paper, it is presented how the AIS can be realized in WLAN, the match procedure of the immune system between the natural one and artificial one, and the results of an application.

2. The Structure of an AIS in WLAN

The connection count in WLAN is not determined and limited on contrary to wired network. This situation causes the security more important subject. A security system should protect the network from the intrusion of usage without permission or an authorization. The ASI applied on WLAN must be protecting the network and computer in the network against the outer intrusion like how the NIS protects the human body from pathogens. In addition, the proposed AIS as a computer security system should protect the network from the inner attacks, the software problems and other inner faults in a tolerance, without a considerable performance loss [5].

2.1. The Structure of WLAN based Negative Selection Algorithm

The structure of WLAN based negative selections; First of all, a set of models to be protected is verified and then called the 'self-set' **(P)**. This set covers the normal states of the wireless network. Normal states include information such as the bandwidth of network and the ports used. Based on the algorithm of negative selection, a set of receptors (detectors) **(M)** responsible for

Manuscript received May 5, 2007
Manuscript revised May 20, 2007

recognizing the elements that do not belong to the set of "self-set" is formed [7]. The working method regarding the negative selection algorithm is shown in Figure 1.

2.2. Described Normal Behavior in WLAN

A computer network in a communication each other is as an environment for communicating computers in a WLAN is used as an application environment for the IS. It is established WLAN in respect to necessary TCP/IP standard to create an area network.

TCP/IP protocol is contains many protocols for computers to send receive data over internet. It is extracted the data structure using the characteristic features of TCP/IP connections. In order to gets the comparable structure with normal behavior in the WLAN. There are the destination address, the source address, the port numbers and the communication flag information in this structure that they are required for TCP/IP communication.

The binary strings are used to be able to match the data structure constituting at the beginning in order to start the detection process. All normal behaviors arising in WLAN are formed as known self-set and others are formed as a known non-self set [6]. In wired network, the data packets cannot reaches all users. However the access point emitting a radio wave transmits the data packets to the all users in the WLAN, the computer out of the network in the area can reach the this data packets.

This situation is cause a dangerous environment in respect to network security. In the presented in study, it is raised the success of the detection and the performance of network, controlling the all conditions over the access point.

3. The matching of Human Immune System and the detection System

In order to match the problem of WLAN anomaly intrusions to an AIS domain we must define how each element of the problem domain matches to the AIS domain. The elements of used the natural immune system such as self-cells, non-self cells, antigen and antibody, negative selections used in our detection system are match to follows. The following mapping follows the convention described in [8].

Human Body: The Whole of WLAN

Self Cells: Non-suspect computer behavior

Non-Self Cells: Suspect computer behavior

Antigen: The represent the observed abnormal events

Antibodies: Antibodies are created randomly and trained since the format matches that of antigens.

Negative Selection: A "negative selection" mechanism eliminates detectors that match all cells presenting a protected environment (bone marrow and the thymus) where only self cells are assumed to be present. Non-eliminated detectors become "naive" detectors; they die after sometime, unless they match something (assumed to be a pathogen), in which case they become memory cells [8].

Clonal Selection: Clonal selection represents the process of creating new antibodies. Poorly performing antibodies are replaced with mutated versions of high affinity antibodies.

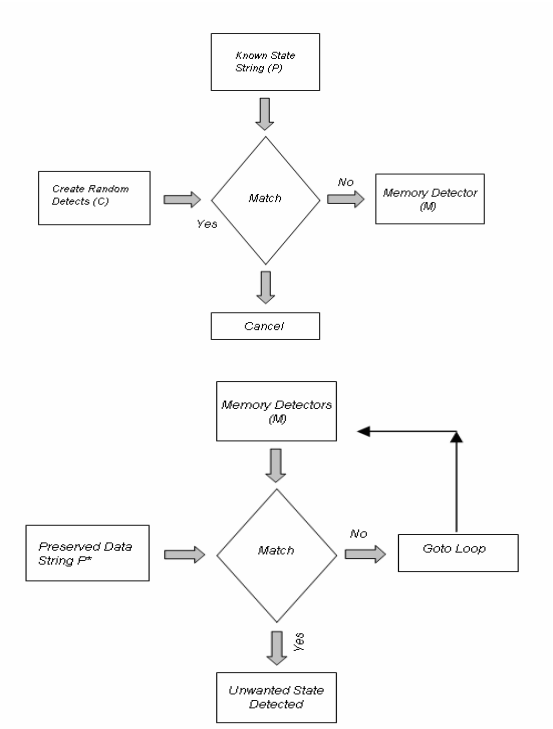


Fig. 1. a) The process of creating Detector set, b) Tracing the presence of non- self substances[6].

3.1 Matching and Compare Process

Data sets are then transformed as follows. First, protocol events are mapped to a finite set of primitives, identified with labels. In the applications, we use the following list in [8]:

A=RREQ sent
B=RREP sent
C=RERR sent
D=DATA sent and IP source address is not of monitored node

E=RREQ received
F= RREP received
G=RERR received
H=DATA received and IP destination address is not of the monitored node

A data set is then represented as a sequence of labels from the alphabet defined above, for example

I_1 = (EAFBHHEDEBHDHDHHDHD….)

Second, a number of "genes" are defined. A gene is an atomic pattern used for matching. We use the following list in [8]

Gen1=#E
Gen2=#(E*(A veya B))
Gen3=#H
Gen4=#(H*D)

I_1 can be mapped to the antigen l_2

I_2 = (3 2 7 6)

I_3 is the final representation of a single antigen. Antibodies have the same representation except that they can have multiple ones in each gene string. We consider an antigen to match an antibody if the antibody has a one is every position that an antigen has a one.

I_3=(0000001000 0000000100 0010000000 0001000000)

For example the antibody:
a_1 = (1100001001 1000010110 0011001000 1001000100) would match antigen I3 because it has a one in every position that I3 does [12].

4. Application Results

4.1. Identification of Application Environment

The realized system consists various differences even if it may be similar the system realized before other studies. The wireless network applied on our application includes 30 active computer connections to the network at the same time in a area wire 500 m2. It is not used on of the any security program addition to our AIS.

The radio waves emitted from the access point can reach a hundred meter distance. The program of AIS is run on a Linux operating system. After the packet traffic is controlled using TCPDump program in Linux operating system, the obtained data is expressed as bits. It is used the flag bits referring the destination address, the source address, the destination port, the source port and the type of packet for the immune system to determine the network behavior. These data carried out by TCPDump program from the packet received in every 0.1-2 second time intervals. We defined so self-behavior for our WLAN. The constitute network may be presented as a schema in figure 2.

That the AIS were run on the access point has provided to control the whole network and has prevented to loss of the computer performance in the network due to intrusion detection for security. In this method, the security program is executed on access point, which it is to provide that exit to internet of all computers in the network.

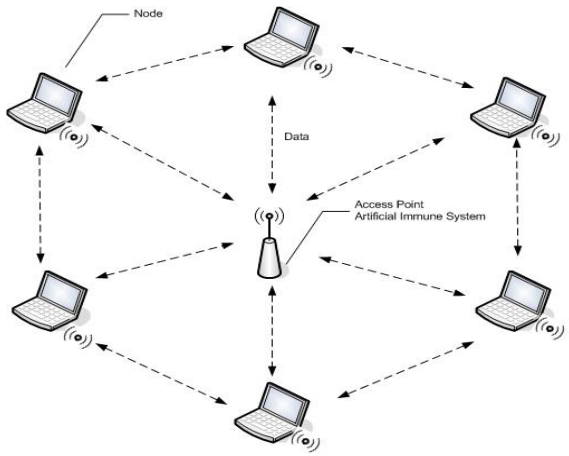


Fig. 2. Application Environment

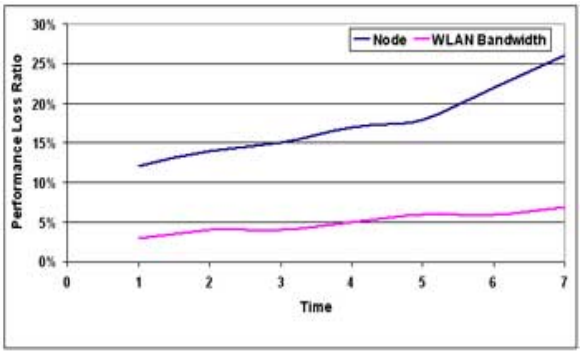
4.2. Application Results

The applications of AIS are putted in practice in two ways which user based and access point based. It is measured the network performance and computer performance in both practices. The performances of the network and the all user computer included from the network are measured for a week.

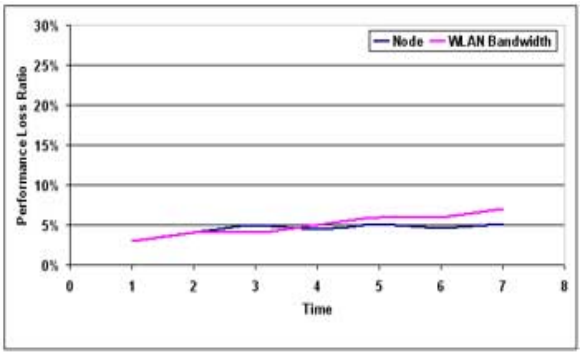
In order to measure the performance in the computer, it is observed the criteria of processor, ram and network performance over the operating system on each computer in the network. We obtained results is graphically given in Fig 3. Fig 3(a) and Fig 3(b) present the busy rates of the user based and access point based immune system for the user computer and the network, respectively.

As seen in figures, The performance loss for the user based AIS is higher than the loss for the access point based AIS, because the application of the AIS keep busy each computer in the network for the user based approach.

This performance loss is especially encountered in the computer having lower hardware configurations.



(a)



(b)

Fig. 3. a) The performance loss of User Based AIS
b) The performance loss of Access Point Based AIS

When the access point based approach is used, it is observed that the computers have better performance and the network performance is nearly same the uses based approach.

5. Conclusion

This paper presents a study on the application of the AIS on WLAN. In this study, it is proposed the access point based approach instead of the user computer based in the literature [9-11, 13]. The busy times of the computer and the network are measured to compare two approaches each other. Beside the intrusion detection is two points important. The performance of the computers and the network is another assessment criterion.

It is observed that the application type of AIS effects on the performance of the network and the computer in the WLAN. The results show that the user based AIS causes the loss performance on the computers. Where as the access point based AIS doesn't decrease the performance of the user computer noteworthy.

Because of the packet traffic is not increase. The performance losses of the WLAN are nearly some for the two approaches, the user based and the access point based AIS. In both methods, the packets on the network reaches the both the computers and the access point. For this reason, the access point based approach presents more the performance in AIS applications.

Acknowledgement

The project is supported by Firat University Scientific Research Projects (FUBAP) department (1167).

References

[1] S. Buchegger and J.-Y. Le Boudec. A Robust Reputation *System for Mobile ad hoc Networks Technical Report*, EPFL-DI-ICA, Lausanne, Switzerland, July 2003.

[2] S.Buchegger and J.,Y. Le Boudec, "Performance Analysis of the CONFIDANT protocol: Cooperation of nodes - Fairness In Distributed Ad-Hoc Networks", In *of IEEE/ACM Symposium on Mobile Ad-Hoc Networking and Computing (MobiHOC)*, Lausanne, CH, June 2002.

[3] S. Buchegger and J.-Y. Le Boudec, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks", In *Proceedings of WiOpt `03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks.*, Sophia-Antipolis, France, March 2003.

[4] F.S., H. S. A. "Immunology as Information Processing. Design Principles for Immune System & Other Distributed Autonomous Systems", L.A. Segel and I. R. Cohen, eds. *Oxford Univ. Pres*. 2000

[5] Kachirski, O., and Guha, R. "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks", *Proceedings of the 36th Hawaii International Conference on System Sciences*, 2003.

[6] Zhang, Y., Lee, W., and Huang, Y., "Intrusion Detection Techniques for Mobile Wireless Networks", *Wireless Networks Vol 9*, 2003, pp 545-556.

[7] De Castro, L.N. and Von Zuben F.J., "The Clonal Selection Algorithm with Engineering Applications", *GECCO 2000*, Las Vegas, Nevada, USA, 2000.

[8] S. Sarafijanovic and J.Y. Le Boudec. "An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile Ad-Hoc Networks" TechReport IC/2003/65, EPFL-DI-ICA, Lausanne, Switzerland, November 2003.

[9] Kenneth S. Edge, Gary B. Lamont, and Richard A. Raines, "Multi-objective Mobile Network Anomaly Intrusion", Air *Force Institute of Technology, Dayton, OH, USA*, 2006

[10] S. Buchegger, Cedric Tissieres, J. Y. Le Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks", *How Much Can Watchdogs Really Do? Technical report*, No. IC/2003/72, November 2003.

[11] J. Y. Le Boudec and S. Sarafijanovic, "An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-Hoc Networks" *Proceedings of Bio-ADIT 2004*, Lausanne, Switzerland, January 2004

[12] Sarafijanovic, S. and Boudec, J., "An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors". *International Journal of Unconventional Computing*, Vol 1, Feb 2005, pp. 221-254.

[13] Patwardhan, A. Parker, J., Joshi,A., Karygiannis, A., and Iorga,M. "Secure Routing and Intrusion Detection in Ad Hoc Networks", *Third IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, Hawaii, 2005.