International Journal of Computer Networking,
Wireless and Mobile Communications (IJCNWMC)
ISSN 2250-1568
Vol. 3, Issue 1, Mar 2013, 95-102

AIS MODEL FOR BOTNET DETECTION IN MANET USING FUZZY FUNCTION

I.M.HANAFY[1], A.A.SALAMA[1], M. ABDELFATTAH[2] & Y. M. WAZERY[2]

[1]Math and Computer Science Department, Faculty of Science, Port Said University, Egypt

[2]Information System Department, Faculty of Computers & Information, Benha University, Egypt

ABSTRACT

Mobile adhoc networks (MANETs) poses a large area of challenges in the field of security, this is due to the lake of infrastructure and the continuous changing in the network topology. Botnets are believed to be the most harmful danger that threatens any type of networks; because it controls the units in a non noticeable manner so detection of botnets is more difficult . in this paper the Artificial Immune System (AIS) is used as the defense system to the MANET to face botnets. Experimental results show that the use of fuzzy based security can enhance the security of AIS in MANETs.

KEYWORDS: MANET, Security, Wireless, AIS, Communication, Fuzzy, HMM, NNs, FDM

INTRODUCTION

Ad hoc networks are widely used in military and other scientific areas. With nodes which can move arbitrarily and connect to any nodes at will [1], it is impossible for Ad hoc network to own a fixed infrastructure. It also has a certain number of characteristics which make the security difficult.

Mobile Ad hoc Networks are self-organized, temporal networks which consist of a set of wireless nodes. The nodes can move in an arbitrary manner and work as its own opinions. They may join or leave the network with no restrictions. Therefore, Ad hoc networks' topologies are dynamic and costly to maintain. Furthermore, wireless channels make the routing and message transmission much more challenging [2]. Nodes of these networks can function as routers that discover and maintain routes to other nodes as well as end-users. They will rely other nodes to relay the messages, which are exposed in an open dangerous situation for any intermediate node to be capable of destroying the integrity or choose as their like to deal with the messages. Last but not least, nodes in ad hoc networks have only limited resource, i.e. Battery power, bandwidth and cpu power. They are usually embedded systems which are produced for certain fixed tasks [3].

PRELIMINARIES

Security in MANETs

Providing adequate security measures for ad hoc networks is a challenging task. In a security concept, typically striving for goals like repudiation and availability and authentication of communicating entities is of particular importance as it forms the basis for achieving the other security goals: e.g., encryption is worthless if the communication partners have not verified their identities before. There are five main security services for MANETs[4]:

- Data confidentiality: keep data secret (usually accomplished by encryption)
- Data integrity: prevent data from being altered (usually accomplished by encryption)
- Data freshness: assuring that data is recent

  - Weak freshness: provides partial ordering of messages
  - Strong freshness: provides total ordering and allows for delay estimation
- Data availability: data should be available on request
- Data authentication: verification that the data or request came from a specific, valid sender

Security never comes for free[5]. When more security features are introduced into the network, in parallel with the enhanced security strength is the ever-increasing computation, communication, and management overhead. Consequently, network performance, in terms of scalability, service availability, robustness, and so on of the security solutions, becomes an important concern in a resource-constrained ad hoc network[1]. While many contemporary proposals focus on the security strength of their solutions from the cryptographic standpoint, they leave the network performance aspect largely unaddressed. In fact, both dimensions of security strength and network performance are equally important, and achieving a good trade-off between two extremes is one fundamental challenge in security design for MANETs[3].

Botnets

A botnet is a collection of compromised Internet hosts (a.k.a. bots), that have been installed with remote control software developed by malicious users. Such software usually starts automatically when a parasite host boots. Each computer is infected with a malicious program called a bot, which actively communicates with other bots in the botnet or with several bot controllers to receive commands from the botnet owner [7]. Botnets usually recruit new vulnerable computers using infection methods from several classes of malware, including self-replicating worms, email viruses, etc. They provide their owners with efficient one-to-many command and control mechanisms, which can be used to order an army of controlled computers (bots) to conduct Distributed Denial-of-Service attacks, email spamming, etc. Botnets have become the most serious threat to Internet security As a result, malicious users (a.k.a. bot masters), can coordinate large-scale Internet activities by controlling the bots (the victims). Bot masters always attempt to compromise as many hosts as possible. Botnets allow bot masters to engage in various malicious activities, such as launching distributed denial of service (DDoS) attacks, sending spam mails [8], hosting phishing sites , and making fraudulent clicks [9]. Statistics show that botnets yield great economic benefits for bot masters. In order for a botnet to function, the bot master and the bots must be able to communicate. The way in which this is achieved is known as the command and control structure. Early botnets distributed commands by having infected machines join a particular room on an Internet Relay Chat server [3]. The use of this chat room introduced a central point of failure, that if shut down, would completely disable the botnet. This weakness was heavily exploited by researchers, who studied botnet infections to see where the bots connected to for commands, and then had the servers shut down [10].

AIS

The human immune system protects the human body against pathogens which try to infect the body. The human immune system consists of three main components [11]:

- **Skin:** The biggest component and the first defence-line of the immune system against pathogens.
- **Innate Immune System**: Present and activated almost directly after the birth of a human. Protects the human body against most basic pathogens and removes these pathogens quickly. The innate immune system does not learn a lot, it applies the given knowledge of basic pathogens.

- **Adaptive Immune System:** The adaptive immune system protects the human body against complex, mutated and novel attacks. It reacts slowly and normally it learns from a local infection by the attacking pathogen. The adaptive immune system also immunizes the human body against known attacks; this functionality is used for vaccination.

The human immune system is a nearly perfect protection-system for the human body. Now, we will look on the artificial immune system which tries to model the human immune system for computer science – here only for network security - in order to obtain the advantages [12].

AIS constitute intelligent methodologies that can be used to churn out effective solutions to real world problems. Inspired by the natural immune system, an AIS banks on concepts derived from theoretical immunology and observed immune functions to solve a problem [13]. The body's defense mechanism can be divided into two sub-systems: (i) the innate immune system and (ii) the adaptive immune system. The former is available for immediate combat while the latter produces antibodies depending on the invading agent. The skin and the lining of the body cavities that are open to the outside world provide the initial protective barrier. A virus or bacteria (generically known as a *germ*) may invade the human body and reproduce.

The germ's presence produces some side effects [14], like fever, inflammation, etc. Some bacteria on the contrary are benign. In immune system terminology, the invading agent is called the *Antigen* while the defending agent is termed the *Antibody.*

In the artificial immune system, the components are artificial cells or agents which flow through a computer network and which process several tasks in order to identify and prevent attacks from intrusions. Therefore, the artificial cells are equipped with the same attributes as the human immune system. The artificial cells try to model the behaviour of the immune-cells of the human immune system [15].

Examples for application of artificial immune systems:

- Computer &Network Security
- Prediction, Forecasting and Optimization Problems
- Cloud and Distributed Computing

THE PROPOSED MODEL FOR BOTNET DETECTION AND PREVENTION

In this section, a Security scheme is applied to MANETs in order to discover and treat botnets. This scheme might be viewed as an immune system that protects and detects any anomaly occurred in the MANET. The detection and protection is based on applying AIS concepts over MANET as will be described later in this section. Instead of using the ordinary AIS method for taking the elimination decision a set of fuzzy rules are used, these rules are rapidly changing in correspondence to the rapidly changing nature of MANET. The rest of this section illustrates the proposed scheme as two stages process.

AIS MODEL

Structure

The security offered by this scheme is based on the efficiency and adaptability provided by the AIS. In this model nodes are viewed as follows:

- The whole set of nodes creates a universe (U) that represents all self and nonself nodes.
- Set of allies (self) nodes (A) .
- Set of enemies (nonself) nodes (E)

These sets must satisfy the following conditions

- $A \cup E = U$ Formulation 1
- $A \cap E = \varnothing$ Formulation 2

To keep generalizing the model the protein chains are modeled as binary short codes. The main purpose of the AIS is to classify a gives set of unknown code into either A or E, to give the decision either to allow or prevent the under classification node.

Sensors

For simplifying purposes we shall address only the *lymphocyte* cells only. This detector combines properties of B-cells, T-cells, and antibodies. AIS is similar to the IS in that it consists of a multitude of mobile sensors called detectors, circulating around a distributed environment.

Lymphocytes have hundreds of thousands of receptors on its surface (and, therefore, called monoclonal). The pathogen receptor regions (epitopes) are linked. Charge to the chemical composition and the same type of receptor may bind to epitopes. Binding event, the correlation between the receiver and the high likelihood of epitopes, both epitopes and receptors modeled as a binary string of fixed length L of the chain, the chemical bonds are modeled as approximate matching. In fact, each detector is a binary string, and that is, to its receptors. A lymphocyte is activated when its receptors accumulated epitopes. Changes in the state of lymphocyte activation and triggers a series of reactions can lead to the elimination of pathogens. Lymphocyte epitopes when left alone for more than a threshold number of receptors bound to be active and survive the elimination process. The chemistry between receptors and epitopes are not permanent, so active, lymphocyte receptors to bind within a short period of time.

System Training

The system training is based on the set of fuzzy rules supplied to the system and system negative selection algorithm, which is expressed in the thymus of the symbols to explore collaborative training, based on the maturation of T cells survive and leave the thymus will be tolerant of all proteins that are associated. This process is called negative selection, because the T cells those has not been activated are selected to survive. Each detector is a randomly generated bit string (similar to receptors) are created for a period of time called tolerization period and remains immature. During this time period, the environment (probably associate the enemy strings) and detector are exposed, and if it matches with any bit string then will be eliminated. If it does not match during tolerization, a mature detector (similar to a naive B cell) becomes then it is assumed to be ally.

Storage

When multiple receptors at a node are activated by the same Enemy string , they competes to become memory detectors. Those detectors that have the closest match (based on the fuzzy rules) will be selected to become memory detectors. These memory detectors regenerates more copies of themselves, which then spread out to neighboring nodes. Consequently, a representation of the string is distributed throughout the graph; future occurrences of will be detected. In

addition, memory detectors have lowered activation thresholds instead of recalling the fuzzy rules again to save time so that they will be activated far more rapidly in future to reoccurrences of previously encountered Enemy strings, i.e., they are much more sensitive to those strings.

Fuzzy Decision Model (FDM)

The proposed scheme uses Fuzzy Decision function for determining when to activate a T cell this is done by activating the FDM when a new code is noticed.

The fuzzy function is a set of rules based on the following parameters as inputs

1- Memory status (MS): a fuzzy variable that ranges from very week to strong corresponding to the passed string status

2- Number of Nodes (NN): a fuzzy variable that ranges from few to many representing the current number of nodes in the MANET.

The output fuzzy variable "the status of the T-cell" has three fuzzy sets (Pass – Steady – Activate). It should be noted that modifying the membership functions will change the sensitivity of the fuzzy logic system's output to its inputs. Also increasing the number of fuzzy sets of the variables will provide better sensitivity control but also increases computational complexity of the system. Table 1 show the rules used in the fuzzy logic system.

Table 1: Fuzzy Decision Model

Input		Output
MS	**NN**	**S**
Very Week	Few	Pass
Week	Normal	Pass
Strong	Many	Activate
Very Week	Normal	Steady
Week	Many	Pass
Strong	Few	Steady
Very Week	Many	Pass
Week	Many	Activate
Strong	Normal	Activate

EXPERIMENTAL RESULTS

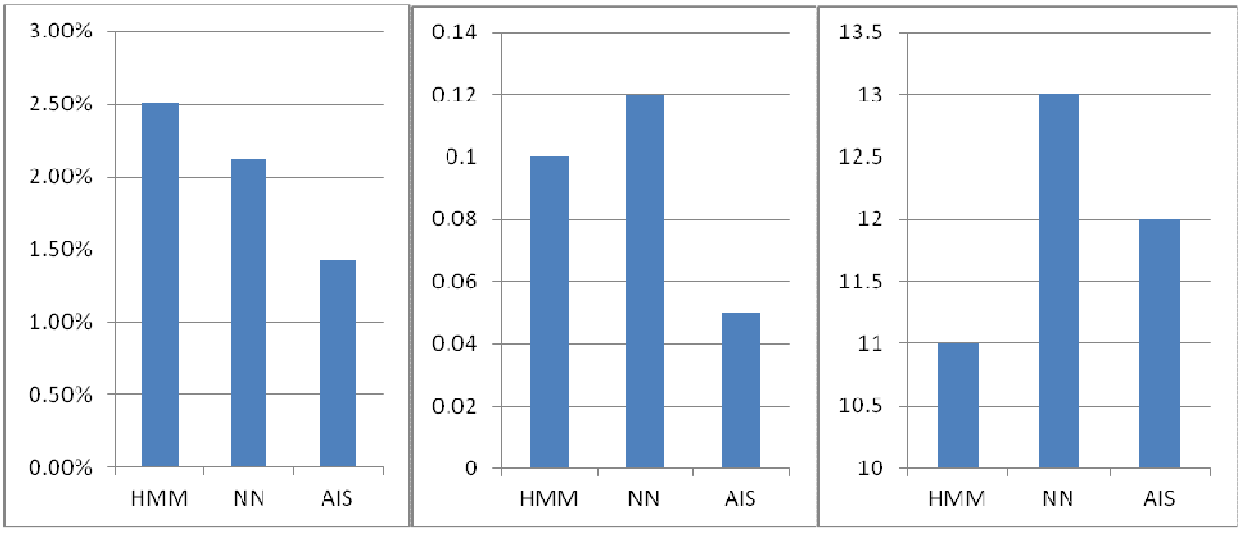
In this research a new security model for Botnet Detection in MANETs is presented, this model is based on the idea of passing a decision to the AIS based on fuzzy rules. In this section the set of experimental results for the attempts to decide the way for creating a more secured MANETs. These experiments are clarified.

AIS vs. Hidden Markov Models (HMMs) and Neural Networks (NNs)

At this point in the research the AIS is compared to two highly used techniques (HMMs) and (NNs).

Table 2: Results of Applying AIS vs NNs and HMMs

Classification System	Error Rate	Average Decision Time	Average Training Time
HMM	2.51 %	0.10 sec	11 minutes
NN	2.12 %	0.12 sec	13 minutes
AIS	1.42 %	0.05	12 minutes



(a) (b) (c)

Figure 1: Results of Applying AIS vs NNs and HMMs

(a) Error Rates **(b) Average Decision Time** **(c) Average Training Time**

As table 2 and figure 1 illustrates the superiority of the AIS over both HMMs and NNs that is AIS provides relatively less error rate and small decision time with an obvious small training time.

Fuzzy vs. Negative Selection Decision

Another important type of experiments had taken place to decide the action of the T-Cells. To assure that the proposed mechanism works better, the ordinary negative selection mechanism is compared to the proposed fuzzy function. The performance is measured with two evaluation criteria

- The Decision correctness
- The Decision time.

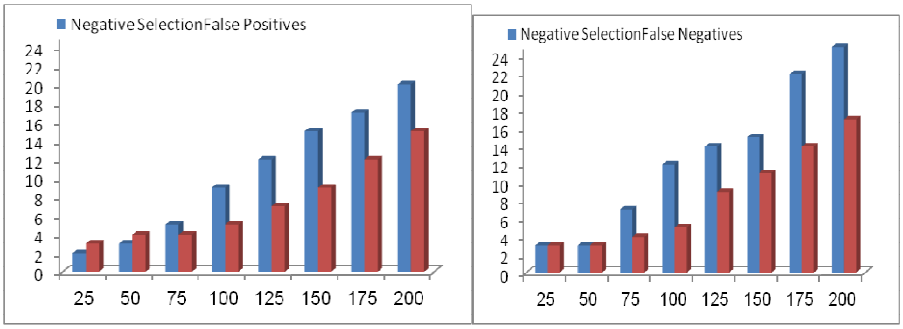
The performance criteria are demonstrated in the following sections:

The Decision Correctness

The Decision correctness is measured for both techniques. The measurement process is based on monitoring both techniques and counting the set of false positives and negatives for a set of nodes varying from 25 to 200.

Table 3: False Positive Decisions for Fuzzy vs. –ve Selection

	Negative Selection		Fuzzy Decision	
	False Positives	False Negatives	False Positives	False Negatives
25	2	3	3	3
50	3	3	4	3
75	5	7	4	4
100	9	12	5	5
125	12	14	7	9
150	15	15	9	11
175	17	22	12	14
200	20	25	15	17



(a) False Positive Decisions **(b) False Negative Decisions**

Figure 2: Average Security-Level vs. the Number of Mobile Nodes

Figure 4 and table 2 shows that the error occurred by the Fuzzy Decision Function is remarkably small than the Negative selection mechanism. Even though in the small number of nodes both mechanisms show almostly the same results but the overall performance of the fuzzy decision function is higher.

The Decision Time

The time required to take the decision either to eliminate the node or not in both cases are measured, the results are shown in table 3 and figure5 both results are in seconds.

Table 4: Decision Time of –ve Selection vs. Fuzzy Function

No. Nodes	25	50	75	100	125	150	175	200	225	250
Negative Selection	0.003	0.007	0.01	0.015	0.019	0.023	0.027	0.032	0.04	0.048
Fuzzy Decision	0.008	0.01	0.015	0.017	0.02	0.021	0.025	0.29	0.033	0.037

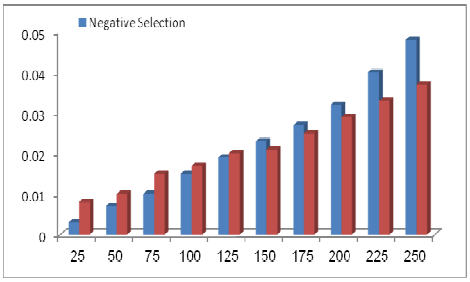


Figure3: Decision Time of –ve Selection vs. Fuzzy Function

Figure 3 and table 4 shows the Key creation time with the number of mobile nodes between 25 and 250. The speed of Decision time is very small for all two techniques. However, the fuzzy decision rules have faster Key decision time than the negative selection, especially with many mobile nodes.

CONCLUSIONS

Botnet elaborates a huge amount of danger to all types of networks especially MANETs that is because of the diversity nature of MANETs.AIS is found to be one of the most reliable security models that could be used to secure such scenario. In this paper, we discussed the extremely vulnerable nature of the MANET. Also the paper covers the diverse challenges to the security of MANET. This paper also presents a new model for securing MANET ,that model take the advantages of the fuzzy decisions then applies them to the AIS as the security infrastructure. Then the paper demonstrates the advantages of the proposed model comparing to other existing methods for securing MANET.

REFERENCES

1. E.M.Hanafty, A.A.salama, M.Abdelfattah and Y.M.Wazery, "Security in MANET based on PKI using fuzzy function".IOSR Journal of Computer Engineering. India.2012.
2. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-Based Systems for Ad-hoc and Sensor Networks," Algorithms and Protocols for Wireless Ad-hoc and Sensor Networks, A. Boukerche (ed.), Wiley & Sons, 2011.
3. Er. Banita Chadhaa, Er. Zatin Gupta," Security Architecture for Mobile Adhoc Networks" (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 9, 2011, pp 101 – 104
4. AW. Stallings; "Cryptography and Network Security – Principles and Practice", 9th Edition; Prentice Hall 2010
5. A.Rajaram, S.Palaniswami ." THE MODIFIED SECURITY SCHEME FOR DATA INTEGRITY IN MANET". International Journal of Engineering Science and Technology. Vol. 2(7), 2010, 3111-3119
6. Y. Zhao, Y. Xie, F. Yu, Q. Ke, Y. Yu, Y. Chen, and E. Gillum, "BotGraph: large scale spamming botnet detection," in Proc. of the USENIX Symposium on Networked Systems Design and Implementation, Boston, MA, 2009.
7. D. Stefan and D. Yao. Keystroke dynamics authentication and human-behavior driven bot detection. Technical report, Rutgers University, 2009
8. M. Polychronakis, P. Mavrommatis, and N. Provos. Ghost Turns Zombie: Exploring the Life Cycle of Web-based Malware. In Proceedings of the USENIX Workshop on Large-Scale Exploits and Emergent Threats, 2008.
9. Yan L. Sun, Wei Yu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks", 2006 IEEE, pp305-317
10. A.Rajaram, S.Palaniswami ." THE MODIFIED SECURITY SCHEME FOR DATA INTEGRITY IN MANET". International Journal of Engineering Science and Technology. Vol. 2(7), 2010, 3111-3119
11. Alatas, B., Akin, E.: Mining Fuzzy Classification Rules Using an Artificial Immune System with Boosting. In: Eder, J. et al. (eds.) ADBIS 2005. LNCS, vol. 3631, pp. 283–293. Springer-Verlag Berlin Heidelberg (2005).
12. J. Y. Le Boudec and S. Sara_janovic. An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-Hoc Networks. Proceedings of Bio-ADIT 2004, Lausanne, Switzerland, January 2004, pp. 96-111
13. J.R. Al-Enezi, M.F. Abbod and S. Alsharhan. ARTIFICIAL IMMUNE SYSTEMS – MODELS, ALGORITHMS AND APPLICATIONS. IJRRAS. May 2010
14. J. Greensmith, U. Aickelin, and S. Cayzer. Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection. In Proceedings of the ICARIS-2005, LNCS 3627, pages 153–167, 2005.
15. Gong M., Zhang L., Jiao L. and Ma W., 2007. Differential Immune Clonal Selection Algorithm. Proceedings of 2007 International Symposium on Intelligent Signal Processing and Communication Systems Nov.28-Dec.1, Xiamen, China.