

# Biological Inspired Intrusion Prevention and Self-healing System for Network Security Based on Danger Theory

Muna Elsadig<sup>1</sup>, Azween Abdullah<sup>1</sup>

<sup>1</sup>Department of Computer and Information Science  
Universiti Teknologi PETRONAS  
Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia

---

## Abstract

This paper presents a model for intrusion prevention and self-healing system for network security. The model detects, prevents, and heals harmful events, which are the actual reasons for damage of any of the system's components. The proposed model explores the design and implementation of artificial immune systems (AISs) inspired by the human immune system. A novel approaches for network security based on the combination of biological intrusion prevention (IP) and self-healing concepts are implemented in the proposed model. These approaches are based upon data inspired by the human immune system (HIS), which applied to the autonomous defence system. The system integrates an artificial immune intrusion prevention system for network security inspired by the immunology theory known as danger theory and adaptive immune system. The present model looks at the danger model and its application to attack defence in order to create a fully decentralized model. The intrusion prevention system (IPS) analyzes the behaviour of system processes and network traffic to detect harmful events. Abnormal behaviours are the actual reason for damage of any of the system's components. The detection of the damage caused by different types of malicious events or attack profiles is used to trigger the self - healing (SH) mechanism. This system is autonomous and enhances the fault repair and system recovery.

*Keywords*—Artificial immune system, Network Security, intrusion prevention, Self-healing, agent

---

---

<sup>1</sup> <sup>c</sup> Corresponding Author: S.A. Ibrahim

Email: [saibrahim@um.edu.my](mailto:saibrahim@um.edu.my) Telephone: +607 5046378

Fax: +607 5046378

© 2009-2012 All rights reserved. ISSR Journals

## 1. Introduction

With the explosive growth of the network systems, information exchange became routine between computers around the world, thus the need for network security has become even more critical with the rise of information technology in everyday life [1]. Meanwhile, the complexity of attacks is on the rise regardless of the beefed up security measures. Intrusion Prevention Systems provide an in-line mechanism focus on identifying and blocking malicious network activity in real time.

Immune system presents valuable metaphor for computer security systems and it is an appealing mechanism because firstly, the human immune system defends the body with high level of protection features from pathogens, in a self-organized, robust, distributed and diverse manner. Secondly, current security systems are not able to handle the dynamic and increasingly complex nature of the computer systems and their security needs. In addressing this deficiency, the artificial immune systems (AISs) have been successfully applied to a number of network security problem domain that includes intrusion detection systems, intrusion prevention systems (IPS) and anti-malware systems. This paper looks at the model of computer immune systems and its application to intrusion prevention system combined with self-healing system, that create an autonomous system using agents of multi layers.

The present model focuses on building biologically inspired AIS for intrusion prevention system that has the following security features:

1. Autonomous security system to secure network system; a system that responds effectively to new malicious activities without human intervention. Would significantly improve network security system and optimize the performance.
2. Robust multi layered security system; decrease the false alerts and errors in detecting and preventing malicious activities.
3. Hybrid Intrusion prevention system: a system that has capabilities to detect and prevent anomalies, and misuse of malicious activities.
4. Heal damages caused by attacks; a combination of features between the intrusion prevention system and self - healing mechanism to enhance survival ability of the network systems.

The paper is structured as follows: section 2 the background about IPS, self healing system and HIS is summarized. The autonomous IPS and SH model design is explained in section 3. The algorithms of the designed model are explained in section 4. In section 5 the model features and limitations of model are presented with comparative study. Finally discussion, conclusion and future work are provided in section 6.

## 2. Background

Intrusion prevention systems IPS were developed to resolve ambiguities in passive network monitoring by placing detection systems in-line [1]. The required capabilities, features methodologies and technologies of intrusion prevention system are clarified in [1,2,3]. To achieve secure and multi defense capability of network security system, the hybrid technology has been applied in the proposed model.

### 2.1 Human Immune

The human immune system (HIS) [4] is responsible for an organism's protection against extraterrestrial particles, and is based on two main mechanisms: innate immune system that is an

organism's first line defense and the adaptive immune system. The HIS features are desirable to be adapted to the network security systems to protect them from harmful activities.

The immune system is one of a multilevel dynamic system of cells, molecules, tissues, organs and circulatory systems [5,6]. By this view HIS provides the basis for a representation of intrusion prevention as systems of autonomous agents. The main roles of the adaptive immune system include: the recognition of specific “non-self” antigens in the presence of “self”, during the process of antigen presentation, the generation of responses that are tailored to maximally eliminate specific pathogen infected cells, and the development of immunological memory, in which each pathogen is “remembered” by a signature antibody. All details are explained in [7,8,9]. This matching between antibodies and antigens explains the core of adaptive immune system and most of the first generation of AIS implementations [10,11]. The mechanisms of the innate immune system is usually triggered when microbes are recognized by pattern identification receptors, which identify components that are conserved among broad groups of microorganisms, or when damaged, or stressed cells send out distress signals. Innate immune system responds to pathogens is a generic, meaning the protection mechanisms of these systems are non-specific. Innate immune response are mainly explained in [12,13,14]. The dendritic cells (DCs) that are one of Antigen Presenting Cells (APCs) act as natural data fusion agents. They are present in three statuses of differentiation, immature, semi-mature and mature, which determines their exact role [14]. Variation between the different statuses is dependent upon the receiving of signals while in the initial or immature status. Overall, the classes of input signals are defined in table 1. Signals that point to damage cause a transition from immature to mature; those signals indicating good health in the monitored tissue cause a transition from the immature to semi mature status. Each DC has the capability to combine the relative extent of input signals to produce its own set of output signals. DCs interpret the signals of the antigen presented in an overall to ‘normal’ or ‘anomalous’ context for more details review [12,34].

To achieve the IPS requirements which are: Security capabilities, Performance, Adaptability, Scalability, Configurability and Robustness, the mechanisms of three HIS cells were mapped: Dendritic cells mechanism, B-cell and T-cells. These cooperation mechanisms are effective in the intrusion and prevention, and specification of an intrusion route for the network security [15]. Many immune system approaches to IDS and IPS have been introduced. There are three major extractions, and accordingly three different views: conventional algorithm, negative selection paradigm, and danger theory [16, 17, 18, 19, 20, 21,24,25]. The framework of the present model uses danger theory as forcefulness base for intrusion prevention system integrated with adaptive immune system, mainly T-cell and B-cell [10].

Applying self-healing properties to network systems could present a way to alter the current fault finding in network systems subjected to various abnormal behaviours. When such abnormal behaviour is detected, the proposed system enters a self-diagnosis mode that aims to categorize the fault and extract as much information as achievable with respect to its source, symptoms, and collision on the system. Once these are recognized, the system tries to adapt itself by generating candidate fixes, which are tested to find the best mark state [22]. The self-healing architecture is combined to complement proposed IPS for more automatons damage repair and system continuity, and functionality.

TABLE 1: SIGNALS DEFINITION IN INNATE IMMUNE SYSTEM [23]

Signal	Definition
Safe	A result of normal cell death. Where cells must die for regulatory reasons. The presence of safe signals indicates that no anomalies are present.
Danger	A consequence of unintended necrotic cell death. The presence of danger signal may or may not indicate an anomalous situation.
PAMP	Pathogen - associated molecular proteins (PAMP). Protein expressed exclusively by bacteria. The occurrence of PAMPs usually indicates an anomalous state, which can be detected by DCs.
Inflammation	Produced via the process of injury. Inflammatory signals and inflammatory signals processes are not enough to stimulate DCs alone, their presence amplifies the above three signals.

### 3. Autonomous IPS and SH System

In [26,28], the authors proposed that bio inspired algorithms to be built-up and analyzed in the perspective of a multidisciplinary conceptual framework that represents biological models. In this work, an analytical computational framework has been built and authenticated based upon this conceptual framework. These frameworks provide principle for designing and analyzing bio-inspired algorithms applicable to non-biological problems. In Figure 1 the abstract design and the model components of IPS and self-healing system are shown. The main agent components of IPS model are: sense agent (SEA), analysis agent (ANA) and the adaptive agent (ADA). SHA agent is combined with the IPS to include additional enhanced mechanism for self-healing purposes. One of the central features of the model is that it needs both expert knowledge and training data. Each agent in the model performs training on multiple types of input data within a specific period. Meanwhile, the model's main requirement is in building an expert knowledge base that assigns input signals and rules to appropriate category. Two knowledge base systems are used, one for misuse attack and the other for self-healing purposes. In autonomous multi-agent system, every agent has its own goals, which drive its decisions. The individual goals of each agent must be specified such that the preferred universal goals of the whole system are achieved [30]. The main three agents *SEA*, *ANA*, and *ADA* form three different function layers. For each agent we specify and identify the states and transitions of each agent according to how an agent behaves with respect to changes in its environment [31, 32]. The environment of each agent consists of a set of states  $S$  and the agent can undertake a set of actions  $A$  and a set of percept  $P$ . The abstract architecture is modeled as a discrete-event system using Petri nets. The structural analysis of the net provides an assessment of the communication and coordination properties of the multi-agent system. Deadlock avoidance in the multi-agent system is considered as an initial key property, and it is evaluated using liveness and boundedness properties using linear algebra.

A Petri net base for the IPS and SH system is defined as a five-tuple  $(P, T, A, W, M_0)$ .

Where;

$P$  is a finite set of places.

$T$  is a finite set of transitions.

$A \subseteq (P \times T) \cup (T \times P)$ .

$W: A \mapsto \{1, 2, 3, \dots\}$  is a weight function.

$M_0: P \mapsto \{1, 2, 3, \dots\}$  is the initial marking.

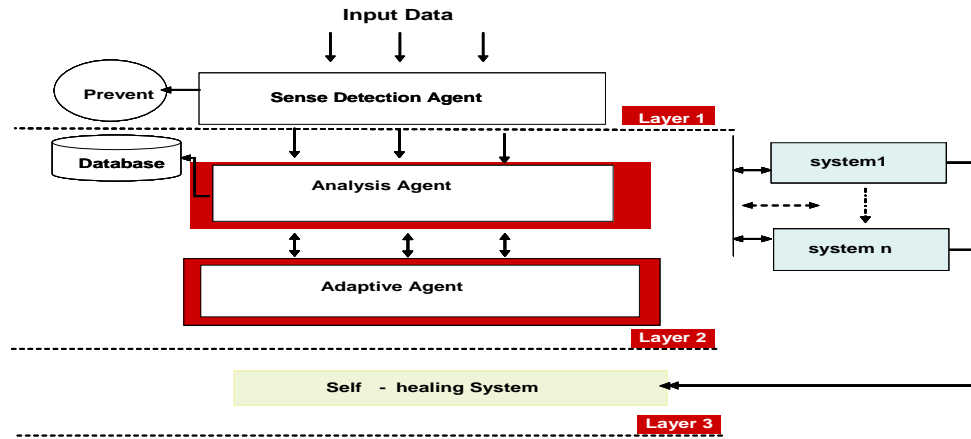


Figure 1: IPS and Self-healing Model for Network System

According to these formulas, a Petri net for the four agents was built and represented graphically. In the analysis we used P-invariants and T-invariants obtained from the incidence matrix [33].

The incidence matrix  $A$  of a Petri net has  $|T|$  number of row and  $|P|$  number of columns.

$$A \text{ P-invariant is a vector that satisfies } A_x = 0 \quad (1)$$

$$T \text{ invariant is a vector that satisfies } A_y^T = 0 \quad (2)$$

A Petri net model is covered by P-invariants, if and only if, for each place  $s$  in the net, there exist a positive P-invariant  $x$  such that  $x(s) > 0$ .

Petri net is structurally bounded if it is covered by P-invariants and initial marking  $M_0$  is infinite.

Further a Petri net is covered by T-invariants, if and only if, for each transition  $t$  in the net  $y(t) > 0$ .

Under this condition, Petri net is live and bounded if it is covered by T-invariants. The conditions for the liveness and boundedness properties were proven to obtain the marking reachability graph [36,37,38]. For each agent, the environment undertaken sets of states  $S$ , actions  $A$  and precept  $P$  has the behaviour represented by the function action:

$$P \mapsto A,$$

and perception function

$$S \mapsto P,$$

and deterministic behaviour of an environment can be represented by the function

$$env: S \times A \mapsto S.$$

### 3.1. Sense Agent (SEA)

The sense agent (SEA) performs the followings:

- Dynamically learns and trains to build a generic knowledge about all the network system normal behaviour (self) for example: system calls, ports and IP addresses. In the training period, all antigens and signal are defined according to the specific scanning criteria.
- Senses all input to the network system and compares it with data set that SEA has trained, and then decides whether it is a source of malicious activities. This is performed and inspired from how DC and tissue sense or capture the danger signal.
- If detection of abnormal behaviour is established, SEA prevents the malicious activities.
- Sends detection message to ANA and Starts retraining dynamically.

The roles, function, and responsibilities of *SEA* are specified logically as follows:

The set of roles ( $R_{SEA}$ ) of the sense agent *SEA* is:

$$R_{SEA} = \{sense\ input\ data\}$$

The set of function  $F_{SEA}$  of the sense agent *SEA* is:

$$F_{SEA} = \{learn\ normal\ behaviour,\ block\ abnormal\ behaviour\}$$

The set of responsibilities  $P_{SEA}$  of the sense agent *SEA* is:

$$P_{SEA} = \{detect\ malicious\ activities,\ send\ detection\ message\ to\ ANA\}$$

The SEA Model states, actions and precept specified as follows

Set of states = {configure, train, detect, complete prevention, continue }

$$S_{SEA} = \{s_1, s_2, s_3, s_4, s_5\}$$

Set of actions = {configure completed, scan, block, detection message, permit }

$$A_{SEA} = \{a_1, a_2, a_3, a_4, a_5\}$$

Set of percepts = {training, detection, prevention, communication analysis agent, continue connection }

$$P_{SEA} = \{p_1, p_2, p_3, p_4, p_5\}$$

For SEA agent each  $j^{th}$  environment has the state:

$$s_{SEAj} \in S_{SEA}$$

Similarly  $A_{SEA}$  be the set of actions of *SEA*;

$$a_{SEAk} \in A_{SEA}$$

where  $K^{th}$  actions of *SEA*. These definitions have been used to build the Petri net sub – model of the *SEA* agent. The incidence matrix for *SEA* is obtained from the Petri net graph and both P-invariant and T-invariant satisfy the conditions mentioned above. The  $T_{SEA}$  and  $P_{SEA}$  invariants for *SEA* vectors are:

$$I_{SEA} = \begin{matrix} & a_1 & a_2 & a_3 & a_4 & a_5 \\ p_1 & -1 & 0 & 0 & 1 & 0 \\ p_2 & 1 & -1 & 0 & 0 & 0 \\ p_3 & 0 & 1 & -1 & 0 & 0 \\ p_4 & 0 & 0 & 1 & -1 & 0 \\ p_5 & -1 & 0 & 0 & 0 & 1 \end{matrix} \quad , \quad T_{SEA} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \quad , \quad P_{SEA} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Figure 2 shows the behaviour of the *SEA* states and transitions which satisfy the properties of liveness and boundedness and proof the reachability feature of the *SEA*.

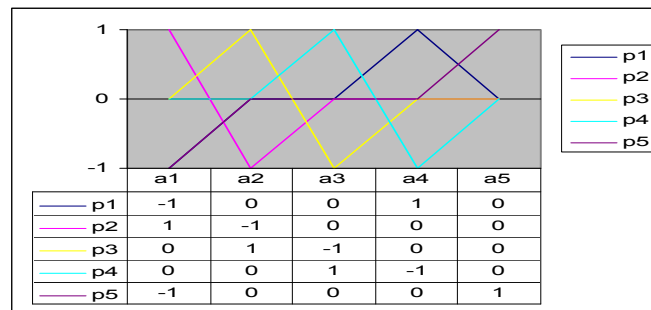


Figure 2: the SEA Transition a and State p graph

### 3.2 Analysis Agent (ANA)

The analysis agents ANA performs the followings:

- Receives detection message from SEA, and then ANA analyzes the received information to extract the malicious signature.
- ANA scans the misuse database to search for a matching signature. If a match is found then the malicious signature is considered as a misuse. ANA checks the system behaviour and if there any abnormal activities detected, ANA sends MisusehealMsg to SHA. Or else, ANA considers the malicious signature as an anomaly and sends AnomalyMsg to ADA.
- ANA waits for RecognitionMsg from ADA which contains the recognition information of the anomaly, and then updates the database records.
- Checks system behaviour if there is any abnormal behaviour caused by the malicious activity, and then ANA sends Anomalyhealmsg to SHA.

The roles, functions, and responsibilities of ANA are specified logically as follows:

The set of roles  $R_{ANA}$  of the analysis agent ANA is:

$$R_{ANA} = \{analyze\ abnormal\ behaviour\}$$

The set of function  $F_{ANA}$  of the analysis agent ANA is:

$$F_{ANA} = \{distinguish\ misuse\ attack\ from\ anomaly\ attack,\ analyze\ attack\ behaviour\}$$

The set of responsibilities  $P_{ANA}$  of the analysis agent ANA is:

$$P_{ANA} = \{receive\ DetectionMsg\ from\ SEA,\ send\ AnomalyMsg\ to\ ADA\ agent,\ receive\ RecognitionMsg\ from\ ADA\ agent,\ call\ self-healing\ system\}$$

The ANA Model states, actions and precept specified as follows

Set of states = {configure, monitor, analyze, decide, wait, update }

$$S_{ANA} = \{s_1, s_2, s_3, s_4, s_5, s_6\}$$

Set of actions= {configure completed, DetectionMsg, scan, MisusehealMsg , send AnomalyMsg, Receive RecognitionMsg, AnomalyhealMsg, register }

$$A_{ANA} = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$$

Set of percepts={monitoring, analyzing, decision, receiving, sending, updating}

$$P_{ANA} = \{p_1, p_2, p_3, p_4, p_5, p_6\}$$

For ANA agent each  $j^{th}$  environment has the state:

$$s_{ANAj} \in S_{ANA}$$

Similarly  $A_{ANA}$  be the set of actions of ANA;

$$a_{ANAk} \in A_{ANA}$$

where  $K^{th}$  actions of ANA

We use these definitions to build the Petri net sub – model of the ANA agent. The incidence matrix for ANA obtained from the Petri net graph and both P-invariant and T-invariant satisfy the conditions mentioned above. The  $T_{ANA}$  and  $P_{ANA}$  invariants for ANA vectors are:

$$I_{ANA} = \begin{matrix} & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 \\ p_1 & -1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ p_2 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ p_3 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ p_4 & 0 & 0 & 1 & -1 & -1 & 0 & 0 & 0 \\ p_5 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ p_6 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & -1 \end{matrix}, \quad T_{ANA} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad P_{ANA} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Figure 3 shows the behaviour of the ANA states and transitions which satisfy the properties of liveness and boundedness and proof the reachability feature of the ANA.

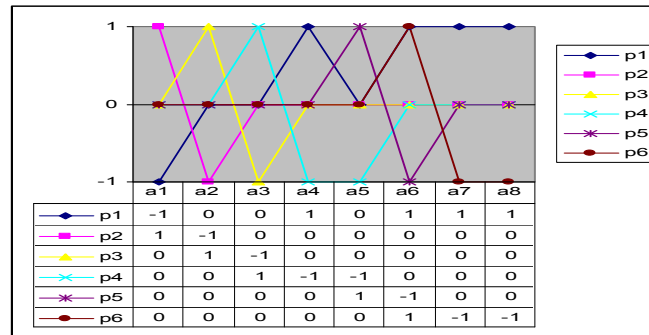


Figure 3: the ANA Transition a and State p graph

### 3.3 Adaptive Agent (ADA)

The adaptive agents *ADA* performs the followings:

- Receives the AnomalyMsg from *ANA* and triggers adaptation method to anomaly behaviour.
- Recognizes and registers the anomaly behaviour signature.
- Sends RecognitionMsg to *ANA* that identifies the malicious anomaly and contains information required for database registration.
- The distributed immune agents have the abilities of self-learning, expert knowledge, memory, work autonomously and decartelized Learn.

The roles, functions and responsibilities, and interaction of *ADA* are specified logically as follows:

The set of roles of the adaptive agent *ADA* is:

$$R_{ADA} = \{adaptationToanomaly, regognize anomaly\}$$

The set of function  $F_{ADA}$  of the analysis agent *ADA* is:

$$F_{ADA} = \{adaptationToanomaly check adaptation to anomaly\}, recognize anomaly\}$$

The set of responsibilities  $P_{ADA}$  of the analysis agent *ADA* is:

$$P_{ADA} = \{anomaly signature, feedback to analysis agent\}$$

The *ADA* Model states, actions and precept specified as follows:

Set of states = {configure, monitor, adaptation, recognize}

$$S_{ADA} = \{s_1, s_2, s_3, s_4\}$$

Set of actions = {configure completed, received AnomalyMsg, fix adaptation, send AnomalyhealMs }

$$A_{ADA} = \{a_1, a_2, a_3, a_4\}$$

Set of precepts = {configuration, monitoring, receiving, adaptation, recognition, sending}

$$P_{ADA} = \{p_1, p_2, p_3, p_4, p_5\}$$

For *ADA* agent each  $j^{th}$  environment has the state:

$$s_{ADAj} \in S_{ADA}$$

Similarly  $A_{ADA}$  be the set of actions of *ADA*;

$$a_{ADAk} \in A_{ADA}$$

where  $K^{th}$  actions of *ADA*.

We use these definitions to build the Petri net sub-model of the *ADA* agent. The incidence matrix for *ADA* obtained from the Petri net graph. Both *P*-invariant and *T*-invariant satisfy the condition mentioned above. The  $T_{ADA}$  and  $P_{ADA}$  invariants for *ADA* vectors are:

$$I_{ADA} = \begin{matrix} & a_1 & a_2 & a_3 & a_4 \\ p_1 & -1 & 0 & 0 & 1 \\ p_2 & 1 & -1 & 0 & 0 \\ p_3 & 0 & 1 & -1 & 0 \\ p_4 & 0 & 0 & 1 & -1 \end{matrix} \quad T_{ADA} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad , \quad P_{ADA} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Figure 4 shows the behaviour of the *ADA* states and transitions which satisfy the properties of liveness and boundedness and proof the reachability feature of the *ADA*.

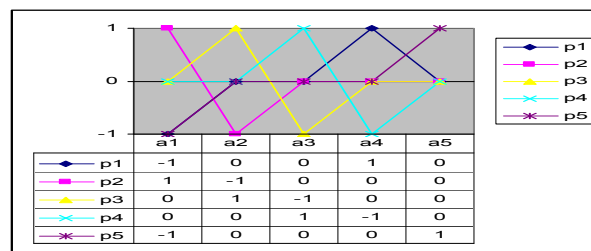


Figure 4: the *ADA* Transition and State p graph

### 3.4 Self – healing Agent (*SHA*)

The Self-healing agent *SHA* performs the followings:

- Receives MisusehealMsg and Anomalyhealmsg from *ANA* agent about harmful malicious activities.
- Diagnoses the system behaviour, captures the fault identification, and extracts anomaly activities configuration.
- *SHA* is an expert knowledge and is trained to adapt to abnormal activities using inspired cell regeneration mechanism.
- Generates fix candidates for each fault and repairs the specific damages caused by harmful activities.
- Finally Performs self - testing for the newly regenerated damaged component and deploys it.

The roles, functions and responsibilities, and interaction of *SHA* are specified logically as follows:

- The set of roles  $R_{SHA}$  of the self healing agent *SHA* is:  
 $R_{SHA} = \{ \text{self-healing} \}$
- The set of function  $F_{SHA}$  of the analysis agent *SHA* is:  
 $F_{SHA} = \{ \text{diagnoses, fault adaptation, testing} \}$
- The set of responsibilities  $P_{SHA}$  of the analysis agent *SHA* is:  
 $P_{SHA} = \{ \text{receive msg, fault identification, candidaet fix generation, deployment} \}$

The *SHA* Model states, actions and precept specified as follows :

Set of states =  $\{ \text{create, train, fault diagnosis, fault adaptation, self test} \}$

$S_{SHA} = \{ s_1, s_2, s_3, s_4, s_5 \}$

Set of actions =  $\{ \text{configure, received message, fault identification, candidate fix generation, deployment} \}$

$A_{SHA} = \{ a_1, a_2, a_3, a_4, a_5 \}$

Set of precepts= $\{training, receiving, fault adaptation, testing, deployment\}$

$$P_{ADA} = \{p_1, p_2, p_3, p_4, p_5\}$$

For *SHA* agent each  $j^{th}$  environment has the state:

$$s_{SHAj} \in S_{SHA}$$

Similarly  $A_{SHA}$  be the set of actions of *SHA*;

$$a_{SHAk} \in A_{SHA}$$

where  $K^{th}$  actions of *SHA*

These definitions have been used to build the Petri net sub – model of the *SHA* agent. The incidence matrix for *SHA* obtained from the Petri net graph, and both *P*-invariant and *T*-invariant satisfy the conditions mentioned above. The  $T_{SHA}$  invariant and  $P_{SHA}$  invariant for *SHA* vectors are:

$$I_{SHA} = \begin{matrix} & a_1 & a_2 & a_3 & a_4 & a_5 \\ p_1 & -1 & 0 & 0 & 0 & 1 \\ p_2 & 1 & -1 & 0 & 0 & 0 \\ p_3 & 0 & 1 & -1 & 0 & 0 \\ p_4 & 0 & 0 & 1 & -1 & 0 \\ p_5 & 0 & 0 & 0 & 1 & -1 \end{matrix}, T_{SHA} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, P_{SHA} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Figure 5 shows the behaviour of the *SHA* states and transitions which satisfy the properties of liveness and boundedness and proof the reachability feature of the *SHA*.

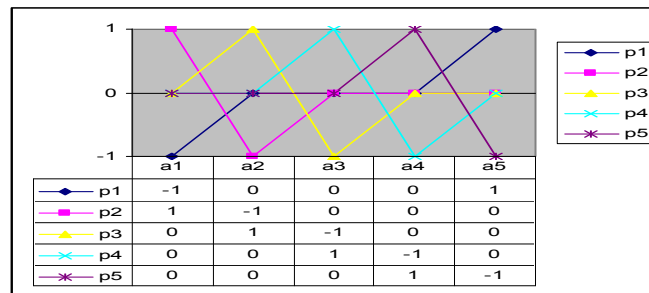


Figure 5: the *SHA* Transition and State p graph

#### 4. IPS and SH Algorithms

The mechanism of DC is mapped and is represented by Sense agent, which has the following constituents:

- As an agent it must have the ability of multi signaling processing And Receptors for each processed input signals are pre defined and updated periodically
- Antigen set that correlated with the input signals and receptors that are predefined.
- Sampling the binding between the receptors and the relation set of antigen and input signals.

This agent must perform the follows:

- Calculate the rate of the binding process.
- Represent the output signal predefined as danger or safe signal to the T-cells.
- Prevent the damage behaviour when the rate exceeds the threshold.

The steps of the detection and prevention algorithm can be represented as illustrated in Figure 6. Firstly, the categories vector that the system must monitor must be specified; according to this we have to define the matrix of signals. For each category, the signal matrix has a relation with

a specific set of receptors. This relation produces a set of antigens related to specific components of signals and receptors. This relation gives the context of the abnormal behaviour that generates two types of output signal: safe signal, or danger signal.

The vector of categories can be defined as;

$$CG_I = [CG_1, \dots, CG_I] \quad 0 \leq i \leq I \quad //N \text{ number of categories}$$

The matrix of the input signals;

$$S_L = [S_1, \dots, S_L] \quad 1 \leq l \leq L \quad //L \text{ number of signal per categories}$$

Vector of receptors;

$$C_H \rightarrow CG_I \times S_L \quad 1 \leq h \leq H \quad //H \text{ number of receptors per categories per period of time } t$$

Vector of produced antigens according to produced receptors per categories

$$A_N = [a_1, \dots, a_n]$$

The set of context per antigen per period of time  $t$ ;

$$R \rightarrow C \times (S \times A)$$

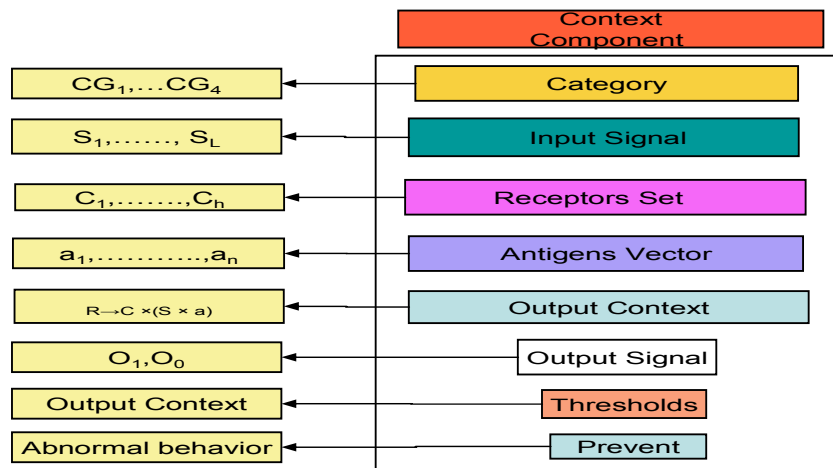


Figure 6: Detection and Prevention Algorithm Steps

During a period time  $t$ , the behaviours contexts are accumulated in  $R$ .

Where;

$$R = R' \cup R''$$

$R'$  is the set of normal behaviour context,

$R''$  is the set of abnormal behaviour context,

$\delta$  The rate of the accumulated abnormal context.

$$\delta = \frac{\sum_{t=0}^T R''}{T} \begin{cases} 0 < \delta < 1 \\ 0 \leq t \leq T \end{cases}$$

The output signal  $O$  is examined against the threshold  $Thd$ .

$$O = \begin{cases} 1 & \delta > Thd & //\text{danger signal or attack detected} \\ 0 & \delta < Thd & //\text{safe signal or normal behaviour} \end{cases}$$

T-cell, which is represented by the analysis agent in this model functions to analyze the signal in terms of abnormal behaviour context. When the analysis agent receives the danger signal, it starts searching the knowledge database, and compares the abnormal behaviour context  $R''$ .

$$\left\{ \begin{array}{l} \in [M_u][B_u] //\text{Misused abnormal behaviour } R''_x \end{array} \right.$$

$\notin [M_u][B_u]$  //Anomaly abnormal behaviour

$[M_u][B_u]$  is the database set of misuse abnormal behaviours.

$\forall R_x'' \in [M_u][B_u] \exists O_{Misuse}$  to *SHA* //  $O_{muse}$  is heal misuse message to the self – healing agent.

$\forall R_x'' \notin [M_u][B_u] \exists O_{Anomaly}$  to *ADA* //  $O_{anomaly}$  is adaptation message to the adaptive agent.

The adaptive agent receives the  $O_{anomaly}$ , tries to recognize the abnormal behaviour, and calculate the distance between the normal behaviour context  $R'$  and abnormal behaviour context  $R''$

which is given by  $f_{dis}(R'', R') = \sqrt{\sum_{x=1}^l (R_x'' - R_x')^2}$   $\forall f_{dis} \exists S(R'')$  // value of  $f_{dis}$  gives the deviation from the normal behaviour

Where,  $S(R'')$  is the function of the signature extraction that distinguishes between abnormal distinguishes abnormal from normal behaviours. The adaptive agent maps the mechanism of B-cell, which produces adaptive antibodies to recognize the pathogens. Adaptive agent sends  $S(R'')$  and  $f_{dis}$  characteristics to the analysis agent to update the knowledge base database. As the self-healing agent receives the healing message from the analysis agent that contains the abnormal behaviour, characteristics and the damage behaviour.

*SYS* is a set of system component in normal behaviour state,

$J$  = total number of the component

$$SYS = \{sys_1, \dots, sys_j\} \quad I < J < \infty$$

After intrusion occurred'

$$\forall sys_j \exists sys_j' \in SYS' \quad // \text{set of damaged system components.}$$

Where;

$$sys_j' = f'(sys_j) \quad f' \quad // \text{is function cause the damage.}$$

*SHA* has a knowledge base containing all candidate system components such that;

$\forall sys_j' \exists heal_k \in Heal_K$  set of healing function that heals the damaged system component.

$$heal_k(sys_j') = f'(sys_j')$$

where

$$S(R'') - S(R') = 0$$

If the above result finds the healing component, which is identified as the successful candidate then the healing component will be deployed, and tested to keep the system continuity.

## 5. Discussion

This model maps the efficient features of HIS. The IPS which combined with SH system is Robust to secure network system with high efficiency. The model is expected to give less rates of false positive and false negative detection error. Moreover, the self-sufficiency in nature of the model by using agents' paradigm shows more efficiency in reducing the period of detection and the corresponding response time for prevention and healing. The interest of this work is in improving the elements of the system that perform the monitoring, diagnosis and healing the abnormal activities damages to carry on system continuity. Meanwhile the model may show limitation in

scalability feature. This is because the sensitivity of defining the categories of authorized normal behaviour and the specification of healing knowledge base in very large network. Recently, new research and algorithm in *AIS* are focusing on building systems that have more biological resemblance, inspired by both the innate and adaptive immune systems. Table 2 illustrates a comparison between the proposed model and the three algorithms for intrusion detection and prevention, which have been based on the danger model as second-generation of artificial immune system.

TABLE 2: COMPARISON BETWEEN THE PROPOSED MODEL AND OTHER DANGER MODELS FOR INTRUSION DETECTION AND PREVENTION SYSTEM

<b>AIS</b>	<b>DCA Algorithm[14]</b>	<b>TLR Algorithm[35]</b>	<b>Adaptive IPS approach[11]</b>	<b>IPS and SH Model</b>
Adaptive immune system		√	√	√
Innate immune system	√	√	√	√
Knowledge base	√		√	√
Training base		√		√
Prevention mechanism			√	√
Self-healing mechanism				√
Standard antigen database	√	√		√
Standard signal database	√	√		√
Processing signal	√		√	√

## 6. Conclusion and Future work

In this paper we have described a novel model for biological intrusion prevention and self-healing system. The model is inspired by the danger theory (dendritic cell, tissue), adaptive immune system (T-cell, B-cell), and human cell regeneration, and has agents paradigm. The approach maps some pertinent features of the immune system to IPS: dynamic, self-monitoring, self-adapting, autonomous and distributed security system. The agent's function and structural specifications are detailed and grouped into sets of roles, functions and responsibilities. The functional algorithms for each agent built upon the specification model are constructed. Network systems are highly autonomously, secured by using the bio prevention mechanisms. Moreover, the self-healing features ensure the survival ability of these systems. For future work, we intend to simulate, prototype, and implementation the model in addition to model reliability testing, which will be carried out as well.

## References

- [1] Andreas.F (2005). "Intrusion Detection Systems and Intrusion Prevention Systems". In Information Security Technical Report ,10, 134e139, Elsevier Ltd.
- [2] Karen. S, P. Mell (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". In National Institute of Standards and Technology Special Publication 800-94 ,Natl. Inst. Stand. Technol. Spec. Publ. 800-94, 127 pages
- [3] NIST (Nov. 2001). "Intrusion detection systems". In NIST Computer Science Special Reports SP 800-31.
- [4] Hofmeyr.S.A, S. Forrest (1999). "Immunity by design: an artificial immune system", Proceedings of the Genetic and Evolutionary Computation Conference, pp.1289–1296.

- [5] Steven H.A (1997). " An Overview of the Immune System", <http://www.cs.unm.edu/immsec/html-imm/immune-system.html>,
- [6] Jamie. T, U. Aickelin (2007). " Biological Inspiration for Artificial Immune Systems ", School of Computer Science, University of Nottingham, UK, [jpt@cs.nott.ac.uk](mailto:jpt@cs.nott.ac.uk).
- [7] Charles .J, P. Travers, M. Walport, and M. Shlomchik (2005). "Immunobiology: The Immune System in Health and Disease". Garland Publishing. Available online at <http://www.ncbi.nlm.nih.gov/books/>, 6th edition.
- [8] John .I.T, (September 2001). "Artificial immune systems - A novel data analysis technique inspired by the immune network theory", PhD Thesis, University of Wales.
- [9] Azzedine. B, R. B. Machado, K.R.L. Juca, J.Bosco M. Sobral , Mirela S.M.A. Notare (March 2007). "An agent based and biological inspired real-time intrusion detection and security model for computer network operations a Paradise", Elsevier B.V pages 2649-2660.25.
- [10] Stephanie A.F, S. A. Hofmeyr , A. Somayaj (1997). "Computer Immunology", Communications of the ACM, Vol. 40, No. 10, pp. 88–96.
- [11] Alexander.K and M. Alexander (2008). " An Approach for Adaptive Intrusion Prevention Based on The Danger Theory", IEEE Xplore.
- [12] Alberts.B, A. Johnson, J. Lewis, M. Raff, K. Roberts, P. Walters (2002). Molecular Biology of the Cell, Fourth Edition. New York and London. Garland Science. ISBN 0-8153-3218-1. <http://www.ncbi.nlm.nih.gov/books/bv.fcgi?call=bv.View..ShowTOC&rid=mboc4.TOC&depth=2>.
- [13] Charles .J, C. P. Travers, M. Walport, M. Shlomchik (2001). Immunobiology; Fifth Edition. New York and London, Garland Science. ISBN 0-8153-4101-6. <http://www.ncbi.nlm.nih.gov/books/bv.fcgi?call=bv.View..ShowTOC&rid=imm.TOC&depth=10>.
- [14] Julie . G, U. Aickelin, S. Cayzer (2005). " Introducing dendritic cells as a novel immune – inspired algorithm for anomaly detection", ICRRIS05.LNCS, vol. 3627, pp.153-67.
- [15] Hiroyuki.N, M. Fumio (2003). " Design and Implementation of Security System Based on Immune System", Springer-Verlag Berlin Heidelberg, ISSS 2002, LNCS 2609, pp. 234–248-
- [16] Kephart J. O, G. B. Sorkin, W. C. Arnold, D. M. Chess, G. J. Teasuro, and S. R. White (1997). "Biologically Inspired Defences against Computer Viruses". In Machine Learning and Data Mining: Method and Applications, pp. 313-334, John-Wiley & Son-
- [17] Thomas. P and E. D. Carosella (2006). " The Self Model and the Conception of Biological Identity in Immunology. Biology and Philosophy", 21(2), pp. 235–252.
- [18] Stephanie A.F, S. Perelson, L. Allen, and R. Cherukuri (1994). "Self-nonsel self discrimination in a computer". In Proceedings of the 1994 IEEE Symposium on Security and Privacy, pp. 202, IEEE Computer Society-

- [19] Kim, J., P. J. Bentley, U. Aickelin, J. Greensmith, G. Tedesco, J. Twycross (2008). "Immune System Approaches to Intrusion Detection - A Review". Natural Computing, Springer.
- [20] Kim J. Bentley P. (July 2001). "Evaluating negative selection in artificial immune system for network intrusion detection". In proceedings of GECCO, pp.1330-7.
- [21] U. Aickelin and S. Cayzer (2002). "The Danger Theory and Its Application to AIS". Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS-2002), pp. 141-148.
- [22] Angelos. D. K (2008). "Characterizing Self-Healing Software Systems".
- [23] Julie . G, J. Feyereisl, U. Aickelin (2008). "DCA:SOME comparison a comparative study between two biologically-inspired algorithm". School of Computer Science, University of Nottingham, UK, [jpt@cs.nott.ac.uk](mailto:jpt@cs.nott.ac.uk).
- [24] Julie . G, U. Aickelin (2007). "Dendritic Cells for SYN Scan Detection". London, England, United Kingdom. ACM 978-1-59593-697-4/07/0007.
- [25] Morton.S (2006). "Using the danger model of immune systems for distributed defense in modern data networks", Elsevier.
- [26] Susan. S, R. Smith, J. Timmis, and A. Tyrrell (2004). "Towards a Conceptual Framework for Artificial Immune Systems". In Proc. of the 3rd International Conference on Artificial Immune Systems, LNCS 3239, pp. 53-64, Catania, Italy.
- [27] Leandro. N. de. C and J. Timmis (2002). "Artificial Immune Systems: A New Computational Intelligence Approach". Springer.
- [28] Susan .S, R. Smith, J. Timmis, A. Tyrrell, M. Neal, and A. Hone (2005). "Conceptual Frameworks for Artificial Immune Systems". International Journal of Unconventional Computing, 1(3):315-338.
- [29] Seleznyov.A (Sept. 21, 2002). "An Anomaly Intrusion Detection System Based on Intelligent User Recognition", Faculty of Information Technology of the University of Jyväskylä, in the Building Agora, (Ag Aud. 2).
- [30] Kim .J and P. Bentley (Sept. 1999). "The human immune system and network intrusion detection". In Proc. Of European Congress on Intelligent Techniques and Soft Computing (EUFIT '99), Aachen, Germany.
- [31] Elizabeth .K (June 2001). "Agent software Engineering with role modeling". In P. Ciancarini and M. Wooldrige, editors, first international workshop of Agent-Oriented Software Engineering, AOSE 2000, number 1957 in LNCS ,pp. 163-170, Limerick, Ireland, Springer-Verlag
- [32] Kephart .J. O. and D. M. Chess (Jan. 2003). "The Vision of Autonomic Computing Computer". IEEE, Volume 36, Issue 1, pp. 41-50.

- [33] Jose R..a, Alan A. . Desrochers, R. J. Graves (2009). “ Modeling and Analysis of Multi-agent Systems using Petri nets”. 1439 1-4244-0991-8/07©2007 IEEE.
- [34] Uwe. Aand J .Greensmith (2007). “ Sensing danger: Innate immunology for intrusion detection ”. Information Security Technical Reports I 2, pp. 218-227, Elsevier Ltd.
- [35] Jamie. T, (2007). “ Integrated Innate and Adaptive Artificial Immune Systems applied to Process Anomaly Detection”. PhD thesis, School of Computer Science, University of Nottingham, U.K.
- [36] Muna. E,A.Abdullah,(2008).” Bio Inspired Intrusion Prevention and Self-healing Architecture for Network Security”, “Innovations in Information Technology conference” Innovation08 , Dubai.
- [37] Muna. E,A.Abdullah,(2009).” Biological Hybrid Intrusion Prevention and Self-healing Model for Network Security”, International Conference on Future Computer and Communication (ICFCC 2009) , kuala lumpur.
- [38] Muna. E, A.Abdullah, (2009).” Hybrid Biological Intrusion Prevention and Self-healing for Network Security”, National Postgraduate Conference (NPC09), university technology petronas.

**APPENDIX 1**

## TERMINOLOGY AND ABBREVIATIONS

Term	Description
SEA	Sense Agent
ANA	Analysis Agent
ADA	Adaptive Agent
SHA	Self Healing Agent
Normal behaviour	Authorized and normal system activities
Abnormal behaviour	Unauthorized and abnormal system activities caused by attacks or malware
Malicious activity	Attacks and malware
DetectionMsg	Message from SEA to ANA which contains all information about the behaviour or malicious activity detected
MisusehealMsg	Message from ANA to SHA which contains all information about the misuse abnormal activities and system behaviour
AnomalyMsg	Message from ANA to ADA which contains the available information in order to recognize the malicious anomaly