I²MANET Security Logical Specification Framework

Yasir Mohamed and Azween Abdullah
Department of Computer Sciences and Information Technology, University Technology Petronas, Malaysia

Abstract: *This paper presents an immune-inspired logical specification framework for securing Mobile Ad-hoc Networks (I²MANETs). The framework simulates the human immune system in: first response, second response, adaptability, distributability and many other Immune features and properties. The framework has the ability to monitor, detect, classify, and block the corrupted packets that transfer between nodes in a distributed environment. Scalability and bandwidth conservation are the well pointed out issues in the framework. The framework can be applied to many applications which depend on Ad-hoc technology such as emergency, health-care systems, and M-commerce.*

Keywords: *Wireless Ad-hoc networks, mobile agent system, immune-based security, framework specification logic.*

Received July 18, 2009; accepted August 10, 2010

1. Introduction

Although a lot of efforts have been made and a lot of studies have been carried out in network security, we cannot go so far as to say the security requirements for the different types of networks have been satisfied. As applications that are applicable to different networks mature, new security methods are undoubtedly necessary. Infrastructure less environments are dynamic and mostly difficult to control; hence security methods designed for other types of networks might not be applicable. Mobile Ad-hoc Networks (MANETs) are subjected to more vulnerabilities than the fixed networks as they are self-organized, self-configured, and self-controlled infrastructure less networks. In this paper we are concentrating more on securing MANETs. The decentralized nature of network control in MANETs makes them more prone to physical security attacks; hence, solutions should follow the same nature and must be distributed as each node at any time could set off the communication range of any other nodes [21].

In spite of the differences between computer systems and living organisms, there are still many undeniable similarities that could point the way to improve computer security. Improvements can be achieved by applying some of the features of the human immune system to computer security [9]. The immune system has many features that are desirable for the imperfect, uncontrolled, and open environment in which most computers currently exist. These include distributability, diversity, disposability, adaptability, autonomy, dynamic convergence, anomaly detection, multi-layers security, identification via behavior, reliability of components, and imperfect detection [17]. A wide variety of architectures for computer immune system has been inspired from the foregoing features [18].

2. The Related Works

While earlier research works have been focused only on problems such as multihop routing and wireless channel access, security has been given a significant attention and it has fast become an active area of research in recent years in order to provide protected communication between mobile nodes in unfriendly environment [13]. Several security approaches have been introduced to solve the security problems in classical MANET routing protocols [10, 19]. The Artificial Immune System (AIS) approach in [7] is one of the earliest attempts of applying HIS mechanisms to intrusion detection. The proposed system first detected viruses using either fuzzy matching from a pre-existing signature of viruses, or through the use of integrity monitors which monitored key system binaries and data files for changes. To reduce the viruses from spreading across networks, systems found to be infected would contact neighboring systems and transfer their signature databases to these systems. There are no testing and performance details given by the authors. In [6] proposed other AIS based Intrusion Detection System (IDS) called ADENOIDS. This approach conforms to the philosophy taken by Kephart *et al.* [13] and De-Paula *et al.* [6] initiated eight different components taken from the innate and the adaptive immune system. From the innate immune system, based on clear evidence, such as a security policy violation, the evidence-based detector is responsible for intrusions detection. The innate

response agent reacts to detect attacks using the evidence-based detector. Their responses, such as limiting bandwidth or disk access, are limited and general like the reactions of the innate immune system. The behavior-based detector, which is an anomaly detector, is initiated only when it receives co-stimulation signals, which are the detection results of the evidence-based detector. However, attempts to implement the processes using the mechanism of the HIS hadn't been made, only to mimic it at a high level of abstraction.

An agent for detecting and analyzing data for intrusion detection has been designed [25]. Negative selection mechanism that was proposed earlier [22] has been improved with mutation mechanism. The redundant detectors check process was considered. Five gene fractions represent both the antibody and antigens sets. Different protocol types can be treated with different agents. Antibody and antigen sets are expressed by the destination IP address, source IP address, source port, and destination port. TCP, IP, ICMP protocols are paid more attention as they influence the protocol analysis. No security features other than detection is proposed. Humming distance has been used to compute feature vectors and detectors.

Another method based on genetic algorithm and agent based computing system has been introduced [8]. In their method, detectors are used to discriminate between self and non-self in a distributed environment. Detectors are activated when they match to incidents; they are either selected as memory detectors or removed. The system is said to discriminate many types of attacks depending on learning capability. The detector set involves 128bit binary strings for a fixed threshold for the matching process. Several sets of detectors are used where an agent in each set plays a master agent role. From each set there is one representative agent that has the best fitness value, the agents reside on the host but they can still share the information with other sets. The IDS is the security feature provided by the system; however, no IDS response is considered.

A system for MANETs that comprises negative selection paradigm for anomaly detection has been presented [4]. Sets of detectors have been deployed to simulate the negative selection mechanism.

Specific packet signature is constructed before the monitoring process starts, and then the detector reports the anomalous behavior to neighboring detector or to the user. Detectors share the information about the intrusion where each agent is equipped with self patterns. Raising alert for intrusion depends on the shared information between the agents. Human interaction is proposed to prevent or treat the intruder.

In [1] presented an architecture of abnormality detection system based on the paradigm of Artificial Immune Systems (AISs), implementing a number of methods for generation of anti bodies and antigens. The approach applied the anomaly detection to the TCP/IP protocol and implemented a number of methods for generation of detectors, simulating the behavior of the immune system; but, as cited, it does not prevent new kinds of attacks which make the system lose adaptability.

3. Immunology

The role of the immune system is to defend the body against destructive diseases and infections. The success in performing such function comes from the ability to recognize virtually any foreign cell or molecule, and eliminating it from the body. To do this, the human body must perform pattern recognition to distinguish molecules and cells of the body called "self" from foreign ones called "nonself". Therefore, distinguishing self from dangerous nonself is the problem that the immune system faces [5]. The immune system architecture is multilayered, providing defenses at many levels. The most significant feature of innate immune recognition is the reality that it persuades the expression of co-stimulatory signals in Antigen Presenting Cells (APCs) that will lead to T cell activation, thus encouraging the start of the adaptive immune response [23] Without innate immune recognition, adaptive immune recognition may suffer the consequence of negative selection of lymphocytes that expresses receptors involved in the adaptive recognition.

4. Security Framework

In contrast to the previous works [14, 15, 16] and as declared in the next subsections, the proposed security framework shows more scalability and conserve the wasted bandwidth appears previously. Table 1 shows the approaches that have been successfully at implementing some immune features compared to our proposed security framework. The security protocol basically consists of four parts, which consider the different scenarios that might happen inside the wireless Ad-hoc domain: the detection part, classification part, blocking/isolation part and recovery part that might follow if data recovery file is replicated.

- *Detection Role:* This phase runs when a connection is established between two wireless nodes. The phase is automatically triggered as a connection request is being received by a node that has the security agent Immune Agent attached to its system.
- *Classification Role:* Discriminating the patterns within the incoming packets to a self or a non-self is considered to be, by most of the researchers, as the basic theory upon which their approaches rely. The system is designed to classify the patterns and

then take the necessary measures accordingly. The incoming events are considered to be malicious if any negative effect is detected in the New Technology File Systems (NTFS).

- *Blocking/Isolating Role:* Simulating the Immune System (IS), where a nonself is physically bound to peptide and then eliminated, the aim of this phase is to block and isolate a node that is being classified as malicious according to preset conditions. These conditions and standards are stored in the Immune Agent (IA) as declared later, it is updated consistently according to the traffic movements among the different nodes, from inside and outside the domain.
- *Recovery Role:* The IA is configured to replicate a data recovery file when it has successfully attached itself to the new node that intends to join the wireless domain. This data recovery file will be stored in the IA database, and the node's entry will be updated consistently whenever a change takes place regarding the node's system. According to the danger theory, when a change in the node's system is detected, a classification for the pattern that causes the change will be ascertained. In the case of positive change, the recovery process is not required; thus the update process will be performed as normal. On the other hand, when a negative change occurs in the system, where the pattern affects the system; the pattern will be blocked/isolated in future. In such a case, the data recovery file is required to recover the infected node.

The dependency on a system that has centralized features for enhancing a decentralized system may directly influence the system scalability. As a similar protective nature that exists in the IS is desired for the network, applying some of the immune features is expected to result in a distinguished contribution in terms of securing mobile ad hoc networks. The security task will be performed as follows:

- Create an agent called IA.
- The IA resides at the first node in the domain, configured by the user.
- The IA will be properly configured before it is released; the configuration includes several steps as described in the following sections.
- The IA replicates whenever another node intends to join the domain. The node must accept the attachment of the IA to its system as a prerequisite for establishing the connection.
- IA remains valid as long as the node remains within the domain, otherwise it must request for a new IA after leaving the domain.
- Self healing process will be performed where possible to recover the corrupted nodes.

Two mechanisms have been used for a comprehensive security framework: the innate immune system and danger theory. The main issues that have been considered in developing the new framework are bandwidth, scalability, and complexity. One of the most limiting characteristics of mobile ad hoc networks is scarce and variable bandwidth. This makes it essential that any system must impose very little traffic overhead on the network. It is necessary to achieve reliable scalability in order to gather and analyze the high-volume audit data correctly from distributed nodes that have a high mobile nature. For that reason and to verify the efficiency, DSR has been preferred as the routing protocol for our security framework. This part is left to be discussed later.

4.1. IA Configuration-Phase I

The first training phase performed in a secured and controlled environment that doesn't have an access to internet, free of viruses, errors, and traffic in the wireless environment was monitored. Different nodes using different protocols were involved in the monitoring process. The involvement of different nodes in the monitoring phase assures the diversity of self, nonself, and consequently the generated detectors. The frequently occurring sequences mostly are the patterns included in the protocol headers, besides some patterns in the payload. It was found that the most repeated sequences regarding the protocols headers are: the source address, destination address, and the services port. Figure 1 shows that the patterns captured during the test period are 93.3% and 6.7% for the frequently occurring patterns and the seldom events in the protocols' headers, respectively.

Table1. Different immune approaches.

Research Work	Negative Selection	Anomaly Detection	Clonal Selection	Danger Theory	Costimulation	Permutation Mask
Byrski and Carvalho (2008)	√	√	√	×	×	×
IDR system for MANET (2006)	×	√	×	×	×	×
S. Sarafijanovic and J. Le Boudec. (2005)	√	√	√	Only for packet loss	×	×
I^2MANET (2010)	√	√	√	√	√	√

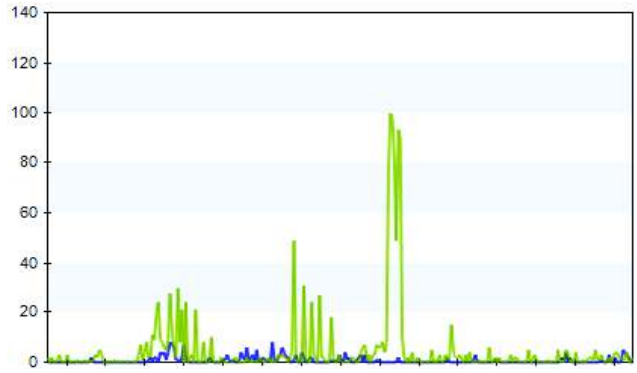


Figure 1. Frequently and seldom occurring patterns in protocol headers.

The figure assures the possibility to construct a self pattern profile from the control data (protocol headers) that contain the mostly needed and repeated events. In contrast, the events in the payload part which is infrequently repeated will be handled by the danger theory, which is explained later in this article.

a. *Genes Generation:* The security process starts with the gene generation function. The generated detectors on the surfaces of lymphocytes bind to the nonself and eliminate it, thus protecting the body. Simulating this process in a highly protected environment, similar to thymus in the immune system, the IA is properly configured, and trained to monitor and capture the packets that transfer between two controlling nodes after connection has been established. The IA captures and stores the frequently and repeated sequences within the protocol header (i.e., sync, TTL, port number, source address, destination address etc.), which is necessary for establishing the connection. These sequences called Genes represent the self cells that the immune system depends on for classification process. Let $U=S_f \cup N_f$ represents the set of all patterns monitored during the monitoring and capturing phase; it contains both self (frequently occurring) and nonself (abnormal) patterns; where $N_f=\{n_{f1}, n_{f2}... n_{fm},\}$, $S_f=\{s_{f1}, s_{f2} ..,s_{fn} \}$, and $S_f \cap N_f=\emptyset$. The output of the Genes generation function is a profile that contains all the self S_f, which is an essential element for generating the detectors in the next object. The IA is equipped with the database during the configuration phase.
b. *Detectors Generation:* The second step in phase I of the configuration is detectors generation. Simulating the lymphocytes, the IA will be equipped with detectors that are randomly generated. With the same gene length (number of bits), detectors are generated. Each generated detector will be matched with the entire genes in the genes profile. The detector that matches any of the genes will be considered as invalid and deleted, or else added to the detectors set. This test simulates the negative selection mechanism in HIS, and many researchers have used the same technique [3]. Although they depended on specific protocols (e.g., TCP), they have suggested for the other protocols to be included among the different considerations. Different protocols have been used in ad hoc networks other than TCP; hence, a method that considers the diverse wireless protocols is more reliable in terms of detection. The negative selection algorithm ensures that the selected detectors will not match with a self which may cause a serious system internal failure. That is similar to the autoimmune disorders in immunity. Scientifically, matching could be accomplished using contiguous bit matching rule in equation 1:

$$Pcontg \approx 2 - r\left(\frac{(1-r)}{2} + 1\right) \quad (1)$$

The most effective factor in equation 1 is the number of bits which set for the matching process. It's shown in Figure 2 that when the r (matching bits number) approaching L (string length), the matching probability approaches zero which means low probability.

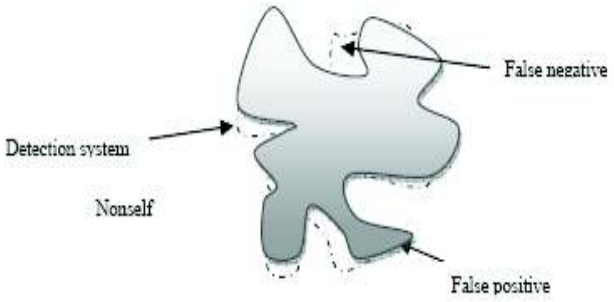


Figure 2. Matching probability.

However, the high probability leads to false alarm, whether it is positive or negative as shown in Figure 3 [11].

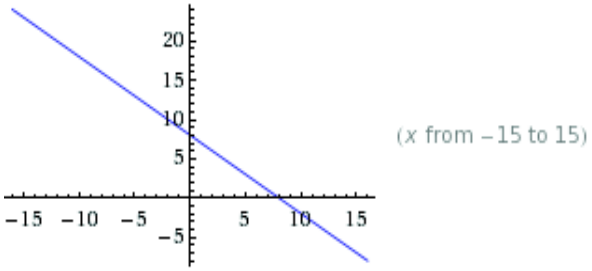


Figure 3. Detection system.

For the preliminary experiments, the r was set to 4 bits while L was 10bits. Let $\psi=\{\delta 1, \delta 2... \delta m\}$ represents the set of the generated detectors, $\psi'=\{\delta'_1, \delta'_2... \delta'_m\}$ represents the successfully maturated detectors. For each of the detectors in ψ' to be maturated (be able to detect nonself patterns), the negative selection test must be applied, whence it is either deleted or successfully selected as a detector. The states to generate valid detectors are depicted in Figure 4.

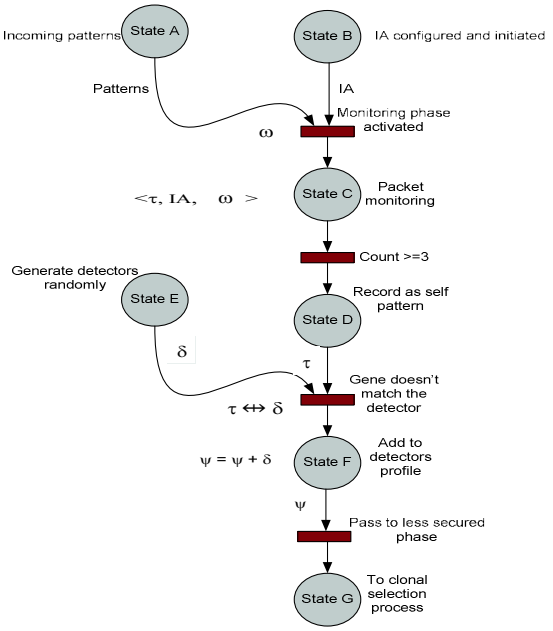


Figure 4. Mapping lymphocytes to the security protocol.

4.2. IA Configuration-Phase II

In the second phase, which was performed in a live network less secured, the detectors was released so as to be trained to detect the various nonself patterns. After the IA has been configured with the database, it is then attached to one node in a wireless environment, and then this node will receive and send packets to other nodes in the normal way. Each node that is a member of the domain will receive the IA with the full and updated database. IA in a live network has the chance to detect the nonself. Since the only set in IA is the self N_f, any other detected patterns will be considered as nonself. The main technique mapped from the immune system in phase II is the Clonal selection (Cs). Cs is complementary to the role of negative selection. It explains how an immune response is mounted when a nonself antigenic pattern is recognized by a specific type of cells labelled as B-cell [24]. 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 attains the score in detecting certain number of nonself.

When the cloned detectors are applied again to the negative selection mechanism, each of the cloned detectors that matches with Genes in the GenesProfile becomes the invalid detector and will be deleted, while the failed ones join the Detectors Profile. An alteration takes place for one bit in the high scored detector, then applied to the negative selection mechanism where it either passes or failed.

4.3. Danger Theory

It is been believed that the Human Immune System (HIS) 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 takes place. Using the danger theory concept [2, 20], some limitations that arise in prior works can be addressed, such as events that may appear as legitimate at some instance and illegitimate at another instance. To map this concept to the security model, the IA saves a replica of data necessary for recuperating from failure. This process takes place the instant the IA gets attached to the host node that accepts the security license. Considering a system β as a set of components at a particular time t, a change in the system components straightforwardly can be recognized since a copy of β is already saved in the IA database. For a change ε that may possibly crop up in a system according to an effect of an exact pattern s, after the transmission completes ($t+\Delta t$), IA checks the system and tracks pattern s that causes the alteration ε in the system components β. If φ (the pattern that causes the change) is categorized neither as a self nor a nonself it will then be considered as a suspected pattern, and will be added to suspect patterns set Sp. If φ affects negatively in β components, it will then considered as a nonself (malicious) pattern and consequently, switched to the nonself set N_f and will be blocked/ ignored in future.

The framework is designed to differentiate between the two terms, detection and classification. A node that participates in a transmission will be detected if it sends a malicious packet, but will not be classified at once as a malicious node.

5. Framework Specification Language

Appendix 1 shows the formal specification logic for the immune inspired framework. Since Dynamic Source Routing (DSR) is better in routing efficiency [12] and doesn't pose extra overhead for the routing process it has been chosen to support the routing services, the different security framework processes depend on the DSR header. There are some assumptions need to be declared for the easy and accurate understanding for the specification logic:

a. Self patterns S_f and non-self N_f both are limited sets i.e., $S_f \cup N_f = U$, and $S_f \cap N_f = \emptyset$.
b. S_p is a new classification for the patterns that are neither classified nor self neither non-self i.e., if $\varepsilon_i \notin S_f$ and $\varepsilon_i \notin N_f$ then save ε_i temporary at Sp.
c. Using the Periodic System Checker (PSC) which is similar to danger theory in IS, the patterns in Suspect Patterns (Sp) will reclassified again according to effects on the system.
d. IA can be configured with the necessary components and embedded in any routing protocol to perform the security task.
e. IA configuration assumes a new node will send RRP using DSR protocol.

6. Proposed Application Domain for the Security Framework

Since the immunological security framework can be applied to many applications that depend on Ad-hoc technology such as emergency, health-care systems, groupware, gaming, advertisements, military applications, and customer to-customer applications, healthcare systems have been chosen as one of the essential domains because they have a tangible and direct social impact [26] as shown in appendix 1. Due to resource constrained sensor nodes, uncontrollable environment, and large dynamic network topology, using sensor network poses unique challenges in security implementation; as a result, strict security mechanisms must always be in place to prevent malicious interactions with the healthcare systems. Such mechanisms should also be scalable as thousands of nodes are expected to be deployed within a healthcare system.

7. Contributions

Most if not all of the proposed approaches to secure mobile ad hoc networks were simulated to verify how these approaches are effective to secure such type of networks. In contrary, I^2MANETs has been simulated and practically implemented in a real-although small-environment. The desired goals have been perfectly achieved and the contributions stated below have been accomplished and verified using the two mentioned verification methods:

- A new mechanism for auto detection system for both previous and future intruders and attackers.
- A new Memory mechanism that remembers the attack, eavesdropper, leading to a much better reaction in the future.
- Gradual self isolation of the malicious nodes resulting in a trusty communication environment.
- A decentralized, reliable, self malicious patterns/nodes blocking.
- A comprehensive security protocol for multi-security functions.
- A self-healing system for recovering the infected nodes.
- Auto periodic system checker.
- No human interaction is required for setting or installation processes.
- Auto distributed-node based-intrusion detection system.

8. Conclusions and Future Work

An immune-based framework for securing MANETs has been presented. In this framework, an IA that contains three profiles viz. Genes profile, nonself profile, and detectors profile has been created. Replicas of the IA are distributed to nodes when connections have been 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. The major well thought-out issues are scalability and conserving bandwidth, which mainly characterize the Ad-hoc networks. We plan, as a future work, to design an immune-based protocol capable of enhancing the security of mobile Ad-hoc network most typically to what the immune system does to keep the body alive.

References

[1] Ahmedi M. and Melaki D., "An Intrusion Detection Technique Using Co-Co Immune System for Distributed Data Networks," *The International Journal of Computer Science and Network Security*, vol. 8, no. 4, pp. 160-169, 2008.

[2] Aickelin U., Cayzer S., Bentley P., Kim J., and McLeod J., "Danger Theory: The Link between AIS and IDS," *in Proceedings of Artificial Immune Systems*, Berlin, pp. 147-155, 2003.

[3] Balachandran S., Nino F., and Garrett D., "A Framework for Evolving Multi-Shaped Detectors in Negative Selection," *in Proceedings of IEEE Symposium on Foundations of Computational Intelligence*, Honolulu, pp. 401-408, 2007.

[4] Bouvry P. and Seredynski F., "Anomaly Detection in TCP/IP Networks Using Immune Systems Paradigm," *Computer Communications*, vol. 30, no. 4, pp. 740-749, 2007.

[5] Byrski A. and Carvalho M., "Agent-Based Immunological Intrusion Detection System for Mobile Ad-hoc Networks," *in Proceedings of the 8th International Conference on Computational Science*, Poland, pp. 584-593, 2008.

[6] De-Paula F., Castro L., and De-Geus P., "An Intrusion Detection System Using Ideas from the Immune System," *in Proceedings of Evolutionary Computation*, pp. 1059-1066, 2004.

[7] Farooq M. and Mazhar N., "BeeAIS: Artificial Immune System Security for Nature Inspired, MANET Routing Protocol, BeeAdHoc," *in Proceedings of Artificial Immune Systems*, Berlin, pp. 370-381, 2007.

[8] Forrest S. and Somayaji A., "Computer Immunology," *Communications of the ACM*, vol. 40, no. 10, pp. 88-96, 1997.

[9] Forrest S., Glickman M., and Ackley D., "Computation in the Wild," *The Internet as a*

Large-Scale Complex System, Oxford University Press, 2002.

[10] Forrest S., Allen L., and Cherukuri R., "Self-Nonself Discrimination in a Computer," *in Proceedings of the IEEE Symposium on Security and Privacy*, USA, pp. 202-212, 1994.

[11] Hofmeyr S., "An Immunological Model of Distributed Detection and its Application to Computer Security," *PhD Thesis*, University of New Mexico, 1999.

[12] Johnson D. and Maltz D., "The Dynamic Source Routing Protocol for Mobile Ad-hoc Networks (DSR)," drafts/draft-ietf-manet-dsr-09.txt, last visited 2004.

[13] Kephart J., Sorkin G., Arnold W., Chess D., Tesauro G., and White S., "Biologically Inspired Defenses Against Computer Viruses," *in Proceedings of the 14th International Joint Conference on Artificial Intelligence*, Canada, vol. 1, pp. 985-996, 1995.

[14] Mohamed Y. and Abdullah A., "Security Mechanism for Manets," *Journal of Engineering Science and Technology,* vol. 4, no. 2, pp. 231-241, 2009.

[15] Mohamed Y. and Abdullah A., "Immune Inspired Framework for Ad-hoc Network Security " *in Proceedings of IEEE International Conference on Control and Automation*, New Zeland, pp. 297-302, 2009.

[16] Mohamed Y. and Abdullah A., "Biologically Inspired Architecture for Securing Hybrid Mobile Ad-hoc Networks," *in Proceedings of International Conference on Innovations in Information Technology*, Al-Ain, pp. 638-642, 2008.

[17] Marti S., Lai K., and Mary Baker "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks," *in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, USA, pp. 255-265, 2000.

[18] Sarafijanovic S. and Le-Boudec J., "An Artificial Immune System for Misbehavior Detection in Mobile Ad-hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors," *in Proceedings of Artificial Immune Systems*, Italy, pp. 342-356, 2004.

[19] Sarafijanovi S. and Le-Boudec J., "An Artificial Immune System Approach to Misbehavior Detection in Mobile Ad-hoc Networks," *in Proceedings of Biologically Inspired Approaches to Advanced Information Technology*, Berlin, pp. 396-411, 2004.

[20] Scarfone K. and Mell P., *Guide to Intrusion Detection and Prevention Systems IDPS*, National Institute of Standards and Technology, 2007.

[21] Somayaji S. and Forrest S., "Principles of a Computer Immune System," *in Proceedings of the Workshop on New Security Paradigms*, United Kingdom, pp. 75-82, 1998.

[22] Stephanie F., Somayaji A., and Longstaff T., "A Sense of Self for Unix Processes," *in Proceedings of IEEE Symposium on Security and Privacy*, USA, pp. 120-128, 1996.

[23] Tonegawa S., "Somatic Generation of Antibody Diversity," *Nature,* vol. 302, no. 5909, pp. 575-581, 1983.

[24] Williams P., Bebo J., Anchor K., Gunsch G., and Lamont G., "CDIS: Towards a Computer Immune System for Detecting Network Intrusions," *in Proceedings of Recent Advances in Intrusion Detection*, Berlin, pp. 117-133, 2001.

[25] Zhongmin Y. and Baowen X., "The Algorithm Design of Agent for Detecting and Analyzing Data in Intrusion Detection Based on Immune Principle," *in Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing*, Shanghai, pp. 1779-1783, 2007.

[26] Zuben F., "Artificial Immune Systems: Part I - Basic Theory and Applications," *Technical Report*, School of Computing and Electrical Engineering, State University of Campinas, Brazil, 1999.

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.

Yasir Mohamed received his BSc in 2000 and MSc in 2003 degrees in computer engineering from University of Gezira, Sudan, PhD in information technology in 2010, Malaysia. His research area is networking security.

Appendix 1

Formal Specification Logic for Securing MANETs (application domain)

Symbol	Description
β	*System components*
γ	*Classification process*
δ	*Detector*
ε	*A change in system*
↺	*Connection between two in a secure environment*
η	*Run periodic system check*
S_P	*Temporary file: suspect patterns file*
τ	*A pattern*
⇆	*Block process (BLCK)*
IO	*Recovery process (REV)*
Φ	*IA deactivation*
PCKs	*Packets*
ρ	*Clone process*
λ	*Checking process*
U	*Set of all patterns (self + nonself)*
⇎	*Connection terminated*
χ	*Nodes inside a domain*
ψ	*Detectors set*
ω	*Monitoring phase activation*
s_f	*Self patterns*
↠	*Save process*
↔	*Match process*
IALCS	*Immune agent license*
∴	*Then*
CS	*Connection establishment*
⇉	*Broadcast process*

1. Configure Immune Agent (IA)

IA := < S_f , N_f , *DrP, DTEC, RVR, BLCK*>

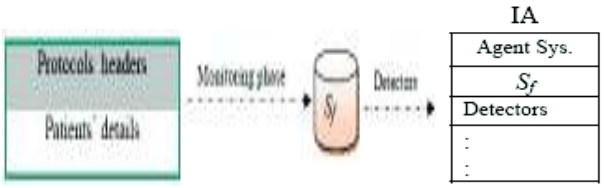
(*Immune Agent configured with the necessary components; self, non-self, and detectors profiles, detection, recovery, and blocking functions)*

1.1. Training phase: Building self/non-self profiles

S/N prf ::= < PCKs,χ_i ,ε_i >

IA:ω PCKs ‖ χ_i ↺χ_j

(IA monitors the packets within a traffic between two nodes, no internet)



IA: ε_i ↠ {S_f} ‖ ε: = l: [a_0 a_1 …a_n], a_i= {0, 1}, i= {1, 2, 3…n};

(Save the frequently occurring patterns as self patterns, each pattern has the fixed length l and consists of a string of Boolean)

IA: ε_i ∉ {S_f} ↠ {N_f}

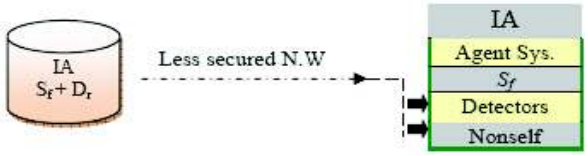
1.2. Building detectors profile (DrP)

DrP::= <δ, ε_i, S_f, N_f , $\delta_{i\ (score)}$, ψ>

BRG (PCK,δ) = l : [b_0 b_1 b_2…b_m] ‖ b_j= {0, 1}

(Applying a function for randomly generating detectors with length l)

∀δ_i: ↔ ε_i; if δ_i = ε_i *delete*; else δ_i↠ψ:= {δ_0, δ_1... δ_n}



(Each generated detector matched with the entire self patterns, either deleted or saved- negative selection test)

IA: ρ = F (ψ)

(Pass the detectors profile to clone function)

ρ : ω PCKs‖ χ_i ⇆χ_j

(Clone process run in a live environment)

ρ : ∀δ_i: $\delta_{i\ (score=0)}$;

(For each detector, set a score for matching the non-self patterns)

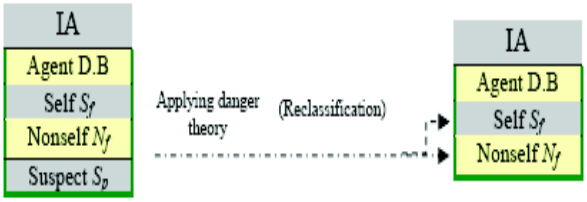
ρ : δ_i↔n_f‖ n_f∈ {N_f} ∴$\delta_{i\ (score++)}$

(If a detector matches a non-self; increase the score for the detector)

ρ : $\delta_{i\ (score)}$≥ Threshold ∴ρ(δ_i)= δ_i*

(Pass the high scored detectors to clone function to generate new detectors from the high scored one)

ρ : δ_i*↔ε_i ‖∈ {S_f} ∴ *delete*; else δ_i↠ψ



2. Connection establishment (CS)

CS::= <RRP, REP, DA, SA, UI, IALCS>

CS:χ_{i+1} → RRP

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

CS: ∀ χ ∃ χ_i (IA)

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

CS: χ_i ← (REP+ IALCS)

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

CS: χ_{i+1} ↞ (IALCS)

(Accepts license)

CS: χ_i (DA, SA, UI, IA) → χ_{i+1}

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

3. Securing Node χi+1

IA: ↤↦$\chi_{i+1(t)}$

(Perfectly connect to the node's system at time t)

IA: ↠DRF $_{(t)}$

*(Save a copy of the **D**ata **R**ecovery **F**ile at time t (before data transfer))*

IA: ω PCKs

(Activate the monitoring phase)

IA: γ PCKs/τ

(Classify the incoming patterns)

IA: ∀τi ↔s_{fi} ‖ i = {1, 2, 3…n}

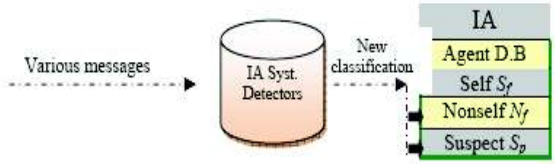
(Match with self patterns)

τ_i :τ_i ∈ {s_f}? ↔ PCKs

(Match? Permit packets transfer)

3.1. Periodic System Checker

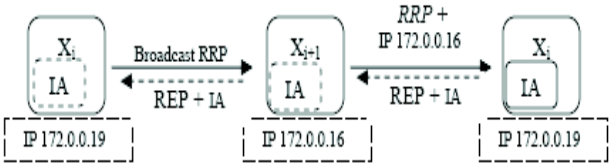
PSC (η) ::= <τ_i, s_f , β_t, S_p >
τi :τi ∉ {s_f} then η
(Run Periodic System Check (PSC))
τ_i :τ_i ↠ {S_p}



(Represents the system components; danger theory part)
η : Let β_t= {β_1, β_2… β_n}
η : IAη $\beta_{(t)}$
(Periodic system check components at time t)
η : IA η $\beta\hat{}_{t+\Delta t}$
(Repeat the check at time t+Δt)
η: $\beta_t = \beta\hat{}_{t+\Delta t}$; τi ↠ S_f
(No negative effects of the pattern τi, (save τi to the self profile)
η: $\beta_t = \beta_{(t+\Delta t)}$
(System harmed)

3.2. Blocking process (BLCK)

BLCK ::< τ_i, N_f , χ, count_>
IA ↹ τi
(τi blocked gradually)
IA $_{(\chi i+1)}$: ⇉ τi ∀ χ_{IA}
(IA in node χi+1 will broadcast the new pattern(s) to all IAs inside the domain)



IA: ∀ $_{(\chi i+1) \in \chi}$ ↠ N_f
(Node $_{\chi i+1}$ update the non-self profile by adding the new pattern(s))
IA: IA **count--**
IA: IA_Φ: Count=0, or χi+1 ⇎ χi
(*IA deactivated in case of connection terminated or agent counter = 0*)

3.3. Recovery process

REV (ƗO)::= < η, DRF, $\beta_{(t)}$ >
IA: IAη $\beta_{(t)}$
(System check)
IA:λ (DRF); if exist ∴ƗO else ↹
Check the data recovery file for recovering missing files, if exists; recover, else call block process)