

A Hybrid Approach for IEEE 802.11 Intrusion Detection

Based on AIS, MAS and Naïve Bayes

Moises Danziger

Department of Computing and Systems
Polytechnic School of Pernambuco
Recife, Brazil
md@dsc.upe.br

Fernando Buarque de Lima Neto

Department of Computing and Systems
Polytechnic School of Pernambuco
Recife, Brazil
fbln@dsc.upe.br

Abstract—Many problems with wireless networks are directly related to the very means used to transport data, in this case, radio waves. In addition to mis-configured equipment lack of adaptable algorithms and wireless networks are major targets for attacks. New tools to refrain that are greatly in need. Due to the fact that it is easy to attack and not so to defend wireless networks, good candidate tools would be the ones that could profit from intelligent techniques. In this paper, we use the Danger Theory (DT) and a Bayesian classifier (using naïve Bayes) embedded in a military style multi-agent system (MAS) to create a lightweight, adaptable and dynamic detection system for wireless networks (WIDS). Experimental results show that the artificial immune aspect of the proposed system is capable of detecting unknown intrusion and to identify them automatically with considerable few false alarms and low cost for the network traffic.

Keywords—component; AIS; Intrusion Detection; Danger Theory; MAS; Naïve Bayes

I. INTRODUCTION

The human immune system (HIS) has been the inspiration for many works, but on security it is possible find a lot more of candidate problems because of the blatant functional similarities. The new approach of artificial immune systems (AIS) may quickly become the new weapon among computational intelligence techniques that could easily be deployed for network security [1, 2]. Shortly after its initial use, the negative selection base of AIS proved not to be scalable and not the first choice for IDS applied in real time [2]. However, with the advent of danger theory (DT), the pitfalls of prior AIS algorithms are dramatically reduced. For instance, the self-non-self (i.e. negative selection) method has been replaced by the signaling processes of DT [3].

Looking at intrusion problems, Aickelin et al. [4] devised the analogy between IDS and DT. Following this new approach, some authors had presented works on that with good results [5, 6]. Thus, in our work, DT is used as primary line of detection method embedded in the intelligent agent.

Intelligent agents are the key component of multi-agent systems (MAS) that present many suitable characteristics to be used in association with DT [7]. The basic principle of an agent is its perception and interaction with the environment.

The IDS uses sensors to detect anomalies, therefore, agents can be used as sensors for other parts of a comprehensive IDS. In this work, six types of agents are devised, each one with different abilities to be performed towards the high goal of intrusion detection.

The model put forward here was developed based on the IEEE 802.11 networks standard operation and this choice was a reflection of the current abundance of problems found. To prove the efficacy of our approach, the experiments were carried out for three types of known attacks on wireless networks, namely: (i) Hirte [8], (ii) Cafe Latte [9] and (iii) ChoChop [10]. Our main objective is to test the detection, identification and agents operation under anomalous events when the system is running in automatic mode.

We divided this paper as follow: section two briefly presents MAS and IDS. In section three we detail the extended version of the proposed model. The methodology and results of experiments can be found in sections four and five, respectively. Results are included in section six.

II. MULTI-AGENT SYSTEM AND IDS UNDER IEEE 802.11 NETWORKS VISION

A. Multi-agent System

Multi-agent systems can be defined as a collection of computational entities that have the ability to solve problems in cooperative or individual manner through the exchange of information [12]. Looking at IDS, the MAS can be represented by set of sensory agents or combatant agents [7]. In this work, we developed specialized agents, using the DT concepts and naïve Bayes, solely for distributed aspects of intrusion detection.

B. IDS and IEEE 802.11 Standard

Actually, the automation and the discovery of new attacks is the focus of most researches on IDS [18]. These IDS problems are viewed on WIDS and are tested as another objective for this work.

Moreover, the IEEE 802.11 network has grown considerably and their security problems follow suit. Many attacks happen with certain facility [16]. This attacks can be classified into passive or active. For this paper we decided use only active attacks.

III. EXTENDED MODEL OF WIRELESS IDS BASED ON DT, NAÏVE BAYES AND MAS – MILITARY STYLE

The extended model of [11] presented here detects anomalies using immuno-based agents within a hierarchical structure of functionalities spread across workstations and servers. Six types of agents inspired in the military hierarchy were devised, namely: (i) basic agent, (ii) subaltern agent, (iii) intermediary agent, (iv) superior agent, (v) logger agents and (vi) messenger agents. In analogy with HIS, hence, (i) belong to the innate system, (ii) can belong to the innate system or adaptive system (i.e. when mapped as Natural Killer cell or T-cell, respectively), (iii) and (iv) belong to the adaptive system. The agents (v) and (vi) are auxiliary agents - signalers.

A. Basic Agent

Its main function is to detect problems through the processing of several signs based on DT-concepts applied under IEEE 802.11 network adapted DCA algorithm [13]. The detection process is made possible by a frame analyzer that preprocesses the data collected to DCA entrance. There is only one agent of this type per node and it can work on or off-line.

B. Subaltern Agent

This agent can represent the T-cell or NK-cell of HIS and can be understood as memory agent too (e.g. this increases the performance if find the intruder again). For each subtype of IEEE 802.11 frame, one subaltern agent may be created. For executing correctly its devised function, the internal structure of subaltern agents is formed by an array with the attack known variation alongside the routines of combating the attack.

C. Intermediary Agent

Created to identify the unknown problems. For this difficult task, it uses a data base with known frames that suffer attacks and the simple and fast naïve Bayes technique embedded.

This technique uses statistics looking for compatibles candidates [14, 15]. The performance of naïve Bayes in dynamic learning is a problem, even so we decided to use because of its expediency that can help in the system automation. For IDS, the process of anomaly identification should not be an extra difficulty to the system.

When a new type of attacks is identified, a new subaltern agent is automatically created with an internal structure that will allow the identification of that attack on the stations rapidly. For a simple variation for a known attack is detected, the new information is added into an existing subaltern agent for that attack.

There is one intermediary agent per server and it is necessary exchange of the base between the servers.

D. Superior Agent

According to proposed model, all processing can be done automatically, so the function of superior agent is very

important to suppress the possible auto-destruction event. This is analogous to what happen in HIS, where auto-destructive processes named auto-immune (i.e. the body combating itself) are controlled by a mechanism that control the T-cells population.

This mobile agent has a structure that permits to read the log files. Each superior agent is guided by a round-robin routine and all superior agents (more than one could be created as well) visit each station in a cyclic manner.

This agent use a simple data mine process to find information that can represent fail in the system. It is the unique contact with administrator by messages of system state.

E. Logger Agent and Messenger Agent

The logger was created to register all activities executed by the system in an orderly and rational manner. All stations have an agent of this type, as well as the server. For simplification, a text log file is generated in which all records can be read by the superior agent.

The messenger agent was created for controlling communication between agents. Each station and the server has a messenger agent. This agent reduces the work of others agents, by managing communications more efficiently avoiding the collapse in network traffic.

IV. METHODOLOGY

A. Attack Scenarios

To test our architecture, we devised a network environment containing five workstations and one server, setting up a client-server environment and one AP is used with an antenna of 2.2 dBm (power).

We have conducted three experiments using Aircrack-ng [16] as tool of attack. We developed the system with JAVA using the framework JADE [17] for agents. Because of space, results of only one station were selected for sampling the results of each experiment. The experiments were divided by type of attack.

B. Signals and Antigens

Following the same mapped antigens and signals as in [11], each frame is transformed into an antigen keeping the same structure model standardized by IEEE 802.11 and the signals are reference of antigens. Three signals formed the basic input entry, namely: safe signal (SS), danger signal (DS) and Pathogen Associated Molecular Patterns (PAMP) (e.g. in other words, a clear attack). For this work, twelve signals were used, three different signals for each type of attack. All signals were chosen after tedious observation of frame IEEE802.11 traffic. The signals are as follows:

- Hirte: SS represent the number of frame with the same sequence number (SN) per second and PAMP is the number of data frame received with 36 bytes. Its DS is the number of frames received per second.
- Cafe-Latte: SS is the number of frame received with size between 69 and 129 bytes. For PAMP, the value is the number of frames received of unknown source

of network. In the case of DS, it is the number of frames received per second;

- **ChopChop:** SS is the value of repeated small frames per second and PAMP is the number of frame with different destination received per second. It DS is the number of frames send per second

After the signals processing of DCA, the DC can have the state changed for semi-mature or mature. In the first case, represents that DC collected more SS. In the second case, the DC collected more DS and PAMP signals. So, the mature state represents attack moments.

V. RESULTS AND ANALYSIS

The results of the experiments are shown in the figures below (1, 3, 5). In all of them, we present the output signals of the detection process using DCA. Semi-mature and mature signals are indicated, referring to attack detection upon the regular traffic. The figures 2, 4, and 6, show the antigen classification by intermediary agent and the naïve Bayes. This happens when the basic agent detects anomaly and there is no subaltern agent to resolve the problem. Then, it requests help to the server. In these figures, in the left vertical axis, 0 represents false (not anomalous) and 1, represents true (anomalous). The right vertical axis shows the frame type of antigen when classified as anomalous. In this case, one specific subaltern agent (i.e. based on frame type) is created. These numbers used refer to codification of frame type of the IEEE 802.11 standard..

The Table 1 presents other relevant experimental results for all simulations carried out.

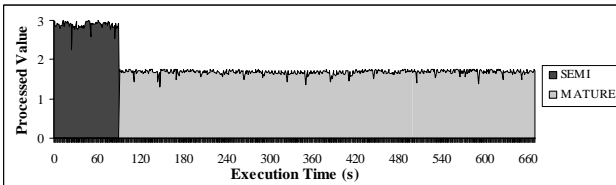


Figure 1. Exp. 1 – Signals processed for Hirte attack

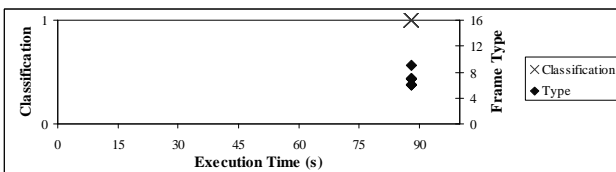


Figure 2. Exp 1 – Classification for Hirte attack

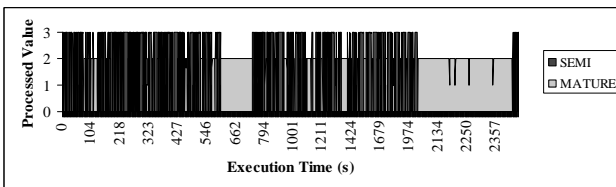


Figure 3. Exp. 3 – Signals processed for Café-Latte attack

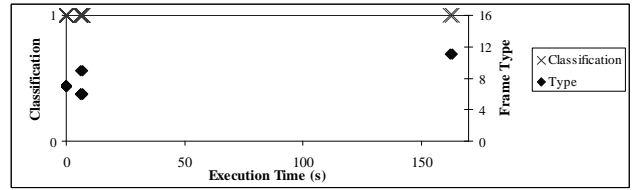


Figure 4. Exp. 3 – Frames classification for Cafe-Latte attack

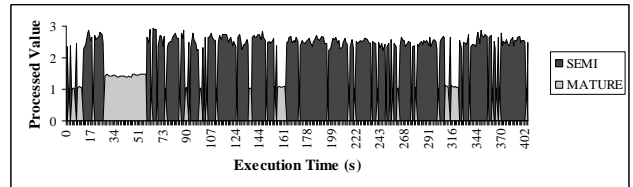


Figure 5. Exp. 4 – Signals processed for ChopChop attack

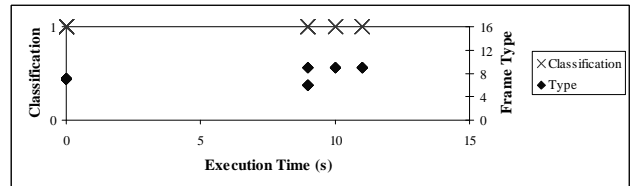


Figure 6. Exp. 4 – Frames classification for ChopChop attack

According to all figures, the algorithm of detection was effective to detect most of the problems (i.e. all types of attacks tested). In the Table 1, for Hirte (Exp. 1), we obtained zero as false negatives. The error rate is calculated using the simple multiplication of seconds that have been detected attack by 100. The result is divided by the total number of seconds that have suffered attacks,

For these attacks, in the classification were found false positive alarm with the creation of subalterns' agents, without actual necessity. This is not a major limitation, as it implied only in some small loss of resources. Some antigens found alone within a second may not be an attack, but, if in the last or in the next second the same antigen is present, then odds of an attack are high. Unfortunately, one antigen in one second may not be attack for the classifier.

During the experiments, we observed that some antigens are classified as attack even when not expected. But, after observation, the classification was correct. The better conclusion is, the behaviors of some antigens can generate interferences of attack and, so, the system can detect other problematic antigens. So, even without processing all types of possible attacks, the system has demonstrated its ability to identify them. This fact shows very clearly that the system can discovered problems even when they pass through the detector and we do not define them as false alarm.

The method of naïve Bayes validation used is the “leave-one-out” and the value of efficiency for classifier was in 83.9%. The experiments combined showed that the value was good enough to generate no false negative alarm.

The response time for the intermediary agent vary. This happen because, for example, the distance between station and the AP. This is the cause of delay on intermediary

response. Because of this problem, in the following seconds, the same problem will can generate other message for intermediary agent, as shown in Fig. 2, 4 and 6.

Even with the delay, a small amount of messages exchanged between the workstation and the server, shown in Table 1 represents the analogy between the system innate and adaptive system of the HIS. When a station has a problem and must seek the help of intermediary agents (in the server), a new subaltern agent is created or updated, from any existing one. All stations receive the same agent created (i.e. the agent is cloned) and, if there are new instances of the same attack, it is not necessary help of the intermediary. In this case the reaction time is very fast (less than 1 second in tests). This process also decreases the amount of messages exchanged between the stations and the server, reducing the impact on the network traffic and helping the automation process.

The number of frames passed by network is calculated multiplying the value found by the average size for messages. The result is divided by 1500 (i.e. represent the maximum value of frame).

During the experiments, one problem happened with the network (e.g. shutdown), as can be seen in the last rows of table 1. In this case, the superior agent detected the problem and signaled for administrator of system. It send a clone to try to resolve the problem to avoid die-itself.

TABLE I. RESULTS FOR ALL MODEL EXECUTION

Description	Exp 1	Exp 2	Exp 3
Frames Collected	54063	142876	56978
Seconds in attack	426	823	314
Antigens	42682	66000	8991
Migration Threshold	0-2	0-2	0-2
DC Population	517	2373	402
Mature Cells	440	861	317
Semi-Mature Cells	76	623	5
False Positive Detection	14	38	4
FN Detection	0	5	3
Error Rate	3,28%	5,21%	2,17%
Subaltern agents created	3	3	3
False Positive classification	1	0	0
False Negative classification	0	0	0
messages sent to intermediary	3	2	4
Frames generated	~200	~133	~266
Time of response	~2s	~3s	~2s
Messages of superior agents	0	0	1

VI. CONCLUSIONS

The use of MAS and AIS-DT as put forward in this paper produced interesting results. The highlights of such combination are: (i) low number of false alarms, especially false negatives, (ii) ability to detect events not known to the system, (iii) simplicity of implementation of automated agents (i.e. without human interference), (iv) low cost of extra traffic upon the network and (v) low response time to anomalous event, mainly, candidate of threats. As for the question of scalability it is not a problem anymore since the proposed system capitalized on DT improvements to the initial AIS.

The good adaptation for the lower layers, of IEEE 802.11, is another important result. Actually, there are few IDS that consider these layers.

REFERENCES

- [1] J. Greensmith and U. Aickelin, "Dendritic cells for SYN scan detection", *Proceedings of the IEEE Genetic and Evolutionary Computation Conference (GECCO-07)*, London.UK. 2007, pp. 49-56.
- [2] J. Greensmith, J. Twicross, and U.Aickelin, "Dentritic cells for anomaly detection", In *IEEE Congress on Evolutionary Computation*, Vancouver, BC, Canada, July 16-21, 2006, pp. 664-671.
- [3] P. Matzinger, "The Danger Model: a renewed sense of self", *Science*, 296 (12 April 2002) 2002, pp. 301-305.
- [4] U.Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod, "Danger Theory: The link between AIS and IDS", In *Proceedings of the Second International Conference on Artificial Immune Systems (ICARIS-03)*, Edinburgh, UK., September 1-3, 2005, pp. 147-155.
- [5] J. Greensmith, U. Aickelin, and G. Tedesco, "Information fusion for anomaly detection with the dendritics cell algorithm", Accepted for the Special Issue on Biologically Inspired Information Fusion, to be appear in *International Journal of Information Fusion*, Elsevier, 2007.
- [6] J. Greensmith and U. Aickelin, and S. Cayzer. "Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection.", In *Proceedings of the Second International Conference on Artificial Immune Systems (ICARIS-05)*, LNCS 4163, 2006, pp. 404-417.
- [7] H. Fu, X. Yuan, K. and N. Wang, "Multi-agents artificial immune system (MAAIS) inspired by danger theory for anomaly detection", In *IEEE International Conference on Computational Intelligence and Security Workshops*, Harbin, Heilongjia, China, December 15-19, 2007, pp. 570-573.
- [8] Aircrack-ng - Hirte Attack. At. <http://www.aircrack-ng.org/doku.php?id=hirte>, (Accessed in January of 2010).
- [9] V.Ramachandran, Md S. Ahmad. "Cafe Latte with a Free Topping of Cracked WEP: Retrieving WEP Keys From Road-Warriors", In 9th Toorcon Hacker's Conference. October 19th-21st, 2007.
- [10] Korek. Chopchop Theory. At. <http://www.aircrack-ng.org/doku.php?id=chopchoptheory>, (Accessed in January of 2010).
- [11] M. Danziger, M. Lacerda, F. B. de Lima Neto, "Danger Theory and Multi-agents Applied for Addressing the Deny of Service Detection Problem in IEEE 802.11 Networks," ISDA, 2009 Ninth International Conference on Intelligent Systems Design and Applications, 2009, pp.695-702.
- [12] S. Russel and P. Norvig, *Artificial Intelligence: a modern approach*, Prentice Hall, 1995.
- [13] J. Greensmith, "The Dendritic Cell Algorithm", *PhD Thesis*, University Of Nottingham, 2007.
- [14] I. Rish, "An empirical study of the naive Bayes classifier", IJCAI 2001 In Workshop on Empirical Methods in Artificial Intelligence. At <http://www.cc.gatech.edu/~isbell/classes/reading/papers/Rish.pdf>. (Accessed in January of 2010).
- [15] Stewart, B. 2002. "Predicting project delivery rates using the Naive-Bayes classifier", *Journal of Software Maintenance* 14, 3 (May. 2002), 161-179.
- [16] Aircrack-ng -802.11 WEP and WPA-PSK keys cracking program, At <http://www.aircrack-ng.org/doku.php> (Accessed in January of 2010).
- [17] JADE - Java Agent Development Framework, At <http://jade.tilab.com/> (Accessed in January of 2010).
- [18] S. Northcutt and J. Novak. "Network Intrusion Detection." Third Edition, New Riders Publishing, USA, 456 p. 2003.
- [19] N. R. Jennings and A. Wooldridgem. "Intelligent Agents: theory and practice." *The Knowledge Engineering Review*, vol 10, n.2. p. 115-152, 1995.