Immune Inspired Approach for Securing Wireless Ad hoc Networks

Yasir Abdelgadir Mohamed **Azween B. Abdullah**

Department Of computer and Information Science, University Technology PETRONAS, Tronoh, MALAYSIA

Summary
New computational techniques are being developed based on the immune system concepts, seeking to solve several engineering problems. Moreover, mobile ad hoc networks (MANETs) have no clear line of defense and no fixed infrastructure; therefore, the known security techniques used for cabled networks might not work perfectly. A security approach based on immune inspired properties and features is presented. Mobile agent system has been used so as to map different immune components that collaborate to defend the human body against different kinds of diseases. Distributed detection, first response, second response, self recovery, adaptability, and danger theory representation are the hallmarks of the proposed security approach which places emphasis on infrastructure less and high nodes mobility capabilities.

Keywords:
Security, MANETs, immune system, Mobile agent.

1. Introduction

Due to unique characteristics of mobile ad hoc networks, nontrivial challenges could be posed to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology. These challenges clearly make a case for building distributed security solution that achieves both broad protection and desirable network performance. The dynamically changing topology poses different vulnerabilities, likewise, the absence of conventional security infrastructures and the open medium of communication. Attacks against routing protocol, attacks that aim at exhausting resources of other nodes in the MANET, and cooperative attacks where malicious nodes cooperate with other to cause harm, are some of the MANETs vulnerabilities.

On the other hand, the use of artificial immune systems in solving security problems is an appealing concept for two reasons. Firstly, the human immune system provides the human body with a high level of protection from invading pathogens, in a robust, self-organized and distributed manner. Secondly, current techniques used in computer security cannot cope with the dynamic and increasingly complex nature of ad hoc networks and their security [1]. The researchers hoped that biologically inspiration, including the use of immune-based systems will be able to bridge the gap.

Many attempts have been made to map peptide, protein, epitope, receptor, monoclonal lymphocyte, and antibody (B-cell, T-cell) using binary string and detectors with a variable region of detector string in a computer system[2], [3]. These attempts established the basic concepts in biologically inspirations. Protecting static data, protecting active processes on a single host, protecting a network of mutually trusting computers, and protecting a network of consistently trusting disposable computers are some of the possible outcomes of mapping. Constructing security mechanisms for mobile ad hoc networks challenged with the fact of resources lack, decentralization, mobility, and distributability [4].

This work is expected to contribute to a current state of the art in the wireless security field by presenting an extra mechanism to secure such networks by mapping and applying human immune mechanisms. Auto detection, memory mechanism, self node blocking, and self-recovery are some of the expected properties that the model can accomplish.

The paper is organized as follows: section 2 discuss the related work, section 3 and the subsections presents a model for securing mobile ad hoc networks followed by the conclusion and the future work.

2. Related work

The work in [5] proposed a mechanism to detect unauthorized and compromised nodes in mobile ad hoc networks, which based on zero knowledge techniques. Two-phase detection procedure of nodes that are not authorized is presented. Authentication mechanism to determine the node' identity and an agent that embedded to all nodes, knows the user's standard profile, record deviations gather and analyze and audit data locally, and pass a confidence interval to the neighbor. Not all the immune properties from the proposed model can be

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

assured. The model can be used as an additional security level to mimic the multi-level security defense that takes place in the human immune system.

Furthermore, the researchers in [6] extended their prior work on mobile ad-hoc networks [7] and [8]. They came up with an approach influenced by the idea of the danger theory and chose to look upon a packet loss in the network as a danger signal. In their system, the danger signal is used to stop the relevant antigens entering the Negative Selection (NS) process. The sequences of protocol events are composed in two positions: at the nodes belonging to the route where the packet loss is observed, and throughout the time on the point of the packet loss time. Consequently, they are considered as non-self antigens. These non-self antigens are not passed to the detector generation process of the NS algorithm. In addition, danger signals are used as co-stimulation signals confirming successful detection through a detector, with good performing detectors becoming memory detectors. Their experiments were carried out on the Glomosim network simulator, where 5-20 nodes, as cited, misbehaved among a total of 40 nodes. The reported test results were, firstly, that the use of danger signals strongly impacted on the reduction of false positive error rates, consequently, helps in system adaptability, and secondly that the addition of memory detectors also improved detection rates.

In [9], a hybrid model for network intrusion detection that combines artificial immune system methods with conventional information security methods has been presented. The Network Threat Recognition with Immune Inspired Anomaly Detection, or NetTRIIAD, model is divided into an Innate Layer and an Adaptive Layer. The first layer conducts the external data collection as well as synthesizing the antigens from the observed packets. The danger model is applied through observing the networks events and states. Innate layer provide the antigens' classification. Two features are included in the NetTRIIAD antigen, address features (32 bits) and protocol features (32 bits). The features are derived from IPv4, TCP, and UDP protocols. The danger model signal in NetTRIIAD includes two elements: single feature value and signal level value.

In [10], the advantages of agent based model, coupled with nature based models such as artificial immune systems, an artificial immune and agent based intrusion detection model for large computer networks is introduced. The presented solution is based upon several security levels; event based model and a simple computational abstraction where an anomaly detection technique is designed to monitor the users' registrations to the operational targeted system. The events' generation model is processed using the UNIX system login tool, the events' analysis using the Log check tool, while the activities of the users and the execution of the both reactive and pro-active events' activities are implemented within an artificial immune and mobile agent based infrastructure. In [11] a combination of biologically and socially inspiration approach is presented to mitigate ad hoc network threads. A biological technique has been used for distribution of attack related information and updating, where the attack level itself is socially inspired. Two layer model for communication between nodes adopted in the architecture; a service usage layer and trust management layer. Four types of interfaces happen in the architecture: nodes interact to use services on each other, nodes may choose to locally monitor service usage by other nodes, and relevant events are sent from the node to its access controller to allow access protections to be updated, possibly in reaction to suspicious activity. The third type of interfaces is between the access controllers themselves when they decide to share trust information ("trust updates") with each other. Finally, an updated trust measure computed by the access controller is fed back to the service usage engine in the form of updated access rules.

Forrest and Hofmeyr presented a valuable work in intrusion detection area [12]. They involved the development of AIS for network intrusion detection, called LYSIS which examines TCP connections, classifying the normal connections as self while the abnormal as nonself. It extracts the data path triple which is source host IP, destination host IP, and TCP service, however, the limited input data suggests that future research may be necessary to evaluate whether LYSIS is able to detect more diverse intrusions. Furthermore, mobile detectors and a replica of detectors not discussed although it would ensure the robustness of signature-based detection in the distributed system, as cited.

Different work had been done in [13] in 2006, an approach presented to detect and isolate malicious hosts for mobile ad hoc networks. The DIMH (Detect and Isolate Malicious Host) method is an attempt to provide the integrity and authentication mechanism for routing information. The preconditions for DIMH model is, firstly, the existence of a key management center that saves the public key and other information of the host, secondly any host can request public key of other hosts from key management center, and lastly, the DIMH-request; DIMH-confirm; and DIMH-ack messages are forwarded by broadcast in ad hoc domain. A time set to the message so as to be forwarded or processed since TTL not equal to zero.

Anil Somayaji [14] made an overview on biologically inspired approaches, recapitulated that the existing work had borrowed very few ideas from the immune system diversity and homeostasis. A negative selection model, diversity, and danger theory mostly influenced the obtainable computer security technologies.

3. Security framework

Below, we initially analyze our previous model, and then come to the modified one, comparing both in some standards.

3.1 Prior work

As a prior version to this work [15], four agents have been proposed to secure the ad hoc network domain; two are static whereas the others are mobile. The static ones are so called manager and monitor agents. Replicate agent and recover agent are the mobile ones. These agents communicate and organize with each other to carry out the security mission. Using the proposed agents hypothesized a node in the ad hoc network acts as a master of domain based on relevant capabilities. A management method for dynamically changes the role of a node to act as a server has been left to be specified later. The rest of nodes perform generally as expected in the mobile ad hoc network. An essential component of the architecture is the database that updated consistently in monitor agent on each node and imitates the memory cells that help in the second response reaction in the immune system. Fig.1 depicts the agents' collaboration as declared there in the reference cited above.

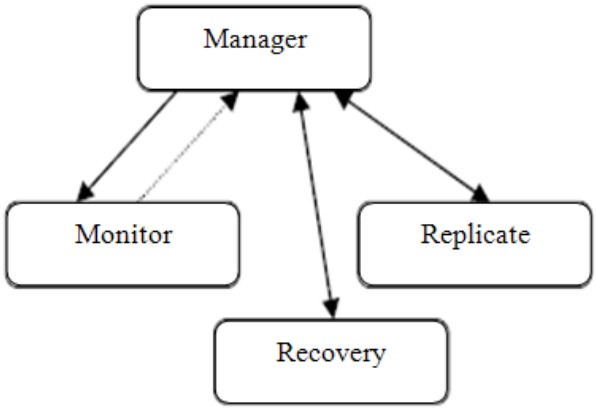

Fig.1. Multi-agent Security system

3.2 The new framework

While modeling the old model, many problems had floated out. The main issues are bandwidth, scalability, and complexity. One of the most outstanding characteristic of mobile ad hoc networks is scarce and variable bandwidth. This makes it essential that any system must impose a very little traffic overhead on the network. On the other hand it is necessary to achieve reliable scalability to gather and analyze the high-volume of audit data correctly from distributed hosts that have a high mobility nature.

Applying the previous model to the network obviously imposes much overhead by occupying most of the bandwidth with control data and messages transmitted between agents reside on different nodes inside the domain. Moreover, the previous model assumes that the manager agent must be aware when a connection is being established between two nodes inside the domain; however, this is not always the case concerning the MANETs nature. Decentralization and node instability are the key features in mobile ad hoc networks. As the same nature exists in the immune system (IS), the assumption above considered as a drawback that affects the whole system capabilities. Furthermore, depending on a system which has a centralized feature in a decentralized nature may directly influence the system scalability which in turn negatively evaluates the system.

So because of MANET nature, and since bandwidth is inadequate (exactly when unicasting), there may not be a centralized unit particularly when two nodes initiate a connection with no need for internet services, or a group through access point (AP), the scenario that proposes four agents collaborate together may cause many problems and may seems has some complexity when practically implemented.

Instead of using many agents, the task of some agents has been represented by multi-rolled agent that is labeled as Immune Agent (IA). The new agent resides on the basic node in the domain and a replica of this IA will be sent to other incoming nodes during new connections establishment.

In an attempt to synchronize the immune components, three profiles will be created:

- Genes Profile. This profile contains the necessary and frequently occurring events for the connection establishment, similar to self cells in the immune system.
- Detectors profile. This similar to the T-cells in the human body which are responsible for distinguishing the nonself so as to be eliminated.
- Nonself profile. It contains the events that harm the system. Realizing these events assures the proper treatment in the future.

Similar to the thymus and bone marrow which are the typical environments in the immune system where the detectors trained, a controlled environment for creating the different profiles in our security approach is established. Fig.3 below depicts the different environments, processes, and components that map the immune system to the security approach. It is shown that the secured, less secured, and application are the different environments where the different profiles created. The profiles' update is a continuous process to ensure the proper future treatment.

3.3 Genes Generation

The security process starts with this object. The essence of the immune system is the ability to differentiate the self from others, subsequently, the detectors generated and maturated to bind to the nonself. Simulating this process and in a high protected environment similar to *thymus* in the immune system, the IA properly configured and trained to monitor and captured the packets that transfer after establishing the connection between two controlled nodes.

The IA captures and stores the frequently and necessary repeated sequences within the protocols header (i.e. sync, TTL, port number, source address, destination address…etc). Let $U = S_f \cup N_f$ represents the set of all patterns monitored while packets transfer, it contains both self and nonself patterns while $S_f \cap N_f$, $N_f = \{n_{f1}, n_{f2...} n_{fm}\}$, $S_f = \{s_{f1}, s_{f2...} s_{fn}\}$ represents the set of all self and nonself patterns the IA captures during the monitoring and capturing phase. The output of the phase as depicted in Fig.3 is a profile that contains all the self S_f that is an essential element for generating the detectors in next object.

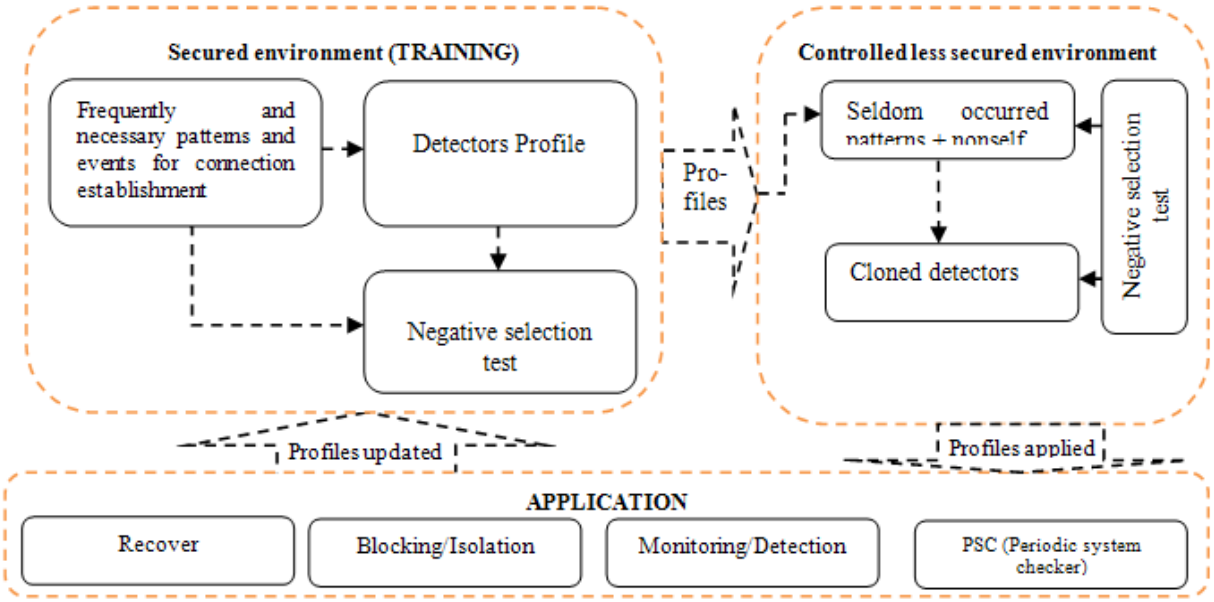

Fig.2. Security architecture

3.4 Generating the Detectors

The adaptive immune system has a lymphocyte cells circulating through the body in the blood, functioning as small detectors binding just to nonself patterns. Simulating the lymphocytes, the IA will be equipped with detectors that are randomly generated. Let $Đ = \{d_1, d_{2...} d_m\}$ represents the set of the generated detectors, $Đ' = \{d'_1, d'_{2...} d'_m\}$ the successfully maturated detectors.

For each of the detectors in $Đ'$ to be *maturated* so as to be able to detect nonself patterns, it must apply to *negative selection* test where it either deleted or successfully selected as a detector. So for detector d_i to be maturated:

If $d_i \; ! \in S_f$ *and* d_i *doesn't match* $s_i \; || \; 1 \le I \le m$

Then $d_i = d'_1$;

$Đ' = Đ' + d_i$;

The negative selection algorithm insures that the selected detectors shall not match with self which may cause a serious system internal collapse, this similar to autoimmune disorders in immunity. A detector d_i will be a pattern with fixed length, same as the genes length, matching could be accomplished using contiguous bit matching rule, same as done by Forrest and Hofmeyr [12] for conventional networks and particularly for TCP packets, the dissimilarity here is the different protocols we already have in ad hoc other than TCP. One of the limitations cited there is that the intrusions can engage network traffic at different protocol layers such as UDP.

3.5 Detectors cloning

Clonal selection is the complementary to the role of negative selection. It explains how an immune response is mounted when a non-self antigenic pattern is recognized

by a specific type of cells labeled as B-cell [16]. The B-cells are proliferated when its receptors bind to pathogens scoring high affinity. The same concept is mapped to our model by setting a score for the detectors, a detector will be cloned when it attain the score in detecting certain number of nonself. The cloned detectors applied again to the negative selection mechanism; each of the cloned detectors matched with Genes in the GeneProfile, success detectors join the DetectorsProfile and the failed ones deleted. The process can be explained in the following format:

Let: $d'_{i\ score} = 0$

For $N_f = \{n_{f1}, n_{f2...} n_{fm}\}$*; bind* d'_i to n_{fj}, *(for i, j=1,2...,m);*

If d'_i *detects* n_{fj}, *then* $d'_{i\ score}$++; *end if*

While $\{d'_{i\ score} \geq max_{\ score}\}$ *do*

clone d'_i // *proliferation phase*

$d'_i = d''_i$;

If d''_i *match* s_{fi} *;(* $1 \leq i \geq n$*); then delete* d''_i;// *negative selection test*

Else $Đ' = Đ' + d''_i$ // *Update the DetectorsProfile*

The different steps including the profiles creations are depicted in Fig.3 below. The Figure is colored Petri Net flow that depicts the different states (A to I) and transitions proposed to formalize the security approach.

3.6 Periodic system check

The human immune system responds to certain danger signals created according to cellular necrosis, the unanticipated stress and/or death of a cell. Necrotic alerts could be produced for a more serious attack where significant system damage was taking place. Using danger theory concept [17], [18], some limitations that came up with prior works can be settled, such as events that may appear as a legitimate at some times and illegitimate at another. In our approach, the IA saves a replica of data necessary for recuperating the node in case of failure. This process takes place the instant the IA gets attached to the host node. Considering the system β as a set of components at time *t*: $\beta_t = \{\beta_1, \beta_{2...} \beta_n\}$ Since a copy of β_t is already saved in the IA database, a change in the system components straightforwardly can be recognized.

Let ε be a type of alter that may possibly crop up to a system according to an effect of an exact pattern(s), so after the transmission completes (after Δt), IA can check the system:

If $\beta\hat{}_{t+\Delta t} = \beta \pm \varepsilon$;

Since ε is not categorized (i.e. $\varepsilon\ !\in S_f$ && $!\in N_f$) it will then be considered as a suspected pattern and will be added to suspect patterns set (S*p*):

$Sp = + \varepsilon$;

But since ε affects negatively in β components, it will then considered as a nonself pattern and consequently switched to the nonself set:

$N_f = N_f + \varepsilon$;

Consequently ε will be blocked/ ignored in future.

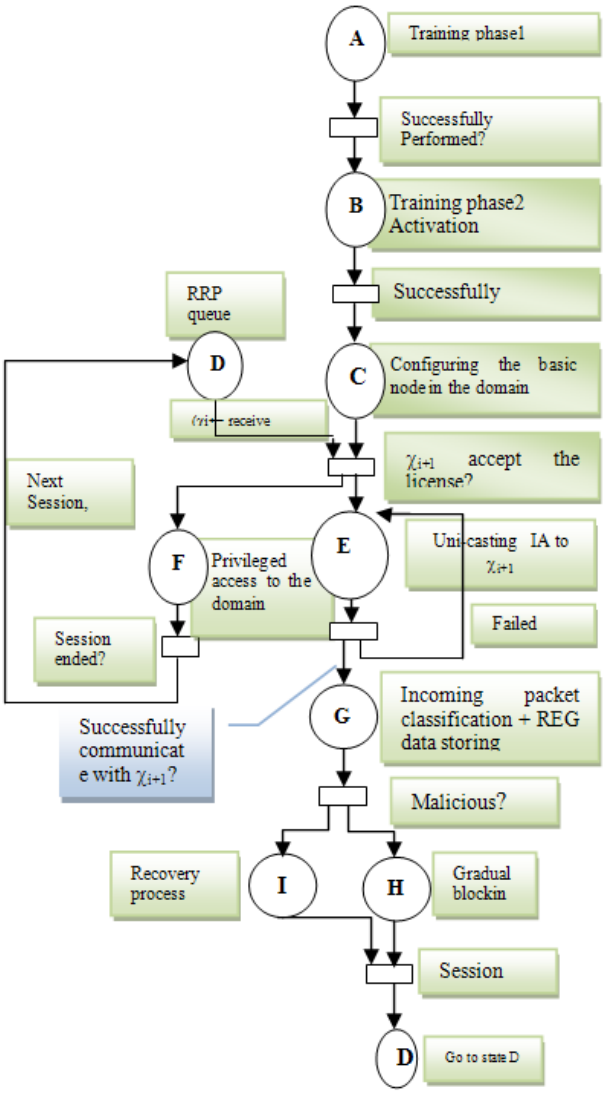

Fig.3. Security Framework states

The approach is premeditated to detach between the two terms, detection and classification. A node that participates in a transmission will be detected when sending a malicious packet but will not classified at once as a malicious node. Classification comes to pass according to a threshold value which set to the number of attacks issued for each node; thereafter the node that exceeds the threshold will be blocked/ ignored when it tries to participate in a transmission.

3.7 Locating the Immune Agent

Scalability is an important issue in designing detection systems [19]. Since MANETs are infrastructure less networks, a centralized server that controlling services

might not be practical. In our approach there is no need for central unit to distribute the security system. For a domain Ɗ that has a set of nodes $\{\delta_1\ \delta_2 ...\ \delta_n\}$, assume that node χ_i has the IA, either installed by user or obtained a copy distributed by the adjacent node. When node χ_{i+1} intend to join the domain group it should firstly broadcast RRP (route request packet in routing on demand protocols) so as to discover the route to a particular destination. This route request contains the address of the destination, beside the source node address and a unique identification number [20]. If the node that receives request already has a copy of IA it adds its own address to the route record of the packet along with a copy of the IA and then forwards the packet along its outgoing links. The process can be specified as follows:

CS:$\chi_{i+1} \rightarrow$ RRP

(Node χ_{i+1} sends route request packet to find a path)

CS: $\forall\ \chi\ \exists\ \chi_i$ (IA)

(*In the domain there exists a node, in which, the IA is installed*)

CS: $\chi_i \leftarrow$ (REP+ IALCS)

(Responds with route path and a license of accepting IA)

CS: $\chi_{i+1} \Leftarrow$ (IALCS) *:(Accepts license)*

CS: χ_i (DA, SA, UI, IA) $\rightarrow \chi_{i+1}$

(Reply (destination address, source node address, unique identification number, and the IA)

Enforcing IA in route reply packet ensures the scalability. Conversely, for the node that intends to disjoin the domain, IA is set to uninstall autonomously as soon as the connection to the ad hoc domain terminated. This certifies IA's safety and not to be abused by malicious and unauthorized nodes. IA deactivation as well solves instability problem; i.e. a node that possibly plays a good role in a time but become malicious in another. When the same node intends to join the domain next time, it receives a copy of IA again from the neighboring node inside the domain; the new copy is memory updated and positively contains last versions of profiles.

As known and according to some ad hoc protocols standards, a difficult evaluation may take place since the nodes still have to share the bandwidth despite the far distance in between [21]. As described above, the previous model consumes most of the bandwidth while sending control data (multi-agents). The new model conserves the bandwidth by locating all tasks of agents in one multi-roles agent.

4. Conclusion and future Works

An immune-based approach for securing MANETs has been presented. In this approach, an Immune Agent (IA) contains three profiles, Gene's profile, nonself profile, and Detectors profile is proposed. Replicas of the (IA) are distributed to nodes when connections established within a domain. A combination of Negative selection, clonal selection, and danger theory mechanisms has been mapped, expecting a self-organized system could be accomplished. The framework attempts to derive a comprehensive security mechanism that can implement the immune system's features effectively. As shown, the framework resolves some limitations early appeared in the previous works including our prior model. The major well thought-out issues are scalability and the bandwidth conserving, which mainly characterize the ad hoc networks. We plan, as a future work, to design an immune-based protocol to secure mobile ad hoc network most typically to what immune system does to keep the body protected.

References

[1] A. Somayaji. S. Hofmeyr and S. Forrest (1998). "Principles of a Computer Immune System." In 1997New Security Frameworks Workshop, ACM1998, pp75-82.

[2] Stephanie Forrest, Steven A. Hofmeyr, and Anil Somayaji, "Computer Immunology", communication of the ACM, Vol. 40, No. 10,1997, pp. 88-96.

[3] S. Forrest, J. Balthrop, M. Glickman and D. Ackley (2002). "Computation in the Wild." In the Internet as a Large-Complex System, edited by K. Park and W. Willins: Oxford University Press. July IS, 2002.

[4] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of MOBICOM 2000, pp. 255.265.

[5] Nikos Kominos, Dimitris Vergados, and Christos Douligeris, "Detecting Unauthorized and Compromised nodes in mobile Ad hoc networks", Elsevier, 2007, pp. 289-298.

[6] S. Sarafijanovic and J. Le Boudec, "An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal and memory detectors", 2004, pp. 342- 356.

[7] J. Le Boudec and S. Sarafijanovic, "An artificial immune system approach to misbehavior detection in mobile ad-hoc networks", Technical Report IC/2003/59, École Poly technique Féderalé de Laussane (EPFL), 2003.
[8] Sarafijanovic, S., Le Boudec, J.Y.: An artificial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks. IEEE Transactions on Neural Networks 16(5) (September 2005).
[9] Robert L. Fanelli, "A Hybrid Model for Immune Inspired Network Intrusion Detection", 2008, Springer journal, pp. 107–118.
[10] S. Forrest, S. Hofmeyr, A. Somayaji, and T. Long staff., A sense of self for UNIX processes, In Proceedings of the 1996 IEEE Symposium on Computer Security and Privacy. IEEE Press, 1996.
[11] Jimmy Mcgibney , Dmitri Botvich, Sasiharan Balasubramanimam, A combined biologically and Socially inspired protocol to mitigating threads in Mobile Ad hoc Networks, 2007.
[12] S. Hofmeyr and S. Forrest, "Architecture for an Artificial Immune System", Evolutionary Computation Journal Vol. 8, No. 4, (2000), pp. 443-473.
[13] Zheng You, Jian Wang, "DIMH: A novel model to detect and isolate malicious hosts for mobile ad hoc networks", Elsevier, 2006, pp. 660-669.
[14] Anil Somayaji, future of biologically inspired computer defenses, information security technical report 12 (2007) pp.228-234.
[15] Yasir A. Gadir, Azween B. Abdullah, Security Mechanism for MANETs, Journal of Engineering and Science Technology, 2008, pp. 231-242.
[16] L. N. De Castro and F. J. Von Zuben, "Artificial immune systems: Part I basic theory and applications", Tech. Rep. RT DCA 01/99, 1999.
[17] Aickelin U., Bentley P., Cayzer S., Kim J. and McLeod J., 2003, 'Danger Theory: The Link between AIS and IDS?' in Proceedings ICARIS-2003, 2nd International Conference on Artificial Immune Systems, 147-155.
[18] Aickelin U, Green smith J, Twycross J. Immune system approaches to intrusion detection – a review. In: LNCS, Springer, 2004. pp. 316–29.
[19] Karen Scarfone, Peter Mell, Guide to Intrusion Detection and Prevention Systems, NIST special publications,Feb.2007,pp.1-127.
[20] Elizabeth M. Royer, A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, 1999, pp. 46-55.
[21] Claude chaudet, Oliver Festor, Isabelle Guerin, and Radu State, A managed Bandwidth Reservation Protocol for Ad hoc Networks, INRIA, 2003, pp.1-13.

Yasir Abdelgadir Mohamed Received the B.S. (2000) and M.S. (2003) degrees in Computer Engineering from university of Gezira, Khartoum, SUDAN, doing the PhD research at University Technology PETRONAS, MALAYSIA.

Azween Abdullah is a senior lecturer in the Department of Computer and Information Sciences at Universiti Teknologi PETRONAS, Malaysia. He obtained his BSc in Computer Science in 1985, MSc in Software Engineering in 1999 and PhD in Computer Science in 2003. His work experience includes twenty-one years in institutions of higher learning and commercial companies. His area of research specialization includes computational biology, modeling and simulation, formal specifications and network modeling, self-healing systems and security.