# A New Approach to Artificial Immune System for Intrusion Detection of the Mobile Ad Hoc Networks

Anass Khannous
CED STI
Laboratory LIST
FST of Tangier Morocco

Anass Rghioui
CED STI
Laboratory LIST
FST of Tangier Morocco

Fatiha Elouaai
CED STI
Laboratory LIST
FST of Tangier Morocco

Mohammed Bouhorma
CED STI
Laboratory LIST
FST of Tangier Morocco

## ABSTRACT

The use of artificial immune systems (AIS) in intrusion detection is an attractive concept for several reasons. Then it is judicious to expect that approaches of biological inspirations in this area, and specifically the abstraction of immune defense mechanism with its high detection capabilities and its strong defense against intrusion, will probably be able to meet this challenge. Researchers have implemented different immune models to design intrusion detection systems (IDS) in order to secure Mobile Ad Hoc Networks (MANET), but the most popular one is the self and non-self model. This model was used in the vast majority of biological inspiration in the field of MANET security. It has demonstrated attractive success, as well as it showed some weakness especially in terms of scalability and coverage. This paper try to incorporate some additional concepts proposed by the new danger theory in order to overcome some of the problems related to the adoption of the self and non-self-model. The proposed algorithm integrates and combines the basic concepts of intrusion detection system based on the role of T cells described by the negative selection algorithm, with those inspired by the role of dendritic cells to process the alarm signals and to judge thereafter whether there is presence of a dangerous element or not.

## General Terms

Security, Mobile Ad hoc networks, Intrusion detection, Artificial Immune Systems.

## Keywords

MANET, AIS, IDS, Danger theory, Negative selection

## 1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a self-organized network consisting of a mass of sensor nodes. MANET differs from traditional network through its own characteristics:

- The memory and computing capability of sensor node is reduced,
- Wireless communication, by its nature, requires optimization of energy and bandwidth,
- The entire network serves to capture, store, process and transfer data,
- The application environments are complex
- Lack of existing infrastructure,
- The network topology is random and dynamic.

Then it is obvious that MANET security is vulnerable, and lots of challenges are to be solved. Indeed, the wireless communication between the sensor network nodes makes the attack easier. Mainly, the attack methods are becoming more diverse. Many research works are oriented towards the implementation of new defense tools that are more appropriate, automatic and particularly adaptive taking inspiration from the Human Immune System (HIS).

Researchers have incorporated different immune models, but the main one is the self and non-self-model. This model, though, has demonstrated attractive success, as well as it showed some weakness especially in terms of scalability and coverage.

This paper try to incorporate some additional concepts proposed by the new danger theory in order to overcome some of the problems related to the adoption of the self and non-self-model. The proposed system should enable the detection of actual intrusions that are generated not only by the external system components, but also by its internal members. This is guaranteed by the incorporation of the danger concept, which is the basic principle of the danger theory, to distinguish and identify self-elements components but harmful and non-self-elements but harmless [1].

Thus, the objective is to maximize the true positive rate on one hand, and to minimize on the other hand the true negative rate. The true positive rate presents a real detection of non-self-members, while the true negative rate presents error rate caused by the detection of self-elements by the system as intruders.

## 2. ARTIFICIAL IMMUNE SYSTEM(AIS)

The comprehensive study of HIS has raised various components and basic operation mechanisms of that system. It has large capacity to protect the human body against a huge variety of foreign pathogenic intrusions. In order to build on the success and strengths of this natural system, researchers have proposed the artificial immune system (AIS) to solve various problems, and the main application was related to the mobile ad hoc networks security [2, 3]. To better understand and introduce the AIS, various approaches and algorithms, listed below, have been deeply studied and some of them are implemented in this article.

- The negative selection algorithm (NSA)
- The positive selection algorithm (PSA)
- The clonal selection algorithm
- Immune memory

- The self and non-self-model
- The danger theory model

A large part of research carried out in the field of artificial security of mobile ad hoc networks, are based on the self and non-self-model. However, despite its reputation, it has shown some limitations. This paper is more interested in the danger theory model in order to try to address the limitations of the self/non-self model already cited. In what follows, these two models are briefly presented.

## 2.1 The self/non-self model

The basic property of the immune response is the ability to distinguish between self-cells and non-self-cells (foreign). This discrimination is learned early in the cells life through different immune processes, and the negative selection is the main process. Self-cells are cells belonging to the human body and are unable to trigger a reaction of the immune system in the normal state. All other cells are considered to be non-self-cells and therefore the immune system is initiated to react against theme.

## 2.2 The Danger theory model

It is a new vision for managing the immune system behavior. Initially Proposed in 1994 by Matzinger [4, 5, 6]. It proposes new conditions for triggering the immune response so that it is triggered by the existence of danger, and not because of the existence of a foreign element. In other words, the immune system does not react against the self, unless it is dangerous, as it should react against non-self, unless it is not dangerous. The emergence of the danger concept is strongly present in the resolution of immune responses.

# 3. INTRUSION DETECTION SYSTEM (IDS)

Kim [1] has defined the intrusion detection system as an automated system whose role is to detect intrusion into a computer system while examining security audits provided by the operating system or network monitoring tools. Its main purpose is to detect unauthorized use, misuse and abuse in a computer system by internal and external users. Given the significant number of possible attacks, they can be classified according to different classifications. Choosing the type of IDS is based on the effectiveness tests, the type of need for security and finally the constraints posed by the systems and users. Various existing IDS classifications have been studied according to:

- The detection method which has two approaches: the behavioural approach and the knowledge-based approach.
- The system response after detection: The majorities of IDS are only detecting attacks or attack attempts, while some of them have the ability to act if necessary. Two models are to be differentiated, Passive IDS and active IDS.
- The source of information: The IDS are also classified according to the origin of the data that will be used to detect intrusive actions. There are two main categories: host-based IDS and network-based IDS.
- Frequency of use: Two models of IDS differ according to frequency of use: continuous or real-time monitoring, and periodic or delayed monitoring.

# 4. STUDYING AIS APROACHES FOR INTRUSION DETECTION

By carefully studying the approaches mentioned in the literature, it is evident that the majority of these studies have focused on the study of the different characteristics of the negative selection algorithm NSA. This is the thing that makes it the most popular algorithm in term of resolving IDS problems inspired from the immune defense, including anomaly detection. However, despite its attractive properties, NSA has not shown great success in real applications. There are two major drawbacks preventing its success to be effective IDS, namely scalability and coverage. To overcome this scalability problem, several researches have been carried out. Much of this work has focused on developing more efficient algorithms for detectors generation. Others have attempted to use new correspondence functions between the detector and the antigen. This may have resulted in a gain of computing time at the detector generation and pairing stage. The objective of these algorithms is to minimize the true negative rate that illustrate error rate caused by the detection of self-elements by the system as intruders, and maximize the true positive rate that presents a real detection of non-self-members.

It appears that even with the introduction of several enhancements to the NSA, it is still not arrived to be an efficient algorithm for IDS. This may be due to its intrinsic limit deduced from the initial hypothesis which assumes that any detection of foreign element is considered as an intrusion. Sometimes the presence of non-self components does not necessarily indicate the presence of an intrusion, so this hypothesis often leads to a high error detection rates or false positive.

Burgess [7,8,9,10] stated that the concept of distinction between self and non-self components , upon which NSA is based, is not up to simulate the entire human immune mechanism, so it is not that simple to apply directly to the security problem. However, He argued for a new theory introduced by Matzinger [4, 5, 6] since 1994 called the danger theory, which describes the interaction between dendritic cells and T cells.

# 5. PROPOSITION OF A NEW APPROACH BASED ON THE DANGER THEORY

## 5.1 The proposed approach objectives

The goal is to build an IDS in order to reduce the error rate represented by the false positive rate. This model gives a great importance to the danger signals in order to decrypt the intrusion scenarios to address threats based on the correlation of these signals just like the ability of the human immune system to identify the danger signals. The proposed system consists of collecting signals from hosts or network, and correlates these IDS alerts signals. An alert is considered good or bad in parallel to two types of signals which coincides with biological cell death that are apoptosis and necrosis.

The algorithm should allow the filtration of the detectors during their generation by processing both the Negative selection and the danger theory concepts. The detectors population then will be very precise which will allow minimizing true negative rate and maximizing true positive rate. True negative rate illustrate error rate caused by the detection of self-elements by the system as intruders, while true positive rate presents a real detection of non-self-members.

## 5.2 Abstraction done from HIS

Apoptosis is the process that corresponds to natural death and that means no bad behavior. While necrosis indicates the presence of serious attacks when real damage exist in the system and when cells have undergone a pathological death.

In the context of an IDS, the apoptosis signals indicate the normal state of the monitored system while necrosis indicate significant changes in the environment as for example CPU usage or memory used, ..etc

## 5.3 Description of the proposed approach

This paper propose to focus on improving the security model proposed by Aickelin et al. [11, 12] This by establishing a Framework as security model of MANET based on the integration and combination of NSA basic concepts based on the role of B and T cells, with concepts inspired by the Danger theory, which presents itself as an intrusion detection technique that describes the interaction between dendritic cells and T cells with the integration as well of alarm signals.

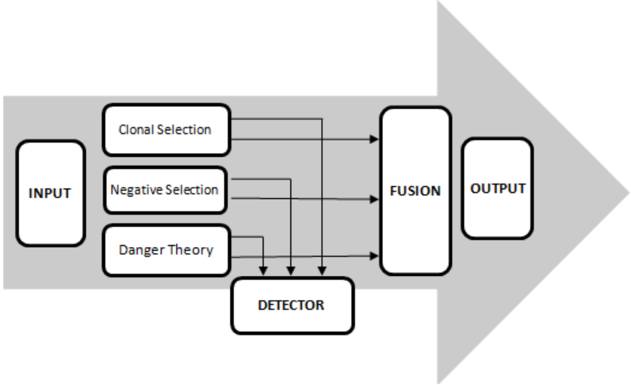

**Fig. 1 Description of the approach: Merging NSA & Danger theory concepts**

## 5.4 Description of the proposed algorithm

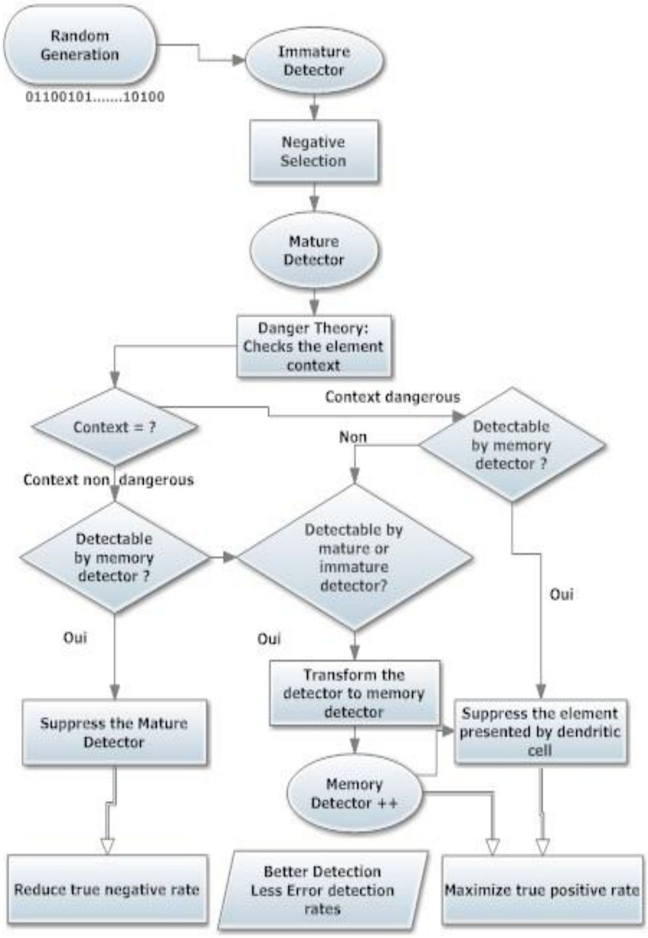
Random Generation
01100101.......10100
Immature Detector
Negative Selection
Mature Detector
Danger Theory: Checks the element context
Context = ?
Context dangerous
Context non dangerous
Non
Detectable by memory detector ?
Detectable by memory detector ?
Detectable by mature or immature detector?
Oui
Oui
Oui
Transform the detector to memory detector
Suppress the Mature Detector
Suppress the element presented by dendritic cell
Memory Detector ++
Reduce true negative rate
Better Detection Less Error detection rates
Maximize true positive rate

**Fig. 2 The algorithm describing the detectors generation process**

To better describe the proposed approach, this section describes the proposed algorithm that is nothing other than a detectors generation process. For each generation, dendritic cells present a set of fixed size elements, randomly chosen from the whole antigen with the corresponding context. According to the context of the presented element, a number of operations will be established in order to allow the memory detectors population to detect intrusive elements. If the element's context is dangerous, then the algorithm checks whether this element is detectable by memory detectors population, and consequently only this protein will be deleted from the set of introduced elements. But if dangerous element is not detectable by the memory detectors population, then the algorithm checks in the population of mature detectors if there's a detector that can detect this element. If such detector exists, then it will be added to the memory detectors population and the corresponding protein will be eventually removed from all the presented elements. In the case where the presented element is harmless, then the algorithm checks if this element is detectable by memory detectors population in order to remove the corresponding detector.

## 5.5 Discussions

To achieve the main purpose of intrusion detection systems, which is to increase the true positive detection rate and to reduce the true negative rate, the proposed system allows detection of real intrusions that can be produced by self or non-self elements.

The proposed algorithm performs some modifications on the NSA by incorporating the danger concept. The incorporation of this new concept is ensured via the combination of two inter-related immune systems that are innate immune system and adaptive immune system. The experimental results of this algorithm show promising results as it is possible to detect harmful components that could be even self or non-self elements, with a progressive tolerance to harmless components. It allows obtaining high true positive rate, and low true negative detection rate.

## 6. CONCLUSIONS

The human immune system HIS protects the body against damage that can be caused by a large number of bacteria and pathogenic viruses. It performs this task without any prior knowledge of the structure of these pathogens. In addition, HIS has several other interesting features that make it the focus of increasing interest to solve various problems. Some AIS have been built for several application areas including classification, pattern recognition and robotics, etc. Computer or Network security is one of the application areas to which AIS is most frequently addressed. This area has a direct application of the immune metaphor. The similarity between the two systems leads to the appearance of several works in this field.

Viewed from such a perspective, the human immune system can be seen as a form of anomaly detector with very low false positive and false negative rates. An increasing number of studies appeared to understand and extract the key mechanisms by which the human immune system is able to perform its detection and its protection and learning capabilities.

After studying the various research works that have used AIS in intrusion detection, it is clear that the self and non-self model is the dominant model because it is adopted by the different proposed works. However, this model based on the discrimination between self and non-self shows some problems. With the appearance of the danger theory that defies this model and presents interesting new ideas, some of new concepts proposed by this theory could be exploited to be used in the context of an intrusion detection system.

NSA is mainly based on the discrimination between self and non-self elements, and does not allow the detection of dangerous elements that constitute actual intrusions. The dangerous elements may be self-elements so as they can be non-self elements. The algorithm proposed in this paper tries to overcome problems related to self and non-self model by improving NSA. The objective is to achieve better detection rates.

The proposed solution allows enhancing more and more the mobile ad hoc networks security. It incorporates several concepts of LYSIS algorithm; as well as the clonal selection and immune memory models. It also integrates some basic concepts of the danger theory through the exploitation of danger concept initiated by the presence of harmful elements in the system. In this algorithm, the intrusion detection is related to the damage that can occur in the system, involved by internal or else by external elements. This detection is possible through the exploitation of items presented by dendritic cells with context information indicating the state of the environment.

As a matter of perspectives, the proposed approach will be generalized and evaluated using several kinds of MANET Attacks like Resource consumption Attack RCA, Black hole Attack, wormhole Attack, Sleep Deprivation, Eavesdropping, flooding. This approach should be also compared with other researcher’s results using OMNET ++ simulator.

## 7. REFERENCES

[1] J W Kim. “Integrating Artificial Immune Algorithms for Intrusion Detection”, PhD thesis, University College London, 2002.

[2] De Castro .L.N & Von Zuben .F.J “Artificial Immune Systems: Part I - Basic theory and applications”, Technical report, TR-DCA-01/99, December 99.

[3] De Castro .L.N & Von Zuben .F.J “Artificial Immune Systems: Part II - A survey of application”, Technical report- DCA RT 02 /00, 2000.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Matzinger. P. “Tolerance, danger and the extended family”, Annual reviews in Immunology, 12: 991- 1045, 1994.

[5] Matzinger .P. “An innate sense of danger”. Seminars in Immunology, 10:399-415, 1998.

[6] Matzinger. P “The Danger Model: A renewed Sense of Self”, Science 296: 301-305, 2002.

[7] M. Burgess. “Computer immunology”. In Proc. of the Systems Administration Conference (LISA-98), pages 283-297, 1998.

[8] M. Burgess. “Evaluating cfegine's immunity model of site maintenance”. In Proceeding of the 2nd SANE System Administration Conference (USENIX/NLUUG), 2000.

[9] M. Burgess. Recent developments in cfengine. In Proceedings of the 2nd Unix.nl conference, Netherlands, 2001.

[10] M. Burgess. “Two dimensional time-series for anomaly detection and regulation in adaptive systems”. In M. Feridum et al., editor, Proceedings of 13th IFIP/IEEE International Workshop on Distributed System, Operations and Management (DSOM 2002), volume 2506 of Lecture Notes in Computer Science, pages 169-180. Springer-Verlag, 2002.

[11] Aickelin. U & Bentley . P & Cayzer. S & Kim . J & McLeod. J “Danger Theory: The Link between AIS and IDS?”, in Proceedings ICARIS – 2003, 2nd International Conference on Artificial Immune Systems, 147 – 155, 2003.

[12] U. Aickelin and S. Cayzer. “The danger theory and its application to AIS”. In J. Timmis and P. J. Bentley, editors, in Proceeding (ICARIS), pages 141-148, 2002.