In Proceedings of ICARIS-2004 (Third International Conference on Artificial Immune Systems), pp. 342-356,
September 13 - 16, 2004, Catania, Italy.

An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors

Slaviša Sarafijanović and Jean-Yves Le Boudec

EPFL/IC/ISC/LCA,
CH-1015 Lausanne, Switzerland
{slavisa.sarafijanovic, jean-yves.leboudec}@epfl.ch

Abstract. In mobile ad-hoc networks, nodes act both as terminals and information relays, and they participate in a common routing protocol, such as Dynamic Source Routing (DSR). The networks are vulnerable to routing misbehavior, due to faulty or malicious nodes. Misbehavior detection systems aim at removing this vulnerability. For this purpose, we use an Artificial Immune System (AIS), a system inspired by the human immune system (HIS). Our goal is to build a system that, like its natural counterpart, automatically learns and detects new misbehavior.

In this paper we build on our previous work [1, 2] and investigate the use of four concepts: (1) "virtual thymus", a novel concept, introduced in this paper, that provides a dynamic description of normal behavior in the system; (2) "clustering", a decision making mechanism for decreasing false positive detections (3) "danger signal", a concept that is, according to the "danger signal theory" of the human immune system [11, 12], crucial for correct final decisions making; in our case, the signal is exchanged among nodes, which makes our detection system distributed; (4) "memory detectors", used for achieving faster secondary response of the detection system.

We implement our AIS in a network simulator and test it on two types of misbehavior. We do performance analysis and show the effects of the four concepts on the detection capabilities. In summary: thanks to the virtual thymus, the AIS does not require a preliminary learning phase in which misbehavior should be absent; the use of the clustering and the danger signal is useful for achieving low false positives; the use of memory detectors significantly accelerates the secondary response of the system.

1 Introduction

1.1 Problem Statement: Detecting Misbehaving Nodes in DSR

Mobile ad-hoc networks are self organized networks without any infrastructure other than end-user terminals equipped with radios. Communication beyond the transmission range is made possible by having all nodes act both as terminals and information relays. This in turn requires that all nodes participate in a common routing protocol, such as Dynamic Source Routing (DSR) [17]. A problem is that DSR works well only if all nodes execute the protocol correctly, which is difficult to guarantee in an open ad-hoc environment.

A possible reason for node misbehavior is faulty software or hardware. In classical (non ad-hoc) networks run by operators, equipment malfunction is known to be an important source of unavailability [18]. In an ad-hoc network, where routing is performed by user provided equipment, we expect the problem to be exacerbated. Another reason for misbehavior stems from the desire to save battery power: some nodes may run a modified code that pretends to participate in DSR but, for example, does not forward packets. Last, some nodes may also be truly malicious and attempt to bring the network down, as do Internet viruses and worms. An extensive list of such misbehavior is given in [7]. The main operation of DSR is described in Section 2. In our simulation, we implement faulty nodes that, from time to time, do not forward data or route requests, or do not respond to route requests from their own cache.

We chose DSR as a concrete example, because it is one of the protocols being considered for standardization for mobile ad-hoc networks. There are other routing protocols, and there are parts of mobile ad-hoc networks other than routing that need misbehavior detection, for example, the medium access control protocol. We believe the main elements of our method would also apply there, but a detailed analysis is for further work.

1.2 AIS Problems We Are Solving Here

Eliminating need for preliminary learning phase: In our previous work [1, 2] we use a preliminary Artificial Immune System (AIS) operation phase for collecting examples of normal behavior (self). During this phase, misbehavior is absent from the system. This is a drawback of the system for two reasons. First, it is very impractical to provide such a protected environment in a real system. Second, if normal behavior changes over time, the information collected about it in the preliminary phase is not fully adequate. Change of observed normal behavior in our case is caused by changes in traffic and mobility patterns of the nodes. Use of a preliminary learning phase is a common problem of many AISs.

Capability of learning changing self: The human immune system (HIS) becomes self-tolerant to some new antigens produced by the body [12]. We want our AIS to (autonomously) become self-tolerant to changed but normal behavior in the network.

Correct decision making for low false positives: The high false-positives detection rate is a common problem of many AISs, although it seems not to be so with the HIS. High false positives are critical in our system because the aim of detection is to respond; and responding to well behaving nodes could (and should) be observed by other nodes as misbehavior. This could cause instability in our AIS.

Achieving a fast secondary response: We consider the problem of detecting nodes that do not execute the DSR protocol correctly. The actions taken after detecting that a node misbehaves range from forbidding the use of the node as a relay [6] to excluding the node entirely from any participation in the network [8]. In this paper we focus on the detection of misbehavior and do not discuss actions taken after detection. However, the actions do affect the detection function through the need for a secondary response. Indeed, after a node is disconnected (boycotted) because it was classified as misbehaving, it becomes non-observable. Since the protection system is likely to be adaptive, the "punishment" fades out and redemption is allowed [7]. As a result, a misbehaving node

is likely to misbehave again, unless it is fixed, for example by a software upgrade. We call primary [resp. secondary] response the classification of a node that misbehaves for the first [resp. second or more] time; thus we need to provide a secondary response that is much faster than the primary response.

1.3 Our Approach for Misbehavior Detection in DSR

We use an Artificial Immune System (AIS) approach, as it promises to overcome some constraints of traditional misbehavior detection approaches (Section 3.1). We map concepts and algorithms of the human immune system (HIS) to a mobile ad-hoc network and build a distributed system for DSR misbehavior detection. Every node runs the same detection algorithm based on its own observations. The nodes also exchange signals among each other (Figure 1).

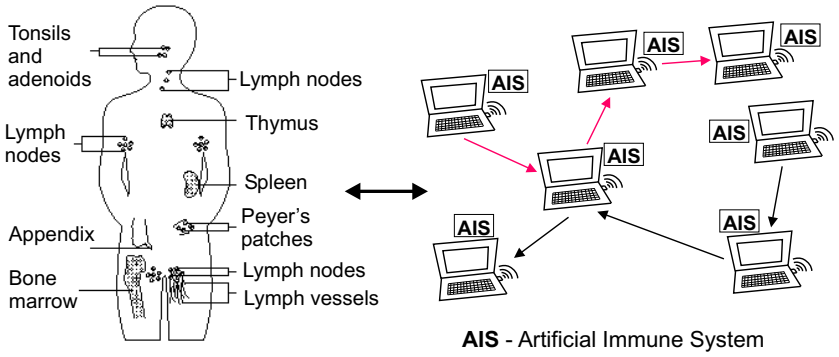


Fig. 1. From the human IS to an AIS: Making DSR immune to node misbehavior.

Our AIS approach and solutions are described in Section 1.4. A detailed description of the detection system components and how it works is given in Section 4.

1.4 Our AIS Approach and Solutions

Dynamic self. Our approach is based on the Danger Signal (DS) model of the HIS [11, 12]. The model can be viewed as a method to protect "dynamic self" in a system. To define "dynamic self" in our system, we extend the notion of self from the behavior specified by the routing protocol (DSR, for example) to any interactive node behavior that does not have negative effects on the normal network trafficking, i.e. does not cause packet losses. As a packet loss, we count any case in which the packet does not arrive at the destination, or the acknowledgment from the destination about receiving the packet does not reach the source, or there is a high delay in any of these packets.

Such a definition of "dynamic self" makes sense, as new interactions that do not cause losses should probably result in some useful traffic, according to the nature of interactions initiated by well behaving nodes. We assume that there are enough nodes that are, for their own reasons (use of the network for own traffic), active in the network

for substantial amounts of time. We neglect the effect of those nodes that are present very briefly in the network in order to use it and then turn off for longer time. The active nodes will be overheard, as well as the routes they belong to (this is possible in DSR, see Section 2), and they will be asked by other nodes to carry traffic on these routes. Within such a definition, self will be dynamically determined through the interaction of nodes and feedback in form of losses in cases when some nodes do not cooperate according to the current established network self.

In the context of the danger signal model of the HIS, the feedback in form of packet losses corresponds strongly to the danger signal generated by cells in a process of necrosis, and there is also notion of the current self; for example, new milk protein antigens produced during pregnancy are tolerated and become current self for the body.

We use three concepts to achieve self-tolerance to possibly changing self, and to eliminate the need for a preliminary learning phase: “virtual thymus”, “clustering” and “danger signal”. To achieve a fast secondary response we use “memory detectors”.

Virtual Thymus Model. “Virtual thymus” is a novel concept that introduce in this paper. It uses the danger signal and provides a dynamic description of the normal behavior in the system.

There are two important assumptions for explaining the role of the thymus in self-tolerance induction, which are part of a thymus model described in the literature on immunology ([13], pages 85-87; [14]): (1) both self and non-self antigens are presented in the thymus; the rules about how antigens can enter the thymus from the blood are unclear; (2) the thymic dendritic cells that present antigens survive for only a few days in the thymus, so they present current self antigens; if a non-self antigen is picked up for presentation during an infection, it will be presented only temporarily; once the infection is cleared from the body, freshly made antigens will no longer present the foreign antigen as self.

We use these two assumptions to build two mechanisms that represent what we call a ”virtual thymus” in our AIS:

(1) Danger signal used for the virtual thymus. In the case of a danger signal based AIS, we can actually decide on the rules that determine which antigens will enter the virtual thymus and be presented in the process of negative selection (antigen represents observed behavior in our AIS; for more details about our AIS see Section 4). For this, we use a danger signal (which is not its standard use). When the danger signal is present, we forbid antigens that could be related to the signal to enter the virtual thymus. The danger signal in our case is a packet loss in the network, experienced by the source of the packet. The signal is then transmitted along the route on which the loss took place. The signal contains the information about time and nodes that are correlated to the loss, and allows us to forbid correlated antigens that could be non-self (observed for a misbehaving node) to enter the thymus. The information is analogous to the information obtained when a dendritic cell samples antigens that are by time and space related to the damage in the body.

In this way we can provide that sampled antigens that are presentated in the virtual thymus are mainly self, and only rarely non-self (there is no guarantee that a danger signal will always be received by a node that samples antigens).

(2) Short time of antigen presentation. We keep collected antigens in the virtual thymus for a time that is finite and short enough to model finite life of thymic dendritic cells and the related effects.

Clustering. Matching between an antigen and an antibody is not enough to cause detection and reaction in the HIS [13, 14]. The clustering of the matches on the surface of an immune cell and an additional danger signal are required for detection. These additional requirements can be viewed as decision making control mechanisms.

We also require more matches between AIS antigens and detectors for the detection, which is analogous to the clustering in the HIS(a detector in our AIS correspond to an antibody in the HIS, for details see Section 4).

Danger signal used for detection control. In the HIS, the danger signal is produced by a necrosis (an abnormal cell death) [11, 12]. The danger signal in our case is a packet loss. We require a danger signal to be related to the observed node's antigens in order to verify the matchings and cause detection (i.e., classification of the corresponding node as misbehaving).

Memory detectors. In the HIS, the antibodies that are useful in the detection of non-self antigens and that receive a danger signal will undergo clonal selection and become memory. They require a small clustering threshold, and do not require the danger signal for detection. Our AIS also has such educated equivalents, called the memory detectors.

1.5 Organization of the Paper

The rest of the paper is organized as follows. Section 2 gives background on DSR. Section 3 describes the related work. Section 4 gives the mapping from the HIS to the detection system for DSR misbehavior detection, description of the detection system components, and a detailed explanation of how the system works. Section 5 gives simulation specific assumptions and constraints, describes experiments used to evaluate separate and joint effects of the system factors to system performance metrics, and gives simulation results and discussion of the results. Section 6 draws conclusions and describes what we have learned and how we will exploit it in future steps.

2 Background on DSR

The dynamic source routing protocol (DSR) is one of the candidate standards for routing in mobile ad-hoc networks [17]. A "source route" is a list of nodes that can be used as intermediate relays to reach a destination. It is written in the data packet header at the source; intermediate relays simply look it up to determine the next hop.

DSR specifies how sources discover, maintain and use source routes. To discover a source route, a node broadcasts a route request packet. Nodes that receive a route request add their own address in the source route collecting field of the packet, and then broadcast the packet, except in two cases. The first case is if the same route request was already received by a node; then the node discards the packet. Two received route requests are considered to be the same if they belong to the same route discovery, which is identified by the same value of the source, destination and sequence number fields in the request packets. The second case is if the receiving node is destination of the route discovery, or if it already has a route to the destination in its cache; then the node sends

a route reply message that contains a completed source route. If links in the network are bidirectional, the route replies are sent over the reversed collected routes. If links are not bidirectional, the route replies are sent to the initiator of the route discovery as included in a new route request generated by answering nodes. The source of the initial route request is the destination of the new route requests. The node that initiates original route request receives usually more route replies, each containing a different route. The replies that arrive earlier than others are expected to indicate better routes, because for a node to send a route reply, it is required to wait first for a time proportional to the number of hops in the route it has as answer. If a node hears that some neighbor node answers during this waiting time, it supposes that the route it has is worse than the neighbor's one, and it does not answer. This avoids route reply storms and unnecessary overhead.

After the initiator of route discovery receives the first route reply, it sends data over the obtained route. While packets are sent over the route, the route is maintained, in such a way that every node on the route is responsible for the link over which it sends packets. If some link in the route breaks, the node that detects that it cannot send over that link should send error messages to the source. Additionally it should salvage the packets destined to the broken link, i.e., reroute them over alternate partial routes to the destination.

The mechanisms just described are the basic operation of DSR. There are also some additional mechanisms, such as gratuitous route replies, caching routes from forwarded or overheard packets and DSR flow state extension [17].

3 Related Work

3.1 Traditional Misbehavior Detection Approaches

Traditional approaches to misbehavior detection [6, 8] use the knowledge of anticipated misbehavior patterns and detect them by looking for specific sequences of events. This is very efficient when the targeted misbehavior is known in advance (at system design) and powerful statistical algorithms can be used [9].

To detect misbehavior in DSR, Buchegger and Le Boudec use a reputation system [8]. Every node calculates the reputation of every other node using its own first-hand observations and second-hand information obtained from others. The reputation of a node is used to determine whether countermeasures against the node are undertaken or not. A key aspect of the reputation system is how second-hand information is used, in order to avoid false accusations [8].

The countermeasures against a misbehaving node are aimed at isolating it, i.e., packets will not be sent over the node and packets sent from the node will be ignored. In this way nodes are stimulated to cooperate in order to get service and maximize their utility, and the network also benefits from the cooperation.

Even if not presented by its authors as an artificial immune system, the reputation system in [8, 9] is an example of (non-bio inspired) an immune system. It contains interactions between its healthy elements (well-behaving nodes) and detection and exclusion reactions against non-healthy elements (misbehaving nodes). We can compare it to the human *innate* immune system ([14, 13]), in the sense that it is hardwired in the nodes and changes only with new versions of the protocol.

Traditional approaches miss the ability to learn about and adapt to new misbehavior. Every target misbehavior has to be imagined in advance and explicitly addressed in the detection system. We use an AIS approach to misbehavior detection as it is promising to overcome these constraints.

3.2 Artificial Immune Systems - Related Work

There are different proposals in the related literature that address the problem of final decision making in AISs. Hofmeyr and Forrest [3] use co-stimulation by a human, which can be viewed as some form of supervised training. Somayaji and Forrest [4] achieve tolerization to new normal behavior in an autonomous way, but their system works only under the assumption that new abnormal behavior always exhibits new patterns that are more clustered than in the case of new normal behavior; if the patterns of a new misbehavior are first sparsely introduced in the system, the system will become tolerant to that misbehavior. Aickelin at all [5] propose the use of the danger signal based on the analogy with the necrosis and apoptosis of the human body cells; with this model, main control signals come from the protected system; the danger signal approach seems to be quite promising for building an autonomous and adaptive AISs.

In our previous work we use a self-nonself model, and define mapping to our AIS. We define representation, matching and the simple use of negative selection and clonal selection algorithms. The system is able to learn normal behavior presented in preliminary training phase and to detect misbehavior afterwards. The drawback is the need for preliminary training phase, and the absence of mechanisms for adaptation to changing self.

For an overview of AIS, see the book by de Castro and Timmis [20] and the paper by de Castro and von Zuben [19].

What is missing in the related literature on AISs is an explicit use of the thymus and a dynamic self presentation; we introduce this concept and incorporate it into a danger signal based AIS.

4 Design of Our Detection System

4.1 Mapping of HIS Elements to Our Detection System

The elements of the natural IS used in our detection system are mapped as follows:

- Body: the entire mobile ad-hoc network
- Self Cells: well-behaving nodes
- Non-self Cells: misbehaving nodes
- Antigen: (AIS) antigen, which is a sequence of observed DSR protocol events recognized in the sequence of packet headers and represented by binary strings as explained in detail in our previous work [1] (representation is adopted from [10]). Examples of events are “data packet received”, “data packet received followed by data packet sent”, “route request packet received followed by route reply sent”.
- Antibody: detector; detectors are binary strings produced in the continuous processes of negative selection and clonal selection; ideally, they “match” non-self antigens (produced by misbehaving nodes) and do not match self antigens.
- Chemical binding of antibodies to antigens: “matching function” between detectors and antigens, as defined in detail in our previous work [1].

– Detection: a node detects a neighbor as misbehaving if the node's detectors match relatively many of the antigens produced by that neighbor (clustering) and if it receives danger signals related to those antigens
– Clustering: clustering of matching antibodies on the immune system cell surface is mapped to the clustering of matches between detectors and antigens in time for a given observed node;
– Necrosis and apoptosis: packet loss
– Danger signal: the danger signal in our framework contains information about the time and nodes correlated with a packet loss
– Antigen presenting cell: transmission of the danger signal
– Thymus: The virtual thymus is a set of mechanisms that provides (as explained in Section 1.4) the presentation of the current self in the system during the continuous negative selection process
– Memory cells: memory detectors; detectors become memory if they prove to be useful in detection; they differ from normal detectors by longer lifetime and lower clustering required for detection.

4.2 How the Detection System Works

The detection system consists of the data and functions shown in the Figure 2, which are present at every node. We explain how the system works by describing a typical series of events at one node. To read this chapter you may need to read first our AIS approach (Section 1.4) and look at the mapping to our concrete problem (Section 4.1).

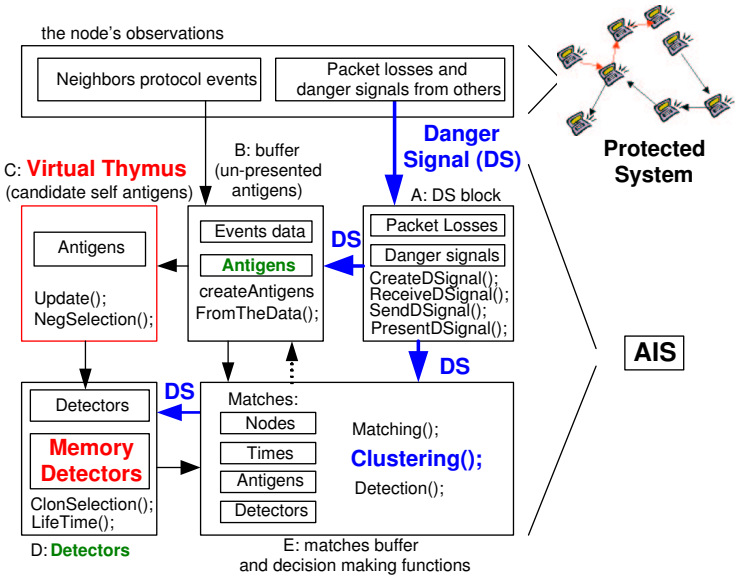


Fig. 2. Components of the detection system.

Observing Antigens. A node overhears the messages exchanged in its neighborhood, during a defined time interval (10s by default), and records separately the routing protocol events of interest (see mapping, Section 4.1) for each of its neighbors. Then it translates the observed data sets into antigens. So, one antigen is created every 10 s for each of the observable neighbors . The antigen represents the behavior of the observed node for the observed time interval.

The collected antigens are buffered (Figure 2, component B) for a time that is greater than the maximum time (64 s by default) needed for the danger signal to be generated and distributed over the route on which a packet has been sent if it got lost. The absence or presence of the danger signal determines whether the related antigen will be presented in the virtual thymus S or not, and whether the matching of the antigens by the detectors will be counted for detection or not.

Generating the Danger Signal. The danger signal is generated by a node when it experiences a packet loss, i.e., when it does not receive an acknowledgment that the packet it sent was received by the destination. The signal is then sent over the route on which the packet loss took place (Figure 3). The signal contains the information about the (approximate) time of the packet loss, and about the nodes on the route over which the lost packet was sent. So, the receivers of the danger signal are able to correlate it with the antigens collected: (1) during the time that is close to the packet loss time; (2) from the nodes that belong to the route on which the loss took place. (There is a strong analogy with the HIS, regarding both the way the danger signal is generated and the information it contains; see Section 1.4.)

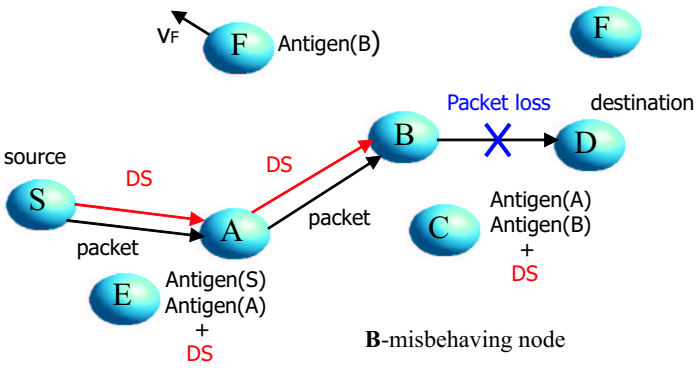


Fig. 3. Generating and transmitting the danger signal: there is packet loss at B; the source S of the packet does not receive the acknowledgment from destination D and sends the danger signal over the route on which the loss took place; the nodes that receive the signal (A,B,C,E) do not present the observed correlated antigens in their thymus; rarely, some nodes (F in this case) move away and do not receive the danger signal, so they present the collected (non-self) antigens.

Virtual Thymus Mechanisms: *(1) Use of the danger signal.* When a node causes a packet loss, it also produces an antigen observable by its neighbors. Most of the neighbors that observe the antigen also receive the corresponding danger signal (Figure 3)

and consequently forbid the (non-self) antigen to enter the virtual thymus (Figure 2, component C). But some of the neighbors will move away from the route over which the danger signal is sent, and not receive the signal, even though they were close enough to collect the non-self antigen at the time of the packet loss; in this case the non-self antigen may enter the virtual thymus. This happens rarely, as the propagation time is relatively short and nodes cannot move very much between a packet loss event and the corresponding danger signal transmission.

Some of self antigens are forbidden to enter the virtual thymus too, as they were generated from the well-behaving nodes that happen to be on the route on which a packet loss took place. As there are always enough other self antigens that are not correlated to the danger signal, this does not affect the self presentation in the thymus.

From the buffered antigens, those that are not correlated with the danger signal are periodically randomly sampled to enter the virtual thymus (one update every 10 sec, by default). Delay caused by buffering the antigens before presentation in the virtual thymus is significantly greater (300 s by default) than the delay for the antigens to be presented for matching by the detectors (70 s by default). This is done on purpose, in order to postpone deleting useful detectors by non-self antigens that accidently enter virtual bone marrow. It would also make sense to check the antigens by memory detectors before letting them to enter the virtual thymus, but this is currently not implemented (a dashed arrow on the Figure 2).

(2) Finite presentation time. An antigen that enters the virtual thymus stays there for a finite time (500 s by default), ensuring that only the current self is presented during the continuous negative selection process.

Producing Detectors. The detectors are produced in the continuous negative selection process in the thymus (Figure 2, component C): new detectors are generated by random and checked if they match any of the antigens from the thymus; only those that do not match survive, leave the thymus, and update the set of current detectors (Figure 2, component D). Whenever a new antigen enters the thymus, first the detectors (but not the memory detectors) from D that match the new antigen are deleted. The memory detectors are deleted only if they match new antigens from C more times than a given threshold (25 by default). Then, the new detectors are generated in the number needed to replace those deleted. The process of continuous negative selection seems to be computationally more feasible, compared to the standard negative selection.

Matching. Antigens that are presented for detection are checked with current detectors, and if any detector matches an antigen one positive matching score is recorded for the corresponding node; otherwise a negative matching score is recorded. Only a finite number of last matches is stored (maximum 30, by default).

Clustering and Detection. Clustering is realized as a function that operates on scored matches between antigens and detectors, and it enables the detection of the related node if there is enough matching evidence. Clustering means that the matches for a considered node are grouped in time.

Assume we have collected n antigens for the monitored node. Let M_n be the number of antigens (among n) that are matched by detectors. Let $\theta_{\max}$ be a bound on the probability of false-positive matching (matching a self antigen) that we are willing to

accept, i.e. the antigens of well-behaving nodes are matched by detectors with a probability that is less or equal than $\theta_{\max}$. We determine a good value by pilot simulation runs ($\theta_{\max} = 0.06$). Let α (=0.001 by default) be the false-positive detection that we target. We detect the monitored node (classify it as misbehaving) if

$$\frac{M_n}{n} > \theta_{\max}(1 + \frac{\xi(\alpha)}{\sqrt{n}}\sqrt{\frac{1-\theta_{\max}}{\theta_{\max}}}) \quad (1)$$

where $\xi(\alpha)$ is the $(1-\alpha)$-quantile of the normal distribution (for example, $\xi(0.0001) = 3.72$). As long as Equation (1) is not true, the node is classified as well-behaving. With default parameter values, the condition is $\frac{M_n}{n} > 0.06 + 0.88\frac{\xi(\alpha)}{\sqrt{n}}$. The derivation of Equation (1) is given in the appendix.

Co-stimulation by the Danger Signal for Detection. Matching by detectors to an antigen require, in addition, the existence of a related danger signal in order the matching to be counted for the detection.

Memory detectors. The detectors that score the detection (verified by the danger signals) will undergo the process of clonal selection: they are cloned, mutated and (which is not the case in the HIS) checked by negative selection once more. As the maximum number of memory detectors is constrained (50), only those with the best detection score are kept. Matches with memory detectors require less clustering for detection (implemented using a larger value of α, 0.2 by default).

5 Performance Analysis

5.1 Analyzed Factors and Experiments

We analyze the effects of: substitution of the preliminary learning phase by the virtual thymus; clustering; use of the danger signal; use of memory detectors. We first compare the preliminary learning phase versus the virtual thymus. Then we add other components to the solution with virtual thymus and follow the effects onto performance metrics.

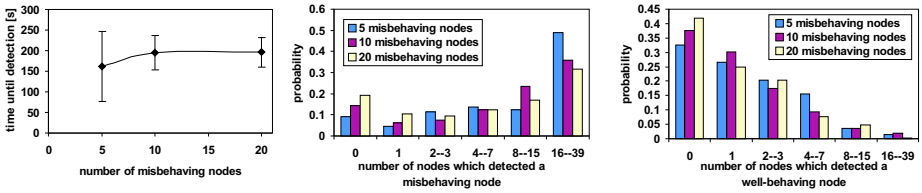
5.2 Performance Metrics

The metrics we use are: (1) time until detection of a misbehaving node; (2) true-positive detection, in form of the distribution of the number of nodes which detect a misbehaving node; (3) false-positive detection, in form of the distribution of the number of nodes which detect a well-behaving node. The metrics are chosen from a reputation system perspective; we see the use of a reputation system [7] as a way to add a reactive part to our AIS.

5.3 Description of Simulation

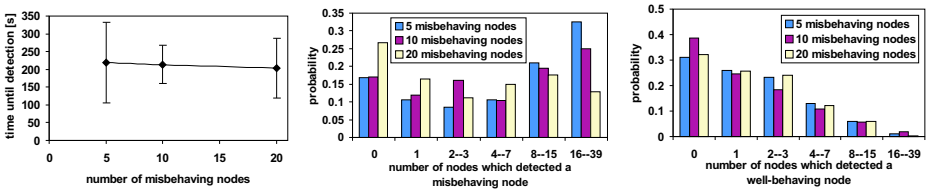
The simulation is done in Glomosim network simulator [15]. The simulation code is available on the Internet [16]. There are 40 nodes, 5-20 nodes are misbehaving. Mobility is the random way point, speed is 1m/s, without pauses. The simulation area is 800x1000 m, and the radio range is 355 m. A node that misbehaves does not forward the packet or does not answer or forward route request messages; this happens with a given probability (0.6 by default) that is also a parameter.

5.4 Simulation results



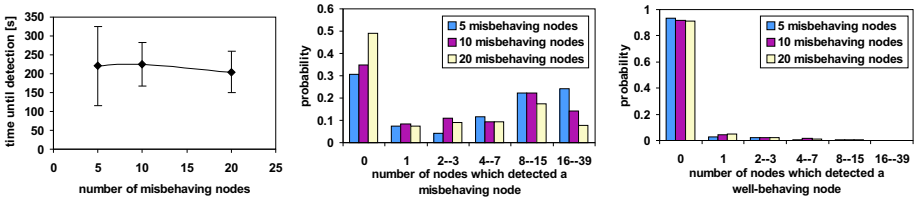
(a) (b) (c)

Fig. 4. Use of the preliminary learning phase: (a) time until detection, (b) correct detections and (c) misdetections.



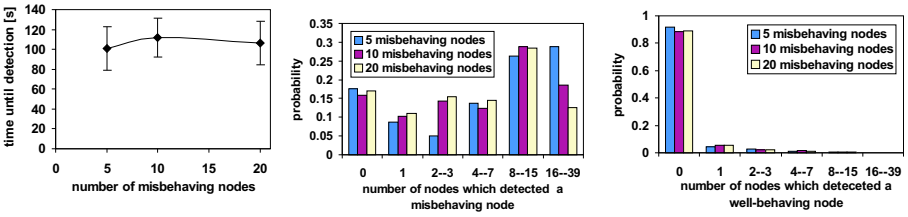
(a) (b) (c)

Fig. 5. Use of the virtual thymus instead of the preliminary learning phase: (a) time until detection, (b) correct detections and (c) misdetections.



(a) (b) (c)

Fig. 6. Use of the danger signal for detection decision making: (a) time until detection, (b) correct detections and (c) misdetections.



(a) (b) (c)

Fig. 7. Use of memory detectors: (a) time until detection, (b) correct detections and (c) misdetections.

The virtual thymus versus the preliminary learning phase: Form the Figures 4 and 5 we see that the preliminary learning phase can be successfully substituted by the virtual

thymus. Time until detection and the false positives are similar in both cases, while the false negatives are slightly worse in the case with the virtual thymus.

The danger signal used for detection decision making has a large impact in decreasing false positives (Figures 6(c) and 7(c)).

The use of the memory detectors significantly decreases the time until detection (Figure 7(a)), and also improves true-positive detection (Figures 6(b) and 7(b)).

6 Conclusions, Discussion and Future Work

From the obtained results we conclude that the examined mechanisms: the virtual thymus, the danger signal and the use of memory detectors can be succesfuly applied for our problem. Moreover, we see "virtual thymus" not only as a solution for eliminating need of the preliminary training phase in our system, but also as a standard component in building the danger signal based AISs.

We do not show here the impact of the clustering separately, because of the lack of the space and because we have shown already in our previous work [1, 2] that it has a large impact in both decreasing the false positives and increasing the true positives, but with a cost of longer time until detection; the increase in the time until detection is here partially compensated by the use of the memory detectors.

We did not compare the preliminary learning phase versus the virtual thymus in a case of dynamic self behavior. As the AIS with the virtual thymus collects and presents current self behavior for producing detectors, we expect that, in a dynamic case, this solution will have better performance than the AIS with preliminary learning phase.

Next step in completing our AIS would be adding its reactive part. With a reactive part, it is important to distinguish between a misbehavior and a reaction against a misbehaving node. This may require the information exchange between the nodes. We see the use of a reputation system a possible solution [7]. Here we have shown that the number of nodes that detect a misbehaving node is statistically considerably larger than the number of nodes that miss-detect a well behaving node (Figures 7(b) and 7(c)). This result gives a promise for a successful use of a reputation system within our AIS.

Our future work also includes testing the scalability of our solution with respect to the number of misbehavior types, as well as a more detailed analysis of the impact of system parameters on the detection capabilities.

References

1. J. Y. Le Boudec and S. Sarafijanovic. An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-Hoc Networks. Proceedings of Bio-ADIT 2004, Lausanne, Switzerland, January 2004, pp. 96-111.
2. S. Sarafijanovic and J. Y. Le Boudec. An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile Ad-Hoc Networks. TechReport IC/2003/65, EPFL-DI-ICA, Lausanne, Switzerland, November 2003.
3. S. A Hofmeyr and S. Forrest "Architecture for an Artificial Immune System". Evolutionary Computation 7(1):45-68. 2000.
4. A. Somayaji and S. Forrest "Automated Response Using System-Call Delays." Proceedings of the 9th USENIX Security Symposium, The USENIX Association, Berkeley, CA (2000).
5. Aickelin, U., Bentley, P., Cayzer, S., Kim, J. and McLeod, J. (2003) Danger Theory: The Link between AIS and IDS? In Timmis, J., Bentley, P. J. and Hart, E. (Eds) Proc of the

Second International Conference on Artificial Immune Systems (ICARIS 2003). Springer LNCS 2787. pp. 147-155.
6. Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of MOBICOM 2000*, pages 255–265, 2000.
7. S. Buchegger and J.-Y. Le Boudec. A Robust Reputation System for Mobile ad hoc Networks. Technical Report, IC/2003/50, EPFL-DI-ICA, Lausanne, Switzerland, July 2003.
8. S. Buchegger and J.-Y. Le Boudec. Performance Analysis of the CONFIDANT protocol: Cooperation of nodes - Fairness In Distributed Ad-Hoc Networks. In *Proceedings of MobiHOC, IEEE/ACM*, Lausanne, CH, June 2002.
9. S. Buchegger and J.-Y. Le Boudec. The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks. In *Proceedings of WiOpt '03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, Sophia-Antipolis, France, March 2003.
10. J. Kim and P.J. Bentley. Evaluating Negative Selection in an Artificial Immune System for Network Intrusion Detection: *Genetic and Evolutionary Computation Conference 2001* (GECCO-2001), San Francisko, pp. 1330-1337, July 7-11.
11. P. Matzinger. Tolerance, Danger and the Extended Family. *Annual Review of Immunology*, 12:991-1045, 1994.
12. P. Matzinger. The Danger Model in it's Historical Contex. *Scandinavian Journal of Immunology*, 54:4-9, 2001.
13. L.M. Sompayrac. How the Immune System Works, 2nd Edition. Blackwell Publishing, 2003.
14. Richard A. Goldsby, Thomas J. Kindt, Barbara A. Osborne, Janis Kuby: Immunology, 5th edition, W. H. Freeman and Company, 2003.
15. Xiang Zeng, Rajive Bagrodia, and Mario Gerla. Glomosim: A library for parallel simulation of large scale wireless networks. *Proceedings of the 12th workshop on Parallel and Distributed Simulations-PDAS'98*, May 26-29, in Banff, Alberta, Canada, 1998.
16. Simulation code: http://lcawww.epfl.ch/ssarafij/ais-code
17. D.B. Johnson and D.A. Maltz. The dynamic source routing protocol for mobile ad hoc networks. *Internet draft, Mobile Ad Hoc Network (MANET) Working Group*, IETF, February 2003.
18. G. Iannaccone C.-N. Chuah, R. Mortier, S. Bhattacharyya, C. Diot. *Analysis of Link Failures in an IP Backbone*. Proceeding of IMW 2002. ACM Press. Marseille, France. November 2002
19. De Castro, L. N. and Von Zuben, F. J. (1999), Artificial Immune Systems: Part I Basic Theory and Application, Technical Report RT DCA 01/99
20. Leandro N. de Castro and Jonathan Timmis, Artificial Immune Systems: A New Computational Intelligence Approach, Springer Verlag, Berlin, 2002

Appendix: Derivation of Equation (1)

We model the outcome of the behavior of a node as a random generator, such that with unknown but fixed probability θ a data set is interpreted as suspicious. We assume the outcome of this fictitious generator is iid. We use a classical hypothesis framework. The null hypothesis is $\theta \leq \theta_{\max}$, i.e., the node behaves well. The maximum likelihood ratio test has a rejection region of the form $\{M_n > K(n)\}$ for some function $K(n)$. The function $K(n)$ is found by the type-I error probability condition: $\mathbb{P}\{M_n > K(n)\}|\theta) \leq \alpha$, for all $\theta \leq \theta_{\max}$, thus the best $K(n)$ is obtained by solving the equation

$$\mathbb{P}(\{M_n > K(n)\}|\theta_{\max}) = \alpha$$

The distribution of M_n is binomial, which is well approximated by a normal distribution with mean $\mu = n\theta$ and variance $n\theta(1-\theta)$. After some algebra this gives $K(n) = \sqrt{n}\xi\sqrt{\theta_{\max}(1-\theta_{\max})} + n\theta_{\max}$, from which Equation (1) derives immediately.