A Biologically-Inspired Type-2 Fuzzy Set Based Algorithm for Detecting Misbehaving Nodes in Ad-Hoc Wireless Networks

Andrea Visconti[1], Hooman Tahayori[2]

[1]*Dipartimento di Informatica e Comunicazione, Università degli Studi di Milano*
[2] *Department of Computer Science, Ryerson University, Toronto, Canada*

Abstract

Implementation of routing protocols in mobile ad-hoc networks relies on efficient node cooperation. However, node misbehavior is a common phenomenon, thus, ad-hoc networks are subject to packet dropping, packet modification, packet misrouting, selfish node behavior, and so on. In this paper, a biologically-inspired type-2 fuzzy set recognition algorithm for detecting misbehaving nodes in an ad-hoc wireless network is presented. Such algorithm, inspired by danger theory and antigen presenting cells, would be implemented in an Artificial Immune System (AIS) for detecting misbehaving nodes without human intervention.

1. Introduction

Ad-hoc wireless networks are collections of autonomous, self-organized, wireless end-user terminals, independent of any fixed infrastructure. The arbitrary topology of ad-hoc wireless network introduces limitations in communication since it relies on efficient and fare nodes cooperation in order to implement specific routing protocols. These limitations in communication provide a fertile ground for attackers [1,2]. Ad-hoc wireless networks are vulnerable to packet dropping, packet modification, packet misrouting, selfish node behavior, DOS attack, etc. hence providing security guarantees is rather a difficult challenge.

In this paper, as an extension of [3], presents a type-2 fuzzy set based recognition algorithm for detecting misbehaving nodes in an ad-hoc wireless network. The recognition algorithm is derived from the binding between lymphocytes receptors and antigens. Such algorithm would be implemented in the framework of an Artificial Immune System (AIS) that enables detecting misbehaving nodes, identifying dangerous situations, protecting the network from reinfection, and mitigating the problem of routing misbehavior without human intervention.

Unfortunately, the challenge of implementing Artificial Immune Systems that protect the networks from unwanted behaviors faces the problem of providing reliable discrimination between normal and abnormal behaviors, in order to take under control the number of false positive. Since no sharply defined criteria for such discrimination exists, fuzzy set is a convenient point of departure for dealing with the problem. Several fuzzy approaches have been described in literature, some based on type-1 fuzzy set [4, 5], others based on type-2 fuzzy set [6, 3]. Knowing that in type-1 fuzzy set approach the membership function is well defined and does not convey uncertainty about the membership values, we apply type-2 fuzzy sets approach that enable handling and minimizing the effects of uncertainties [7].

Three sources of uncertainties are identified. First, system parameters of wireless networks may be negatively affected by background noise, introducing significant changes in the observed values. Second, a subset of system parameters – number of packet lost, number of packet sent, throughput of the network, and so on – may be sufficient for describing a routing misbehavior, but how to identify precisely such subset is not always well-defined. Third, once chosen a specific subset of system parameters that can help describing a routing misbehavior, the alarm thresholds for such system parameters may have different values to different experts – i.e. the same value has different meaning to different people. All these sources of uncertainties are convincing enough for designing the recognition algorithm based on type-2 fuzzy sets.

The rest of the paper is organized as follows. In Section 2 we discuss the principles of immune systems, focusing on dendritic cells, antigen-specific immune response and danger signal. In Section 3, we briefly present the state of the art of artificial immune system in the field of network security, while in Section 4, we describe the design principles of the proposed AIS. In Section 5, we present the interval type-2 fuzzy set based recognition algorithm for granulating nodes' behavior. Finally, Section 6 concludes the paper.

2. Dendritic cells, specific immune response, and danger signals

2.1. A link between innate and adaptive immune system: dendritic cells

The innate immune system is the first line of defense of vertebrates meant to protect the body from birth. Such line of defense recognizes and attacks enemies in a non-specific manner, without the necessity of previous exposure to them. This means that innate immune cells recognize and remove pathogens in a generic way. The most important functions of the innate immune system are (a) releasing chemical factors that cause inflammation and swelling, (b) recruiting immune cells to sites of infection, (c) recognizing and killing foreign intruders within the body, (d) removing pathogens and dead cells, and (e) activating the adaptive immune system. Focusing on the last point – (e) – we will investigate the rule of dendritic cells, a specific kind of innate immune cells, which provide a link between innate and adaptive immune system.

Dendritic cells (DCs) which are considered as potent *antigen presenting cells* (APCs), are phagocytes of the innate immune system that engulf, process, and present antigen material to lymphocytes. Therefore, dendritic cells are able to stimulate lymphocytes of the adaptive immune system: the naïve T-cells. DCs are distributed in peripheral blood, lymph nodes, and peripheral tissues, especially in those that provide an interface on external environmental – e.g. the skin, lugs, etc. – and are involved in both specific and non-specific immunity. In one sense, their capacity to stimulate cells via antigen presentation is essential for inducing an antigen-specific immune response; while in the other sense, they play a central role in host defense – e.g. anticancer host defense.

DCs exist in different states of maturity: *immature* DCs (iDCs), *semi-mature* DCs (smDCs), and *mature* DCs (mDCs). These states of maturity are strongly related to the chemical signals (*cytokines*) released by pathogenic and regular cells of the body. Such signals can have *anti-inflammatory* effects – when cytokines are released by programmed cell death (*apoptosis*) – or *pro-inflammatory* effects – when cytokines are released by premature, unnatural, or non-programmed cell death (*necrosis*) – on the cells of the body [8].

DCs remain in an immature state in absence of infections. iDCs do not possess the ability to stimulate T-cells because they lack the essential accessory signals for T-cell activation. When iDCs are exposed to a number of pro-inflammatory cytokines, iDCs acquire the ability to stimulate T-cells, and their state changes from immature to mature (mDCs). Similarly, when iDCs are exposed to anti-inflammatory cytokines, iDCs' immune-regulatory ability is enhanced, and their state changes from immature to semi-mature (smDCs) [8].

Once invaders that are present on the skin surface find an injury and enter the body, the cells surrounding the injured area release a range of chemicals. These chemical signals (cytokines) cause swelling, redness, heat, and pain which are the symptoms of the inflammation. The inflammation reduces the probability of the spread of infection, and causes local blood vessel dilation that will bring more blood to the injured area for helping the healing process. iDCs, that engulf invaders in the affected area, are exposed to numerous chemical signals that stimulate dendritic cells to change their state from iDCs to mDCs. After appropriate maturation, mDCs migrate to lymphoid tissues where they present antigen material to T-cells, triggering the adaptive immune response.

2.2. Antigen-specific immune response

The *adaptive* or *acquired immune system* provides the second line of defense in the fight against intruders. The ability of the adaptive immune system to kill invaders is based on the capacity of recognizing various kinds of pathogens and remembering them after the resolution of the infection. Compared to the generic response of innate immune system, the adaptive immune system works in a more complex way, in fact, the recognition process is done through a binding between lymphocytes *receptors* and special parts of pathogens called *epitope*. The receptors cannot bind to any type of pathogens because, in a given time, the number of different antigens could potentially be superior to the number of receptors present in the body. This means that a lymphocyte can get bound to a group of structurally related epitopes which define *similarity subset* of pathogens. Evidence is mounting to support that adaptive immune system necessitates a sort of approximate binding. For this reason, a lymphocyte will be activated by a pathogen when the binding between receptors and epitopes exceeds the so called *affinity threshold*. The side effect of this approach, based on an affinity threshold, is the possibility that a lymphocyte erroneously binds to cells of the body and activates the adaptive immune system (*autoimmune reaction*).

Lymphocytes are composed of two major classes: B-cells (*B- and memory B-cells*) and T-cells (*Helper* and *Killer T-cells*). Although all lymphocytes derive from cells in bone marrow, T-cells migrate from bone marrow to *thymus gland* to be matured. In thymus, T-cells are educated to react with foreign antigens through the process of *positive* and *negative selection*, during which more that 90% of T-cells die by apoptosis.

Helper T-cells are a subgroup of T-cells, which help to stimulate and control immune system reactions. Helper T-cells do not kill, neutralize, or engulf foreign antigens but promote the activation of adaptive immune response through *stimulatory signals*. When activated, helper T-cells release cytokines that trigger killer T-cells and stimulate B-cells to produce antibodies. Moreover, helper T-cells control and prevent immune system disorders, inhabiting autoimmune reactions.

Killer T-cells are a subgroup of T-cells, which kill cells with abnormal behavior, destroying damaged and infected cells. Killer T-cells, activated by Helper T-cells through stimulatory signals, are tightly controlled because they release potent cytokines in response to infected cells found, contributing to tissue damage. Sometimes pathogens, that are not always fluid in the body, get enter into the cells – like viruses and some bacteria – and are referred to as *intracellular* pathogens. Body cells are equipped with a special molecule, *Major Histocompatibility Complex* (MHC), that replicate a collection of inter-cell protein fragments on the surface of the cell. Killer T-cells bind such fragments and kill the infected cell by making holes in the target cell membrane, or releasing chemical factors that induce apoptosis in the target cell.

B-cells are the second class of lymphocytes that react against intruders by producing proteins called *antibodies*. B-cells need two signals for activation. The first is the stimulatory signal that comes from helper T-cells, while the second is the binding between B-cell receptors and antigens. Becoming active, B-cells secrete antibodies against invaders and then clone itself, subjecting their receptor to very high mutation rate known as *somatic hypermutation*. This process will continue with new emerging B-cells and, with respect to Darwinian process, new B-cells will have higher affinity threshold with the existing pathogens. When infection is under control, the level of antibodies in the blood declines quickly, a major number of B-cells die by apoptosis, but a small number of such cells mature into *memory B-cells*. Such cells are the *immunological memory* of the body, that in a future encountering with the same pathogens, will help the body to provide a quick secondary response [9].

2.3. Danger theory

In 1994, Polly Matzinger suggested "Danger Theory" [10], a controversial new theory that introduces additional levels of control to adaptive immune responses for explaining the existence of a phenomenon such us immune tolerance, never fully explained by self/non-self paradigm. Matzinger suggests that endogenous danger signals, released by damage or stress tissue cells, can be thought as one of the triggering signals for immune response activation. As consequence, the immune system mobilizes the innate immune cells to attack the infected area. For activating an adaptive immune response, the biological immune system (BIS) needs a second signal, provided by antigen presenting cells (APCs) during the antigen presentation process in lymph nodes. Thus, Matzinger supposes that the immune system does not discriminate between self/non-self elements but between dangerous and harmless signals.

Following the danger theory, an adaptive immune response is induced by danger signals and foreign materials presented by APCs to lymphocytes. For these reasons, antigen presenting cells of the innate immune system such us dendritic cells, play a key role for guiding an antigen-specific immune response.

3. Related works

Wireless networks are subjected to several attacks and security problems that are well studied [1, 2, 11]. In particular, for mitigating routing misbehavior in mobile ad-hoc networks, a number of solutions have been published in literature. Marti et al. [1] suggest two techniques – the watchdog and the pathrater – for increasing throughput of the network with moderate and extreme mobility. In [2], authors have investigated performance degradation in mobile ad-hoc networks caused by misbehaving nodes, suggesting the 2ACK scheme for detecting and mitigating routing misbehavior. Buttyan and Hubaux [12] introduced the concept of "nodes payments" for packet forwarding, trying to countenance the number of misbehaving nodes. Buchegger and Le Boudec suggest a reputation-based protocol called CONFIDANT [13], in which nodes calculate the reputation of all others and use neighbours' reputation for avoiding false positive, making misbehavior unattractive. These useful works can be defined as traditional works, because are based on the recognition of misbehaving patterns.

The second class of works tries to exploit the advantages of using learning-based and adaptive-based approaches. Toward this aim, a number of works based on immune theories are published in literature, e.g. [11], in which Sarafijanovic and Le Boudec have presented an AIS based on virtual thymus, dynamic self and danger signals for mitigating routing misbehavior in ad-hoc wireless network and taking under control the number of false positive. Drozda et al. [14] discuss performance of AIS based on random set of detectors, negative selection process, and performance measurement genes, for detecting misbehaving nodes in wireless sensor networks. Geensmith et al. introduced dendritic cell algorithm (DCA) for recognizing anomaly detection [15]. Kim et al. extend the work presented in [15] suggesting CARDINAL [16], an

automated worm detection system. Aickelin et al. [17] have applied danger theory approach for intrusion detection. In [18], Kim et al. have combined the idea of artificial tissue, danger theory and dendritic cells for recognizing the execution of malicious code. In [5] Gomez et al. and in [4] Gomez and Dasgupta, have introduced a type-1 fuzzy set approach for detecting intrusions and anomalies, while Visconti and Tahayori in [6] have suggested a type-2 fuzzy set approach for intrusion detection systems.

4. Design of the artificial immune system

4.1. How BIS elements are mapped to AIS elements

To design a misbehavior detection system based on the workings of the biological immune system, clear understanding about the mapping of BIS elements to AIS elements is of great importance. Given the complexity of interaction between biological elements, the proposed AIS does not fully and faithfully mimics its natural counterpart, but merely take inspiration from some features of its natural counterpart presented in Section 2. In particular, biological features and elements mapped are:

- Body: nodes and packets of a wireless ad-hoc network;
- Tissue cells: packets of the network;
- Immune cells: nodes of the network;
- Apoptosis: packets successfully received;
- Necrosis: packets lost or received with high delay;
- Cytokines anti-inflammatory: signal released by packets successfully received – acknowledgment (ACK);
- Cytokines pro-inflammatory: signal released by packets lost – there is no ACK, – or received with high delay – delayed ACK;
- Immature Dendritic Cells (iDCs): are nodes of the ad-hoc wireless network – regular users – that fully cooperate in a common routing protocol, for generating a flexible and decentralized network topology. iDCs have never had experience with packets lost;
- Mature Dendritic Cells (mDCs): are nodes of the ad-hoc wireless network – regular users – that have had experience with packets lost;
- mDCs' migration to lymphoid tissues: Packets (called migration signals) sent from mDCs to Helper T-cells that contain information about misbehaving nodes;
- Danger signal: in the proposed AIS it is a collection of two signals that are the cytokines pro-inflammatory and migration signal;
- Antigen presentation process: in the proposed framework, this process is simulated by an interval type-2 fuzzy set based (IT2FS) algorithm that recognizes a misbehaving node presented by mDCs;
- Helper T-cells: Special network nodes that promote and control the artificial immune reaction when abnormal network parameters are recognized. They execute the IT2FS based algorithm and activate Killer T-cells through a stimulatory signal;
- Stimulatory signal: signal used for activating Killer T-cells;
- Killer T-cells: special nodes of the network that punish misbehaving nodes, temporally excluding them from the network;
- Memory B-cells: special network nodes that remember misbehaving nodes previously encountered. These nodes constitute the immunological memory of the AIS;
- Autoimmune reactions: uncontrolled nodes of the network that wrongly, or maliciously, try to activate the adaptive immune response in absence of misbehaving nodes.

4.2. How the AIS works

Base on the aforementioned points, we can design an AIS, focusing on the observation that any kind of routing misbehavior produce local or global side effect in ad-hoc wireless network. Identify such side-effects would be fulfilled through monitoring and analyzing network parameters like the number of packets lost, number of packets sent, throughput of the network, and so on.

Suggested AIS consists of autonomous network nodes that try to face and mitigate routing misbehavior. In this regards, iDCs fully cooperate for executing a common routing protocol. When a packet is lost in the network (*necrosis*), the ACK does not reach the source, releasing the first component of a danger signal (*cytokines pro-inflammatory*). iDCs exposed to a number of pro-inflammatory cytokines, are stimulated and their state changes from immature to mature (*mDCs*). mDCs send to Helper T-cells a migration signal that contains information about misbehaving nodes (*migration to lymphoid tissues*), activating the misbehavior detection process (*antigen presentation process*).

Helper T-cells spent their lifetime collecting the sample data of various network parameters. When helper T-cells receive a migration signal from mDCs, they begin the antigen presentation process, analyzing the network parameters through the type-2 fuzzy set recognition algorithm (Section 5). For the sake of security, we designed helper T-cells as a subset of network nodes (*distributed approach*), which cooperate in order to take the final decision: well-behaving or misbehaving node. If helper T-cells get to the conclusion that a node misbehaves – i.e.

the binding between helper T-cells' *receptors* and *epitopes* exceeds the *affinity threshold*, – a signal is sent to killer T-cells (*stimulatory signal*) for taking appropriate countermeasure (*antigen-specific immune response*). Otherwise, if helper T-cells get to the conclusion that there is no abnormal behavior, we are in presence of an uncontrolled node (*autoimmune disease*). This means that such node wrongly, or maliciously, trying to activate the adaptive immune system. Also this node is considered a misbehaving node and a stimulatory signal will be arisen for the suppression. In both cases, activated killer T-cells temporally exclude (*kill*) the misbehaving node from the network. The excluding period is not always the same, but will be directly proportional to the number of times that a specific node misbehaved. Such number is stored by memory B-cells, which constitute the memory of the AIS (*immunological memory*).

When a misbehaving node is excluded from the network (*infection confined*), mDCs, helper and killer T-cells stimulated by danger signal became inactive (*apoptosis*), and come back in their normal state. If in future the same node misbehaves, the immunological memory reduces the time required for mounting a specific response against attackers (*secondary immune response*). In fact, during the antigen presentation process, helper T-cells use a backward propagation factor – i.e. the misbehaving nodes' history, – for quickly recognizing a misbehaving node. Such backward propagation factor follows the principle "did it, will probably do it again".

5. Misbehavior Detection

5.1. Type-2 fuzzy set approach

The arbitrary topology of ad-hoc wireless networks, independent of any fixed infrastructure, introduces limitations in communication that could be a fertile ground for misbehaving nodes and attackers. A feasible method for monitoring an ad-hoc wireless network, and deciding whether nodes misbehave or perform regularly, is through observing the network parameters. In the simplest scenario, given M useful network parameters that each can take N_i values; we can imagine $\prod_{i=1}^{M} N_i$ different states for the system from which a portion may be an indication of misbehaviors. Imagine it is possible to sharply discriminate the $\prod_{i=1}^{M} N_i$ states of the system to T_1 regular and T_2 pathogenic patterns that is $T_1 + T_2 = \prod_{i=1}^{M} N_i$. Consequently, to detect the intrusions with 100 percent of precision, we must recognize T_2 different pathogenic patterns. Unfortunately, T_2 can be astronomically high, making in practice this solution unfeasible.

Setting aside for a moment these practical limitations, we turn our attention on three important issues unresolved. First, not all network parameters are required for monitoring the system, but which and how far each network parameters may be effective for this purpose is not well-defined. Second, once chosen a specific subset of network parameters that can help describing a routing misbehavior, the alarm thresholds for such network parameters should be identified, but different experts may believe in different values. Third, system parameters of wireless networks may be negatively affected by background noise. These three unresolved issues combined with the ability of fuzzy set to handle the uncertainties, make type-2 fuzzy set framework a proper choice for designing misbehavior detection algorithm.

5.2. Interval Type-2 Fuzzy Set Based Recognition Algorithm

When mDCs send a migration signal to helper T-cells that contain information about misbehaving nodes, the *antigen presentation process* begins. Independent network nodes – artificial helper T-cells – monitor the $F=\{f_1,\ldots,f_M\}$ network parameters and based on the observed changes in the values of the parameters, are able to recognize a misbehaving node presented by mDCs. As discussed in Section 4.2, a factor f_i is used as backward propagation impulse for remembering the nodes' behavior history previously stored in memory B-cells. Such factor will improve the recognition capability and it is the starting point of the secondary immune response.

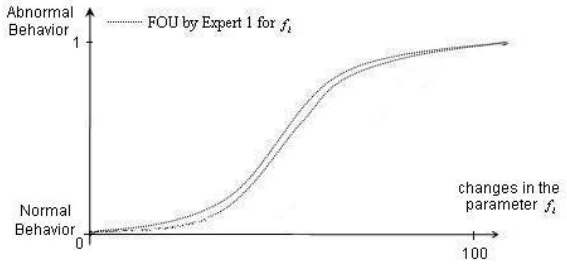

Figure 1. FOU by expert 1 for parameter f_i

In order to capture the real behavior of a node under investigation, we have surveyed a number of experts on their intuitions on how far the changes in different system parameters may be an indication of an attack. This information constitutes the basis of the recognition capabilities of helper T-cells. Using the *person MF approach* discussed in [19] that enables modelling intra and inter uncertainties of the experts about the effects of changes in parameters, primarily we asked each expert to provide a broad-brush Footprint of Uncertainties (FOU) [19] for each network parameter in the domain of X=[0,100] (see Figures 1, 2 and 3).

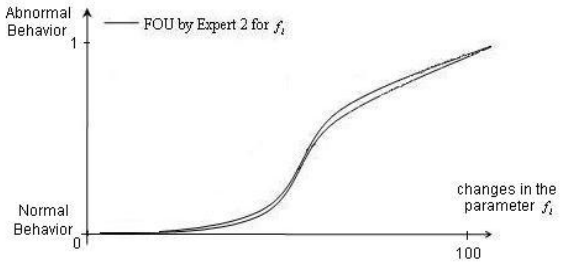

Figure 2. FOU by expert 2 for parameter f_i

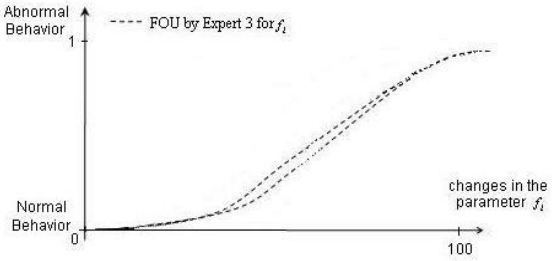

Figure 1. FOU by expert 3 for parameter f_i

Aggregating the experts' FOUs through mathematical operation of union (see Figure 4) and filling the results of the union, we reached to the final FOU that here we called *interval type-2 fuzzy map* (*IT2FM*) of each parameter (see Figure 5).

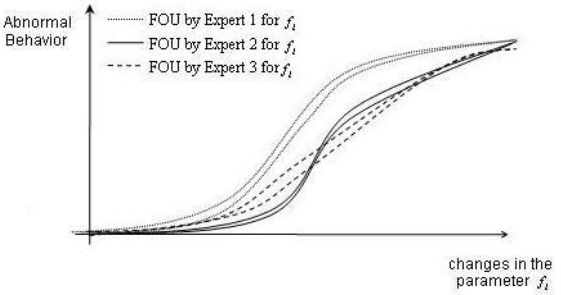

Figure 4. Union of the FOUs for network parameter f_i, given by the experts

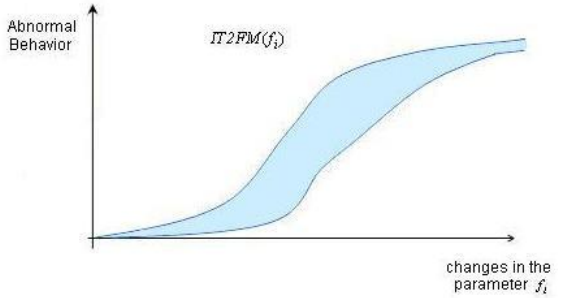

Figure 5. Interval Type-2 Fuzzy Map (IT2FM) of the system parameter f_i

Figures 1–5 show an example of driving IT2FM of the parameter through f_i person MF approach.

The IT2FM of the network parameter f_i would be formally depicted as,

$$IT2FM(f_i) = \{(x, [\underline{u}_{f_i}(x), \overline{u}_{f_i}(x)]), x \in [0,100]\} = \left\{\left(x, \tilde{\mu}_{f_i}(x)\right), x \in [0,100]\right\}$$

where $\tilde{\mu}_{f_i}(x) = [\underline{u}_{f_i}(x), \overline{u}_{f_i}(x)] \subseteq [0,1]$ represents the uncertain attack-indication of x percent change in the network parameter f_i, defined by the experts. We also assumed that negative changes – i.e. x<0, – be considered as $\tilde{\mu}_{f_i}(x) = \tilde{\mu}_{f_i}(0),\ x < 0$ while very high changes in network parameters – i.e. x>100, – be treated as $\tilde{\mu}_{f_i}(x) = \tilde{\mu}_{f_i}(100),\ x > 100$. The experts are also surveyed for indicating the importance of the changes in any network parameter. These surveys resulted in the recognition of non-necessarily pair-wise disjoint regions in [0,1], namely *White*, *Yellow*, and *Red* for each network parameter f_i (Figure 6). The *White* region indicates a normal behavior in the case of the corresponding change, the *Yellow* region indicates a suspicious behavior, while the *Red* region indicates a misbehavior of the network parameter f_i.

Antigen presentation process induce helper T-cells to measure the actual changes v_i of the network parameter f_i, and find the region (Red, Yellow or White) to which $\tilde{\mu}_{f_i}(v_i)$ is closer (Figure 6).

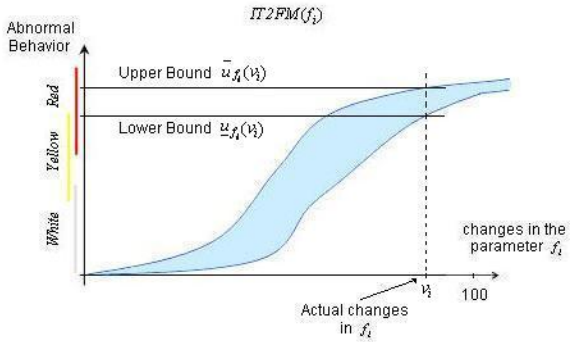

Figure 6. An example of $\tilde{\mu}_{f_i}(v_i)$

Figure 6 shows an example that both lower and upper bound of actual changes v_i are in a misbehave region (Red region). This result could suggest the presence of misbehaving nodes, but is not enough for completely describing a bad node's behavior. In fact, a parameter can be negatively affected by background noise and it can be found in the Yellow or Red region even if we are not in presence of misbehaving node (*false positive*). For this reason, helper T-cells need a more general view of the network for drawing the final decision, therefore, they build the IT2FM for the whole network based on all M network parameters. To do so, Helper T-cells have to

i. evaluate all network parameters f_i, $i \in \{1,\ldots M\}$, building the *Interval Type-2 Fuzzy Map of the System* – also known as *IT2FM*(*sys*). To do so, initially *IT2FM*(*sys*) is set to null, i.e. *IT2FM*(*sys*)={(*x*,0), 0≤*x*≤100}. When each network parameter is put in the Red region, the *IT2FM*(*sys*) will be iteratively built as $\tilde{\mu}_{sys}(v_i) \leftarrow Hull\left(\tilde{\mu}_{sys}(v_i) \cup \tilde{\mu}_{f_i}(v_i)\right)$, where

$Hull([\underline{a},\overline{a}] \cup [\underline{b},\overline{b}]) = [min(\underline{a},\underline{b})(\overline{a},\overline{b})]$ and iϵ{1,…*M*};

ii. calculate the boundaries of the centroid of *IT2FM(sys)* (see details in Appendix A);
iii. compare the result with the predefined granules *G={Normal-Behavior, Suspicious-Normal-Behavior, Suspicious-Misbehavior, Misbehavior}* defined by experts using the same method of person MF approach [19] – the *affinity thresholds algorithm* between helper T-cells' *receptors* and *epitopes*. To do so, it should calculate the distance of the centroid bounds of IT2FM(sys) with each granules in G;
iv. find the minimum distance between the centroid bound and the granules;
v. indicate the status of the node under investigation: Normal-Behavior, Suspicious-Normal-Behavior, Suspicious-Misbehavior, Misbehavior, through identifying the one whose centroid's distance to the centroid of IT2FM(sys) is minimum.

For the sake of security, we designed helper T-cells as a subset of network nodes that cooperate in order to take the final majority decision: well-behaving or misbehaving node. Once got the final decision, if necessary, helper T-cells send to killer T-cells a *stimulatory signal*, for activating the specific-immune response.

6. Conclusions

Nodes of mobile ad-hoc network communicate via wireless links through a decentralized network topology. These networks rely on efficient nodes cooperation among all their member in order to implement a routing protocol. A flexible network topology, that is a consequence of the node mobility, brings with it the well-known problems of regular networks and introduces several new security issues. This makes mobile ad-hoc networks highly vulnerable to attacks and selfish node behaviors, which caused the degradation of routing performance.

In this paper, we have introduced a biologically-inspired interval type-2 fuzzy set based algorithm for detecting misbehaving nodes in ad-hoc wireless networks. The algorithm is inspired by the approximate binding between lymphocytes receptors and epitopes, and it is triggered by network danger signals and antigen presenting cells. In this paper we have propose how to implement the algorithm as AIS recognition engines, for mitigating routing misbehavior without human intervention. We believe that the proposed AIS does not need a preliminary training phase because such phase can introduce noisy data into the system, generating a new source of uncertainty.

The proposed algorithm is based on simple arithmetic/logic operation and does not require specific hardware features. Its strengths can be counted as (i) multilayered – the final decision is based on *M* intervals of confidence, one for each network parameter, that can help the artificial immune system to take under control the number of false positive, (ii) distributed – to take the final decision, i.e. well-behaving or misbehaving node, the recognition algorithm is executed by a number of helper T-cells. On the other hand, possible weaknesses of the algorithm are the necessity to have all the information of the system parameters available in advance, and the difficulty to build a better interval type-2 fuzzy map during the lifespan of the system. These drawbacks could lead to the generation of a static artificial immune system. For these reason, future work will be devoted to improve learning phase of the algorithm.

7. References

[1] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proc. of MOBICOM 2000, 2000.

[2] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", *IEEE Transaction on Mobile Computing,* Vol.6, No.5, 2007, pp.536-550.

[3] A.Visconti, H.Tahayori, "Detecting Misbehaving Nodes in MANET with an Artificial Immune System Based on Type-2 Fuzzy Sets", in Proc. of the 4th International Conference for Internet Technology and Secured Transactions, 2009.

[4] J. Gomez, D. Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection", in Proc. of the 3rd Annual IEEE Information Assurance Workshop, 2002.

[5] J. Gomez, F. Gonzalez, and D. Dasgupta, "An Immuno-Fuzzy Approach to Anomaly Detection", in Proc. of the 12th IEEE International Conference on Fuzzy Systems, 2003.

[6] H.Tahayori, A.Visconti, "Distributed-Interval Type-2 Fuzzy Set Based Recognition Algorithm for IDS", in Proc. of the 2008 IEEE International Conference on Granular Computing, 2008.

[7] J.M. Mendel, *Uncertain Rule-Based Fuzzy Logic Systems: Introduction and New Directions*, Prentice-Hall, Upper-Saddle River, NJ, 2001.

[8] M.B. Lutz, G.Schuler, "Immature, semi-mature and fully mature dendritic cells: which signals induce tolerance or immunity?", *Trends in Immunology*, Vol.23, No.9, 2002, pp.991–1045.

[9] B. Alberts, A. Johnson, J. Lewis, M. Raff, K. Roberts, and P. Walter, *Molecular Biology of the Cell 5th ed.*, Garland Science Publishing, London, 2007.

[10] P Matzinger, "Tolerance, danger and the extended family", *Annual Reviews in Immunology*, Vol.12, 1994, pp.991–1045.

[11] S. Sarafijanovic, and J-Y. Le Boudec "An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors", in Proc. of the 3rd International Conference on Artificial Immune Systems, 2004.

[12] L. Buttyan, J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs", in Proc. of 1st IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing, 2000.

[13] S. Buchegger, J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol", in Proc. of the 3rd ACM International Symposium on Mobile ad hoc networking & computing, 2002.

[14] M. Drozda, S. Schaust, and H. Szczerbicka, "AIS for Misbehavior Detection in Wireless Sensor Networks: Performance and Design Principles", in Proc. of IEEE Congress on Evolutionary Computation, 2007.

[15] J. Greensmith, U. Aickelin and S. Cayzer, "Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection", in Proc. of the 4th International Conference on Artificial Immune Systems, 2005.

[16] J. Kim, W. Wilson, U. Aickelin, and J. McLeod, "Cooperative automated worm response and detetction immune algorithm (cardinal) inspidred by t-cell immunity and tolerance", in Proc. of the 4th International Conference on Artificial Immune Systems, 2005.

[17] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod, "Danger theory: The link between ais and ids", in Proc. of the 2nd Internation Conference on Artificial Immune Systems, 2003.

[18] J. Kim, J. Greensmith, J. Twycross, and U. Aickelin, "Malicious code execution detection and response immune system inspired by the danger theory", in Proc. of the Adaptive and Resilient Computing Security Workshop, 2005.

[19] J. M. Mendel, "Computing with Words and Its Relationships with Fuzzistics", *Information Sciences*, 2007.

[20] N.N. Karnik, J.M. Mendel, "Centroid of a type-2 fuzzy set", *Information Sciences*, Vol.132, 2001, pp.195–220.

[21] H. Wu, J.M. Mendel, "Uncertainty bounds and their use in the design of interval type-2 fuzzy logic systems", *IEEE Transaction on Fuzzy System*, Vol.10, No.5, 2002, pp.622–639.

Appendix A

For calculating the exact bounds $[c_l,c_r]$ of the centroid of the interval type-2 fuzzy set

$$\tilde{A} = \left\{\left(x, \left(1, \left[\underline{u}_{f_i}(x), \overline{u}_{f_i}(x)\right]\right)\right), x \in X, \left[\underline{u}_{f_i}(x), \overline{u}_{f_i}(x)\right] \subseteq [0,1]\right\} = \left\{\left(x, \tilde{\mu}_{f_i}(x)\right), x \in X\right\}$$

Karnik and Mendel have proposed an iterative algorithm (KM Algorithm) [20]. Moreover, Mendel and Wu have proved that the end points of the centroid of an interval type-2 fuzzy set are bounded and have driven formulas for calculating c_l and c_r [21], that is

$$\underline{c_l} \le c_l \le \overline{c_l}$$
$$\underline{c_r} \le c_r \le \overline{c_r}$$

Toward the aim, since FOU is fully characterized by two type-1 fuzzy set, named *Upper Membership Function* (*UMF*) and *Lower membership Function* (*LMF*), and their centroid is defined to be

$$C_{LMF(\tilde{A})} = \frac{\sum_{i=1}^{N} x_i \underline{u}(x_i)}{\sum_{i=1}^{N} \underline{u}(x_i)}$$
$$C_{UMF(\tilde{A})} = \frac{\sum_{i=1}^{N} x_i \overline{u}(x_i)}{\sum_{i=1}^{N} \overline{u}(x_i)}$$

So the bounds would be calculated as

$$\overline{c_l} = min\{C_{LMF(\tilde{A})}, C_{UMF(\tilde{A})}\}$$
$$\underline{c_r} = max\{C_{LMF(\tilde{A})}, C_{UMF(\tilde{A})}\}$$
$$\underline{c_l} = \overline{c_l} - \frac{\sum_{i=1}^{N}\left(\overline{u}(x_i) - \underline{u}(x_i)\right)}{\sum_{i=1}^{N}\overline{u}(x_i)\sum_{i=1}^{N}\underline{u}(x_i)} \times \frac{\sum_{i=1}^{N}\underline{u}(x_i)(x_i - x_1) \;\; \sum_{i=1}^{N}\overline{u}(x_i)(x_N - x_i)}{\sum_{i=1}^{N}\underline{u}(x_i)(x_i - x_1) + \sum_{i=1}^{N}\overline{u}(x_i)(x_N - x_i)}$$
$$\overline{c_r} = \underline{c_r} + \frac{\sum_{i=1}^{N}\left(\overline{u}(x_i) - \underline{u}(x_i)\right)}{\sum_{i=1}^{N}\overline{u}(x_i)\sum_{i=1}^{N}\underline{u}(x_i)} \times \frac{\sum_{i=1}^{N}\overline{u}(x_i)(x_i - x_1) \;\; \sum_{i=1}^{N}\underline{u}(x_i)(x_N - x_i)}{\sum_{i=1}^{N}\overline{u}(x_i)(x_i - x_1) + \sum_{i=1}^{N}\underline{u}(x_i)(x_N - x_i)}$$