Journal of Engineering Science and Technology
Vol. 4, No. 2 (2009) 231 - 242
© School of Engineering, Taylor's University College

SECURITY MECHANISM FOR MANETS

YASIR ABDELGADIR MOHAMED*, AZWEEN B. ABDULLAH

Department of Information and computer science, University Technology PETRONAS
P. O. Box 10, 31750, Seri Iskandar, Tronoh, Perak, Malaysia
*Corresponding Author: Yasir_eym@yahoo.com

Abstract

Be short of well-defined networks boundaries, shared medium, collaborative services, and dynamic nature, all are representing some of the key characteristics that distinguish mobile ad hoc networks from the conventional ones. Besides, each node is a possible part of the essential support infrastructure, cooperate with each other to make basic communication services available. Forwarding packets or participating in routing process, either of each can directly affect the network security state. Nevertheless, ad hoc networks are suspectable to the same vulnerabilities and prone to the same types of failures as conventional networks. Even though immune-inspired approaches aren't essentially new to the research domain, the percentage of applying immune features in solving security problems fluctuates. In this paper, security approach based on both immunity and multi-agent paradigm is presented. Distributability, second response, and self recovery, are the hallmarks of the proposed security model which put a consideration on high nodes mobility.

Keywords: Immune system; Architecture; Security; Mobile ad hoc networks

1. Introduction

Mobile ad-hoc networks are classified as self organized networks without fixed infrastructure. They can be rapidly deployed and reconfigured. Set of applications for MANETs is diverse, ranging from small static networks that are constrained by power sources, to large scale, mobile, and highly dynamic networks. Success in operations of a mobile ad hoc network depends on cooperation of the nodes in providing services to each other. Since mobile ad hoc networks make it possible for the devices to join or leave the domain without required permission, node in the domain can not considered to be trusted. Conventional security approaches do not address all concerns of ad hoc networks since both benign and malicious parties

Abbreviations

CPN	Colored Petri Net
D.B	Database
DSR	Dynamic Source Routing
HIS	Human Immune System
IDS	Intrusion Detection Systems
MANETs	Mobile Ad hoc Networks
Mgr	Manager Agent
Mtr	Monitor Agent
Rp	Replicate Agent
Rv	Recover Agent

have full admission to communicate with peers. The wireless channel is accessible to both legitimate network users and malicious attackers. Attackers may intrude into the network through the subverted nodes. In spite of the dynamic nature, mobile users may apply for anytime, anywhere security services as they are in motion from one place to another. Consequently a security solution is required which has both extensive protection and desirable network performance.

Conventional approaches to misbehaviour detection use the knowledge of predictable misbehaviour patterns and identify them by looking for specific sequence of events [1]. These techniques are beneficial for detecting the known intruders, viruses, and worms but no longer work with detecting the anomalies. An integrated security system needed that considering all MANETs special characteristics and considerations. As a result, researchers turned to the immune as a perfect amazing adaptive system that defend the human body against both known and anomaly intruders[2]. In this paper, immunity based architecture that attempts to simulate the immune behaviour is introduced so as to make the mobile ad hoc domain self detecting, reacting, and healing against different known and unknown attackers.

2. Related Works

Most of the work has been done previously in this field focused on the routing process and how it is been affected by the intruders or attackers. We do not argue that security and routing processes are different, but in our approach we will look even at the routing process from a security perspective.

Taguchi [3] proposed intruder detection and tracing algorithm using a mobile agent which dynamically generated. The mark type uses information log which is single. No solution planned after detection.

Nishiyama and Mizoguchi [4] designed a security system which consists of different immunity agents. These cells, which are dynamically generated through recognizing the access via the network, gather the information and detect illegal intruders by cooperation between immune agents.

Machado et al [5] developed a model with aim of intrusion detection based on the immune system paradigm. The model constructed based on registries' signature relevant information. Real-time approach is host-based and adopts the

anomaly detection paradigm. The model consists of many components that analyze logs registries for auditing and use anomaly detection scheme for monitoring. The model designed for intrusion detection in general networks, however ad hoc networks have a unique features and characteristics.

Zhang et al [6] have developed a cooperative intrusion detection system where IDS agents are located on every node. Agents run separately, detect intruder locally and perform a response. Random packet dropping and forging route entry in a node route are the details of the intrusion detection methods addressed by the researcher. The random packet dropping detection scheme relies on the eavesdropping transmission of adjacent nodes.

Madhavi [7] proposed IDS for mobile ad hoc networks. The system can detect whether the node get the fair share of the transmission channel. It relies on overhearing packet transmission of neighbouring nodes that makes it effective system in networks where nodes use different transmission power and directional antennas for different neighbours. The proposed system can select the threshold dynamically. The proposed solution does not rely on any of the immune system features that we plan to apply in our approach.

Ping et al [8] provided an immunity based security architecture for mobile ad hoc networks. An attempt is made to map the mobile agents to lymphocytes for detection and isolation purpose. As mentioned, the main advantages of the architecture are distributability, autonomy, and adaptability. Three mobile agents were suggested, monitor agent, decision agent, and killer agent, simulating T-cells, B-cells, and anti body respectively. The monitor agent monitors and sends the data to decision agent that decides who is the invader, then it produce a killer agent to surrounds and isolates it. Self recovery for the corrupted nodes is not a part of the proposed architecture.

Mcgibney [9] combined the biologically and socially inspiration to present an approach to mitigate ad hoc network threads, a biological techniques for distribution of attack is used where the attack level itself is socially inspired.

Inspired by the lymphocyte' working mechanism in the immune system, an immune agent-based model is introduced by Zhang et al [10]. Three immune agents are proposed: centre control agent, B-agent, and memory agent. C-agent plays a role of manager, responsible of producing detectors and their carriers besides some control issues. B-agent travels in the network and monitor and collect information, and can become M-agent under certain conditions. M-agent has a detector set, can travel in the network and quickly can adapt for future response.

A body mapped as the MANET by Boudec and Sarafijanovic in [11], well behave nodes, misbehaving nodes, and antigen as self-cells, non-self cells, and a sequence of observed DSR protocol respectively. Negative Selection and Bone Marrow Antibodies are created during offline learning phase. Network with only certified nodes in approach simulated as bone marrow where the B cells maturated in the immune system.

3. Proposed Architecture

In the approach, multi-agent system has been proposed to secure the ad hoc network domain; two of them are static whereas the others are mobile. The static ones are manager agent and monitor agent. The replicate agent, 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 anode in the ad hoc network that acts as a server based on relevant capabilities such as computing power, battery power, signal strength, hardware, etc. A management method for dynamically changing the role of a node to act as a server will be specified later [12]. The rest of nodes behave normally as expected in the mobile ad hoc network. An essential component of the architecture is the database that updated incessantly in detector agent on each node and imitates the memory cells that help in second response reaction in the immune system.

3.1. Mapping IS to proposed approach

The immune system consists of a large number of different innate and acquired immune cells which interact to provide detection and elimination of the attackers [13]. Success in mapping more immune processes and features result in a robust security system for the concerned application. Figure 1 depicts natural immune system components, the ones that applied to our approach are mapped as in Table 1 below.

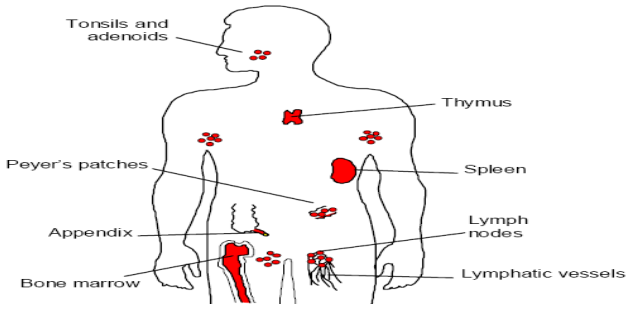

Fig. 1. Human Immune System Components.

Table 1. Mapping Immune System to Security Architecture.

Natural immune	Security approach
Body	Mobile Ad hoc domain
Lymph nodes	Mobile nodes
Self	Normal behaviour
Antigens	Sequence of normal observed patterns
T cells	Monitored agent
Detectors	Special patterns in monitor agents
Memory cells	Database distributed in both monitor and manager agents
Distributability	Detectors (agents) distributed in each nodes
Adaptive immune system	Database updated and distributed periodically between the agents
Antibodies	A patterns with the same format as the compact representation of antigens
Elimination	Blocking/ignoring the incoming packets

3.2. Overview

The manager agent which resides on the server side frees the other agents almost immediately as it recognizes the other network nodes as shown in Figs. 2a and b. Bidirectional arrows indicate mobile gent return to the home platform. The database (memory cells) will be rebuilt periodically in both manager and monitor agents. A feedback from the monitor agent (discrete arrow) results in recovering process (self healing process) as shown in next sections.

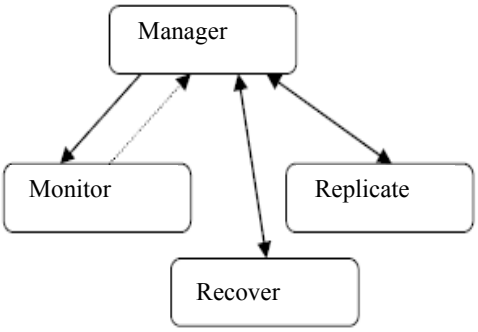

Fig. 2a. Multi-agent Security System.

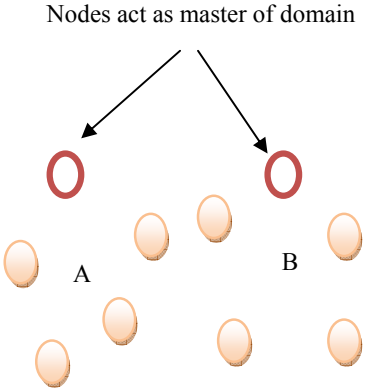

Fig. 2b. Two Ad hoc Domains.

3.3. Identifying manager agent

The manager agent recognizes the configuration of the network periodically; therefore, a change in domain will be updated as happens in the routing table. As shown in Fig. 3, the configuration includes learn function where monitor agent be taught to distinguish and differentiate between the self (customary behaviour) from others (anomalous behaviour) [14]. This phase simulates the maturation one that takes place in thymus in immune system. Patterns in the Monitor agents mimic the T-cells' behaviour as it released after it get matured enough to detect the foreigners. Releasing the monitor and replicate agents is the state following the recognition. The monitor agent, who is static, resides permanently on the node side. Releasing agents takes the manager agent to listening state where it updates trust table, construct recovery system, or release a recover agent to get well failure node' system to a previous good condition.

As described in the symbolic forms below, all the agents are configured after creation. If the agents successfully configured, copies are distributed to all nodes that exist in the domain. In C the manager agent enters the wait status where it waits for a response from the released agents {Rp, Mtr}. The manager behaves according to the response sends either by the monitor or the replicate agents. If the monitor sends an update message, it indicates an abnormal behaviour (nonself) from possibly a corrupted node has been ascertained. The monitor agent sends a message in cases of no information there established regarding to the sender in monitor's local data base.

As depicted in Fig. 3, checking the node membership in place D results in either a node has no entry in manager database, or already it has. In the first case, the negative membership Acknowledge leads to block/ ignore the incoming packets from the corrupted node and broadcast its identity to all, though helping in proper reaction in future. The second case means a restore point for the corrupted node exists; consequently uploaded to the recover agent for the sake of recovering (self healing process).

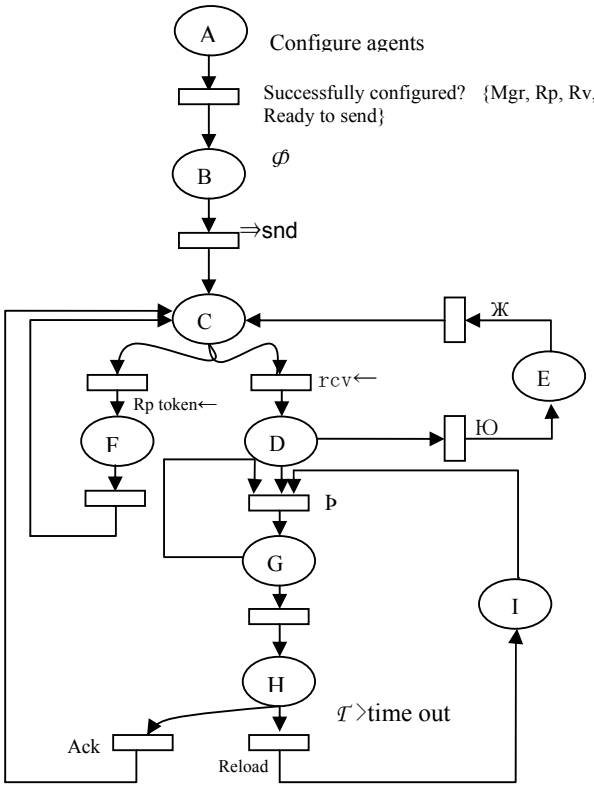

Fig. 3. Basic CPN Model for Manager Agent.

Table 2 illustrates notations used in the symbolic frame work for the agents; those frameworks exemplify how the task of agents is being performed. A basic CPN (Coloured Petri Net) model that describes the transitions and places of the manager agent is depicted in Fig. 3 above. A time set for feeding back whether the node has been healed successfully. If it is out before receiving the acknowledge, the manager will reload the restore point, else wise, the monitor will be informed that a node already has been fixed, hence the node will be treated as normal in future.

Conversely, if the response received from the replicate agent, also two cases expected; either the node has an entry in the restore point table, hence will be updated with the new restore point held by the replicate, or the node has joined

the domain freshly, therefore a new entry will be established. So the manager administration depends on the response received while listening.

Table 2. Notations.

Notation	*Definition*
Mgr	Manager agent
Mtr	Monitor agent
Rp	Replicate agent
Rv	Recover agent
CP	Copy of each agent
⇒*snd*	Send process
{ δ }	Set of nodes in the domain
Ю	Block process
rcv←	Receive process
Ð	Ad hoc domain
Ф	Upload process
Ж	Broadcast message
∫∫	Distributability
{Я}	Restore points set
u	Update
{£}	Set of agents
$Š_f$	Self
$Š_{nf}$	nonself

symbolic framework specifying the manager agent

(∀ {δ} ∈*Ð* ⇒SND*ϕ* :(3, Mtr, Rp, Rv)); *then wait*;
If ((Mgr) rcv← Mtr ACK) *then*
    If (δ !!∈ *Ð*) *then* Ю ∧ Ж *else*
    (∃$Я_i$ ∈ {*Я*}): *ƒ (Яi);*
    Mgr ⇒snd (*ƒ (Яi)*) *then check τ;*
    If (*τ* >time out) (∃$Я_i$ ∈ {*Я*}): *ƒ (Яi);*
    Else ⇒snd (ACK) then (*back to wait state*);
Else // *a token received from replicate agent*
If (*Яi* ∈ {*Я*}) then *u* (*Яi*);
Else (i= i + 1);
$δ_i = δ_{i+1;}$

3.4. Identifying monitor agent

The Monitor agent monitors the neighbour node' behaviour and react accordingly. Four components form the structure of the monitor agent: monitoring part, database part, decision part, and communication part.

The monitoring part watches the neighbour's traffic and pass the suspectable ones to the database part where scanning process take place to decide whether a self or nonself is passing. Through communication part, the monitor agent

communicates with the same parts in monitor agents distributed on other nodes, likewise, communicate with the manager agent.

Figure 4 depicts the monitor agent components. The monitor agent configured to properly communicate with the manager agent as well as distinguishing the self patterns and block the others. Short sequences of system calls and checking protocols headers are some of the techniques proposed to identify the nonself patterns. If correctly configured, the monitor agent released to communicate with node and monitor the packets that pass in. In case of self patterns, packets accepted and transferred normally.

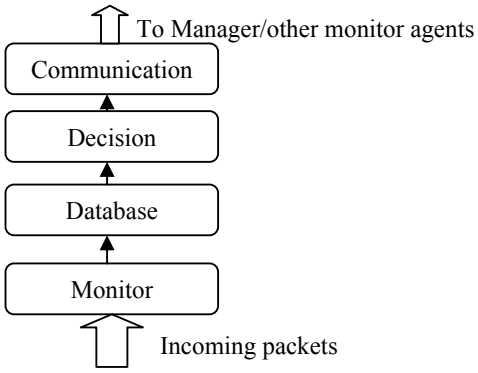

Fig. 4. Monitor Agent Components.

Otherwise, the packets blocked/ignored and the monitor check local database. If the packet's info already exist, no updates come to pass, else, monitor informs the manager about the new suspectable node.

The monitor then keeps blocking the packets until acknowledged by the manager. If positive, which means the problem fixed, the monitor unblock the packets for the next connection. For fear that a negative acknowledge received, the monitor will block the node and inform the manager, which, in turn, informs other nodes in the domain for proper treatment futurely. A symbolic form for the monitor agent followed by CPN model is depicted Fig. 5.

Symbolic framework Specifying monitor agent

$Mtr_0 \in \{£\}$: $(\forall \{\delta\} \in \Phi \Rightarrow SND\ Mtr_0$
If IP: =IP_δ *then monitor pckts*
If $\check{S}_f$ *then rcv← pckts*
Else IO pckts ^ check D.B
If $Mac_\delta \in \{Mac_{D.B}\} \rightarrow IO\ \delta$*// Mac address*
Else (info) ⇒snd → Mgr && wait
If –ve ack then IO δ Else rcv←pckts

From the fact: *An agent is software that can pass through from a node to other performing different tasks before it communicates with the original source* [15].

The assertion (1) can be derived:

An agent can skilled to distinguish the self patterns while monitoring packets transfer between two communicated nodes. Besides, from fact 1 and the assertion 1, assertion 2 can be derived that consider some of the immune features.

Assertion (2)**:** *Immune detectors distributed in human body, can be mapped to Ad hoc networks for the purpose of security as a trained agents distributed in an entire nodes in the domain performing the same functions of self detection, anomaly detection, and elimination of the nonself patterns.*

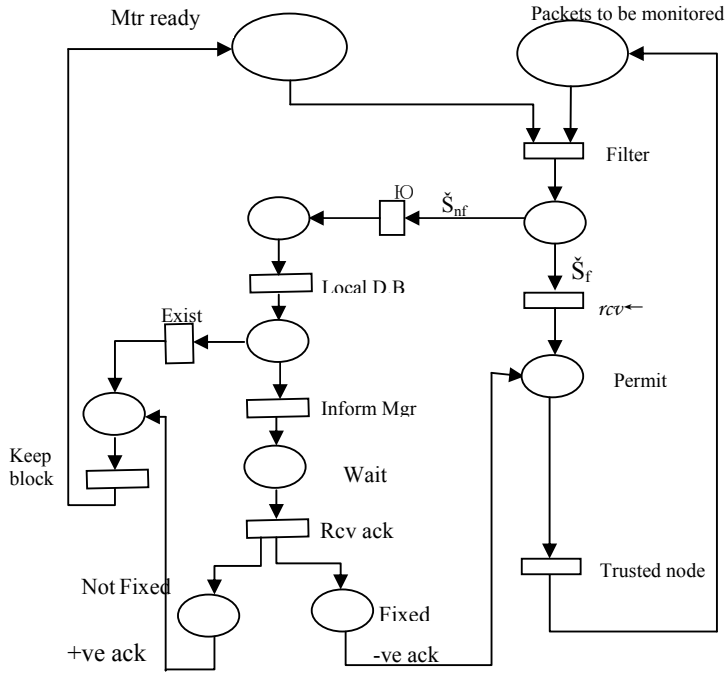

Fig. 5. Basic CPN Model for Monitor Agent.

3.5. Specifying replicate agent

As illustrated in the basic CPN model below (Fig. 6), replicate agent starts the task whenever the two conditions be present, properly configured, and a restore point at the visiting platform is available.

Therefore, it either creates a new entry for the new nodes that join the domain, or updates for an existing ones. From the specification and the CPN model depicted below, assertion (3) can be derived.

Assertion (3): *A timed-controlled intelligent mobile agent can act as a part of an organism self healing system leading to a comprehensive recovery system, therefore, helps to build an immunity-based security system for mobile ad hoc networks.*

Symbolic framework Specifying replicate agent
$\mathcal{R}p \in \{\mathcal{E}\}: (\forall \{\delta\} \in \Phi \Rightarrow SND \ \mathcal{R}p_0$
If IP: =IP$_\delta$ then copy $\mathcal{A}$
IP: =IP$_{Mgr}$ // back to Mgr
If $\mathcal{A} \in \{\mathcal{A}\}$ *then* μ *// already has an entry*
Else n: = n+ 1// create new entry in D.B
Check Γ *then*
Next IP

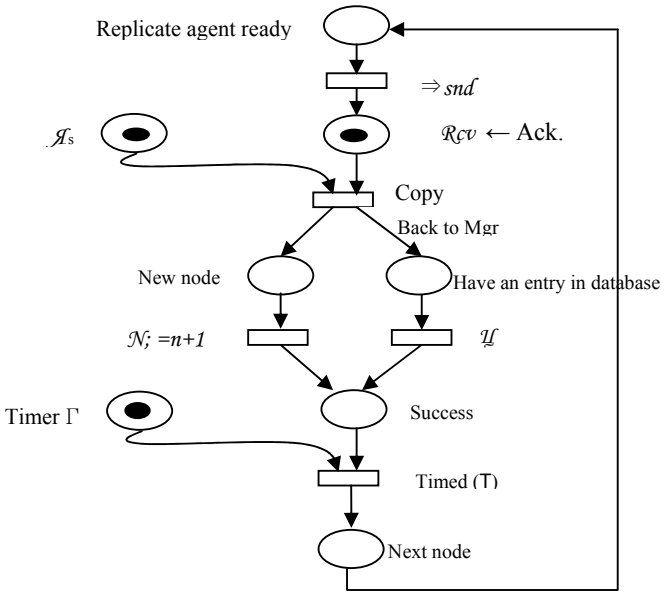

Fig. 6. Basic CPN Model for Replicate Agent.

3.6. Recover agent

Stringent requirements on security and reliability, considering dynamic nature of the ad hoc network, present a motivation for self forming, self-configuring, and self-healing capabilities in the network. As a part of self healing system that specialize the immune system, an attempt is made to add a similar feature to the proposed architecture. The architecture provides an automated feedback loop so that information reported by monitoring agents can be used to automatically trigger correction of nodes problems based on policies that will be specified later. The mobile recover agent carries a restore point to a failure node system (Fig. 7).

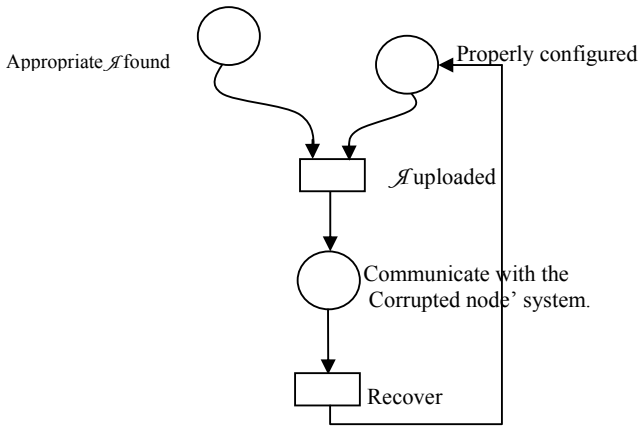

Fig. 7. Basic CPN Model for Replicate Agent.

4. Conclusion and Future Work

In this approach, multi agent system based on the immune system concept has been presented. The whole security system made use of the concept of immune system of human body and map immune system to the security system. Four agents with many roles and functions are proposed to secure a domain in mobile ad hoc networks.

A manager agent controls one static and two mobile agents. A part of self healing system has been applied so as to replicate and recover a failure node system. First response, second memory response, adaptability, maturation, imperfect detection, anomaly detection, and self recovering part, all are some of the immune features that the proposed architecture imitates.

Coloured Petri Net model has been used to describe how different agents coordinate to protect the mobile ad hoc network from intruding and attack. Different agents have corresponding parts in an immune system to map into. A protocol for securing mobile ad hoc networks based on the proposed architecture will be implemented.

References

1. Sergio Marti; T.J. Giuli; Kevin Lai; and Mary Baker (2000). Mitigating routing misbehaviour in mobile ad hoc networks. *In Proceedings of MOBICOM 2000*, 255-265.
2. Forrest, S.; Perelson, A.S.; Allen, L.; and Cherukuri, R. (1994). Self-nonself discrimination in a computer. *IEEE Computer Society Press*, 202-212.
3. Taugchi, A. (1999). The study and implementation for tracing intruder by mobile agent and intrusion detection using marks. *Symposium on cryptography and information security*.

4. Nishiyama, Hiroyuki; and Mizoguchi, Fumio (2003). Design and implementation of security system based on immune system. *Software Security - Theories and Systems Lecture Notes in Computer Science,* Hot Topics No.2609 Springer-Verlag, 234-248.
5. R.B. Machado; A. Boukerche; J.B.M. Sobral; K.R.L. Juca; and M.S.M.A. Notare (2005). A hybrid artificial immune and mobile agent intrusion detection based model for computer network operations. *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium* (IPDPS'05), workshop 6, 191.1.
6. Y. Zhang; W. Lee; and Y. Huang (2003). Intrusion detection techniques for mobile wireless networks. *Wireless Networks and Applications*, 9(5), 545–556.
7. S. Madhavi (2008). An intrusion detection system in mobile Ad hoc networks. *The 2nd International Conference on Information Security and Assurance, (ISA 2008)*.
8. Yi Ping; Yao Yan; Hou Yafie; Zhong Yiping; and Zhang Shiyong (2004). Securing mobile ad hoc networks through mobile agent. *Proceedings of the 3rd international conference on Information* security, ACM International Conference Proceeding Series; Vol. 85, 125- 129.
9. McGibney, J.; Botvich, D.; and Balasubramaniam, S. (2007). A combined biologically and socially inspired approach to mitigating ad hoc network threats. *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, 2010-2014.
10. Zhang, Zeming; Wenjian, Luo; and Xufa Wang (2005). Designing abstract immune mobile agents for distributed intrusion detection. International conference on Neural Networks and Brain, 2005. ICNN&B '05, Vol 2, 748-753.
11. Le Boudec, J.Y.; Sarafijanovic, S. (2004). An artificial immune system approach to misbehaviour detection in mobile ad hoc networks. Proceedings of Bio-ADIT 2004, 96-11.
12. Ritu Chadha; Yuu-Heng Cheng; Jason Chiang; Gary Levin; Shih-Wei Li; Alexander Poylisher (2004). Policy-based mobile ad hoc network management for DRAMA. *Proceedings of the Military Communications Conference (MILCOM 2004)*.
13. Anil Somayaji; Steven Hofmeyr; and Stephanie Forrest (1998). Principles of a computer immune system. *In Meeting on new security paradigms, UK, ACM*, 75-82.
14. Sarafijanovic, S.; and Le Boudec, J.Y. (2005). An artificial immune system approach with secondary response for misbehaviour detection in mobile ad hoc networks. *IEEE Transactions on neural networks*, 16(5), 1013-1303.
15. John E. Hopcroft; Rajeev Motwani; and Jeffery D. Ullman (2006). *Introduction to automata theory, language, and computation* (3rd Edition). Addison-Wesely Longman Publishing Co., USA.