Critical Infrastructure Automated Immuno-Response System (CIAIRS)

Sahar Badri, Paul Fergus, William Hurst
Department of Computer Science,
Liverpool John Moores University,
Byrom Street
Liverpool, L3 3AF, UK
S.KBadri@2010ljmu.ac.uk, P.Fergus, W.Hurst{@ljmu.ac.uk}

Abstract— Over the last decade, critical infrastructures have become increasingly complex. They now possess levels of automation which requires the integration of, often, mutually incompatible technologies. In addition, the data sets generated are t, vast and intricate level of interdependency between infrastructures has grown. Any failures, caused by cyber-attacks, have the ability to spread through a system of systems and are a challenge to detect. Therefore, this paper firstly discusses the interdependency challenges facing critical infrastructures; and how it can be used towards creating a support network against cyber-attacks. In much the same way as the human immune system is able to respond to intrusion, our proposed system is able to detect cyber-attacks and share the knowledge with interconnected partners. In order to demonstrate our approach, a simulation framework of 8 critical infrastructures is presented. Furthermore, our big data analysis techniques, used to identify and share threats between infrastructures, are discussed in depth.

Index Terms— Critical Infrastructure, Big Data, Cyber-Security, Simulation, Data Analytics, Immune System, Interdependency

1. INTRODUCTION

Critical infrastructures play a significant role in the world around us. Their service provision has become more widespread, to the point where it is ubiquitous in many societies [1]. To maintain continuous supply, infrastructure interconnectivity has become highly complex; particularly due to the increase in demand for the amenities. This has led to an increased interdependence between infrastructures and their underlying physical layers. One infrastructure's provision relies heavily on another. Due to this increased connectivity, now, more than ever before, critical infrastructures face a number of possible digital threats. In result, Critical Infrastructure Protection (CIP) has become an significant topic for research focus [2].

This interdependency challenge, within the critical infrastructure system of systems, has the potential to cause a cascading effect, with unprecedented disaster outcomes. Therefore, understanding the interconnectivity behaviour between the CI's, and how it changes depending on the complexity, can help in reducing the effect before cascading occurs. This would control the damage and limit the impact [4].

Every new interdependency reveals a fresh vulnerability in the system of systems, which creates new attacks risks [5]. The research presented in this paper, focuses on understanding the links between critical infrastructures. The aim is take advantage of the concept of an immune system characteristic to simplify and predict potential problems before they spread through a network of infrastructures. As with any other systems, critical infrastructure faces a number of possible types of digital attack. In this paper, a system framework, which is able to identify threats to a network and communicate the potential impact, is put forward. The system is evaluated using data constructed through a simulation of a network of critical infrastructures. Data analysis is conducted using data classifiers to identify system anomalies and present a model of behaviour to share with other infrastructures.

The paper is organised as follows. Section 2 presents a background discussion on critical infrastructures, interconnectivity in a system of systems and on mapping the concept of an immune system to a computing environment. Section 3 highlights the data collection process used for our system design and development. Section 4 provides an overview of the system framework and presents initial results. A discussion of the findings is put forward in Section 5 and the paper is concluded in Section 6.

2. BACKGROUND

Critical infrastructures (CI) are defined as the arrangement of both systems and assets, which are essential and affect the security, economy, public health or safety of a nation [6][7]. As Command *et al*., detail, critical infrastructures, can be divided into three groups: physical assets, human assets, and cyber assets [7]. Specifically this can include water, energy, information and telecoms, chemical, industry, transportation, banking and finance, public health, agriculture and food, postal and shipping, and the defence industry [2].

2.1 Critical Infrastructure Security Challenges

Considerable effort has been expended on the protection of critical infrastructures; it is still an ongoing and persistent challenge. Various factors contribute to this, for example, there is a lack of understanding about the interdependency

scheme within critical infrastructures groupings. Moreover, there is no single approach about how the elements of a critical infrastructure's functionally affect a connected partner. Rinaldi *et al*., [9][3] for example, identify four groups to categorise infrastructure interconnectivities.

- Physical interdependency: Two infrastructures are physical interdependent to each other if their output materials are linked.
- Geographic Interdependency: The infrastructures are geographically interdependent if an environmental change can affect both infrastructures.
- Logical Interdependency: Two infrastructures logically interdependent of each other if their connection is through a specific mechanism such as policies, regulation, etc.
- Cyber Interdependency: The infrastructures are cyber interdependent if the infrastructures depend on information transmission. SCADA is one example of a communication system that could cause cyber interdependency between infrastructures.

With many systems, this raises several problems, particularly with the analysing or modelling of infrastructure networks which are relied on by multiple CIs. Some of these factors, which could affect the interdependencies, are indicated by Rinaldi *et al*., [9]. They can include elements such as time scales, geographic scales, cascading and higher order effects, social/psychological elements, operational procedures business policies, restoration and recovery procedures, government regulatory, legal, policy regimes and finally stakeholder concerns. These factors are critical and can have a detrimental impact on the system.

2.2 Interconnectivity Modelling

Modelling individual infrastructures is well researched area, however, modelling of multiple interdependent infrastructures is still at an immature phase [9]. Interdependency models can be grouped into six different broad categories ranging from highly aggregated tools to very detailed, high-resolution and high-fidelity models [9].

The first category is the aggregate supply and demand tools category, which evaluates the total demand for infrastructure services in a region. The second category is the dynamic simulation category. This can be used to examine a CI's operations, the effects of disruptions and the associated downstream consequences. In addition, dynamic simulation can be used to examine the effects of law, policies and regulations upon the operation of a CI. The third category is that of agent-based models, which are used in a wide spectrum of interdependency and infrastructure analyses. The fourth category is the physical-based model category where physical aspects of infrastructures can be analysed with some standard engineering techniques.

As an example of modelling, discussed by Han *et al*., is known as Interpretive Structural Modelling (ISM) [11]. According to Han *et al*., the ISM methodology can analyse the interactions of several critical infrastructures in relation to their mutual influences within a complex system [11]. Hence, it is possible to identify the driving infrastructures which can aggravate other infrastructures and their dependents. In their research, Han *et al*., apply ISM techniques on a system of eight infrastructures to develop a framework that shows interrelationships of CIs. They also classify the different infrastructures criticality according to their driving dependence and power [11]. Those relationships which can be used to lead the whole system to be a more efficient infrastructure system were found as a result.

By using both modelling and CI interdependency simulation methods, to find the relationship between different CI systems, this research aims to be able to predict the next system that might fail and prevent cascading failure occurring. Much how the human immune system is able to work a complex system to fight off illness, it is our ambition to develop a system which can repel cyber-attacks from a network of critical infrastructures. Consequently, the following subsection focuses on mapping the human immune system into a computational environment.

2.3 The Human Immune System Model

Various important systems within the human body function intangibly but are vital to our life. One of these systems is the immune system. This is considered as one of the most complicated smart systems due to the manner in which is able to keep the human body healthy. One of the most remarkable behaviours of the immune system is the way it can distinguish between self-cells (which are the body's own cells) and the non-self-cells (which the immune system attempts to destroy). Moreover, the functionality or the method the immune system uses to succeed, had encouraged researchers to try to emulate the immune system in other areas, such as computer technology. This field of research is referred to as Artificial Immune Systems (AIS). The transfer for the AIS has results important achievement, which lead to entering new prospective to the computer technology defence [13].

The properties of the immune system make it function differently from other systems, in order to perform its duties in the most effective way. Castro *et al*., list a number of properties of the immune system [14]. Some of these properties include the following:

- Pattern recognition.
- Anomaly detection
- Uniqueness.
- 'Distributivity'.
- Self-identity.
- Immune learning and memories.
- Autonomy.
- No secure layer.
- Integration with other systems.

Sompayrac *et al*., describes how the immune system works in a very comprehensive way [15]. The immune system is divided into two systems: the first system is the Innate Immune System, which is a natural barrier. The second

system is the Adaptive Immune System, which is lymphocyte. Both systems have a remarkable feature in being able to memorise different attacks. However, the mechanisms, which the innate and the adaptive immune systems use in order to memorise attacks, differ. The Innate Immune System memorise mechanism depends on a 'hard-wired' memory that has developed a pattern-recognition process to spot the signatures of regular attackers. Moreover, the innate memory mechanism knowledge built up over a long period of time and this system has the ability to develop itself as human but not updatable.

On the other hand, the Adaptive Immune System memorise mechanism depends on remembering the attacks the body has previously faced during its lifetime. The immune system mechanism idea in the human body could help in protecting different computer systems, and in particular computer networks that are relied upon by critical infrastructure systems. However, establishing methods for how the human defence concept can be applied effectively in the context of computer networks is a challenge. In order to do this, a number of examples will be highlighted to show how the functionality can be translated to apply to different infrastructures.

Elsadig *et al.*,[16] have used the concept of self-healing from the human body and translated it to software based on danger theory. Their method uses three different agents. The three agents are sense, adaptive and self-healing agents (SH), which cooperate in order to achieve a full healing system.

Province *et al.*, use multi-agents in order to imitate the human immune system idea based on the B cell [17]. The main concept of their work is to build an immune system based on the multi-agent functionality, which communicates two agents who have the same goal using an immune network. Taking Yeom *et al.*, as the last example, they used the immune system idea in order to create a distributed multi-agent method [18]. They present the B and the T cell as two different agents. They used a number of algorithms in order to simulate the T and B cell mechanisms. Highlighting, through the literature survey, critical infrastructure systems and the human body systems share some similarities, such as the interdependency between their systems. This can result in a new way of predicting a failure or a problem in an interdependent critical infrastructure system. However, all of these techniques contributed towards the design of our framework for a Critical Infrastructure Automated Immuno-Response System within a big data environment.

3. Data Collection

In order to reach the aim of this research a highly comprehensive simulation program is developed using Siemens Tecnomatix. The simulation is used to evaluate the proposed system, form the process layout and constructed the product lifecycle management. This stage involved the development of seven critical infrastructures that could affect a compound of housing units. Implementing the system involved two main points: Setting up the interconnectivity at a high level, and constructing the mechanisms of each infrastructure down to a low level. These points present a realistic data from the building construction components. Using this approach, granular dataset are constructed for the big data analysis process.

3.1 Simulation

The eight infrastructures are: Hydroelectricity, Electricity Grid, Water Distribution, Sewage System, Nuclear Power, Coal Power, Factory and House infrastructure, which are linked either by pipes or cables. The selection of these critical infrastructures was made, as they are the well-known infrastructures present in most developed countries.

The data construction process depends on the connectivity between the different system and the system's faults, each based on realistic infrastructure behaviour. The expectation is that, through analysing the data from different attack scenarios on the system, cyber-attacks can be communicated between different infrastructures and suitable countermeasures can be established. Figure 1 presents an overview of the global critical infrastructure system of systems, and the different supply chains, such as water pipes, electricity cables and sewage system.

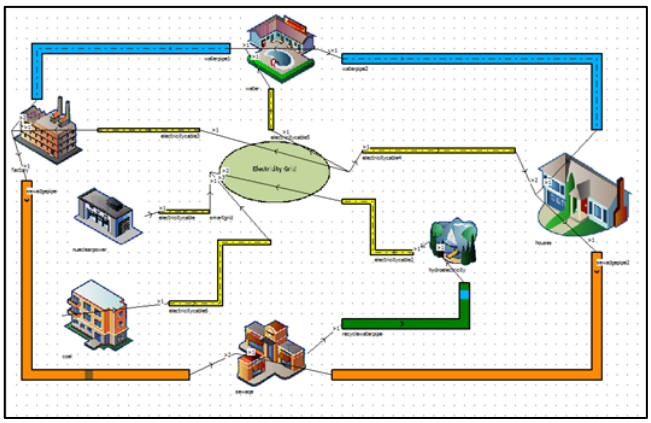

Figure 1. System Overview

Figure 2 illustrate the components within the water distrusted system, as a sample of one of the eight main CI that are presented in Figure 1.

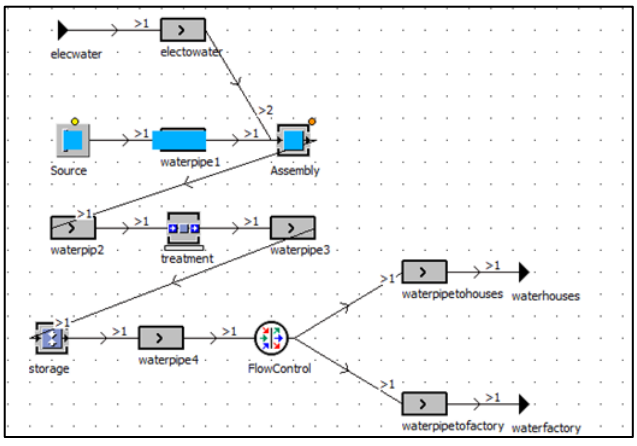

Figure 2. Water System Overview

3.2 *Data Sample*

In order to understand the behaviour of the system two data sets are constructed for analysis. A normal system set, constructed from a two hour simulation sample. Then numbers of recognized faults were introduced to the system as abnormal behaviours in order to construct a dataset of the system under attack. For this paper, a fault in the water pipe 1 and the water pipe connected to the houses compound inside the water distributed critical infrastructure are selected as an example. Table (1) and (2) display data samples from normal behaviour mode and the abnormal mode in the Water Distribution Infrastructure, consecutively.

Table 1 Normal Simulation Data Sample

Time	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
Normal Data Set										
01:57.0	0	3	1	0	0	0	0	1	0	0
01:57.2	0	3	1	0	0	0	0	0	1	0
01:57.5	0	3	1	0	0	0	0	0	1	0
01:57.8	0	3	1	0	0	0	0	0	1	0
01:58.0	0	3	1	0	0	0	0	0	1	0
01:58.3	0	3	1	0	0	0	0	0	1	0
01:58.5	0	3	1	0	0	0	0	0	1	0
01:58.7	0	3	1	0	0	0	0	0	1	0
01:59.0	0	3	1	0	0	0	0	0	1	0

Table 2 Abnormal Simulation Data Sample

Time	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
Abnormal Data Set										
01:57.0	0	3	1	2	1	0	0	0	0	0
01:57.2	0	2	1	2	1	1	0	0	0	0
01:57.5	0	3	1	2	1	1	0	0	0	0
01:57.8	0	3	1	2	1	1	0	0	0	0
01:58.0	0	3	1	2	1	1	0	0	0	0
01:58.3	0	3	1	1	1	2	0	0	0	0
01:58.5	0	3	1	1	1	2	0	0	0	0
01:58.7	0	3	1	1	1	2	0	0	0	0
01:59.0	0	3	1	1	1	2	0	0	0	0

The Water Distribution Infrastructure consists of 10 components. Data collection was conducted with a sampling rate of 4 Hertz (which is every 0.25 of a second). The system consists of 147 components in total. The numbers in the tables represent the units which flow in the water pipe. It is clear that the between the time 1:57 to 1:59 the level of the water was increased. Table (3) explains the Water Distribution components in detail.

Table 3 Component Description for Water Distribution Infrastructure

Abbreviation	**Component Description**
F1	Electricity cable from the Electricity Grid to the WD in the WD
F2	Water pipe 1 from the source in the WD
F3	WD Assembly
F4	Water pipe 2 in the WD
F5	WD treatment
F6	Water pipe 3 after the treatment in the WD
F7	WD Storage
F8	Water pipe 4 in the WD
F9	Water pipe from WD to Houses in the WD
F10	Water pipe from WD to Factory in the WD

4. APPROACH

The framework put forward in this section assists and guides critical infrastructures on how to behave when abnormal behaviour is detected. This information is then shared to other infrastructures. This concept draws from the example of an immune system characteristic, to share and assist other infrastructures from abnormal behaviours and prevent cyber-attacks from having a cascading impact.

4.1 *System Framework*

The framework presented below (Figure 3), displays a high-level of functions work together in order to indicate abnormal behaviours are occurring and the mitigation process.

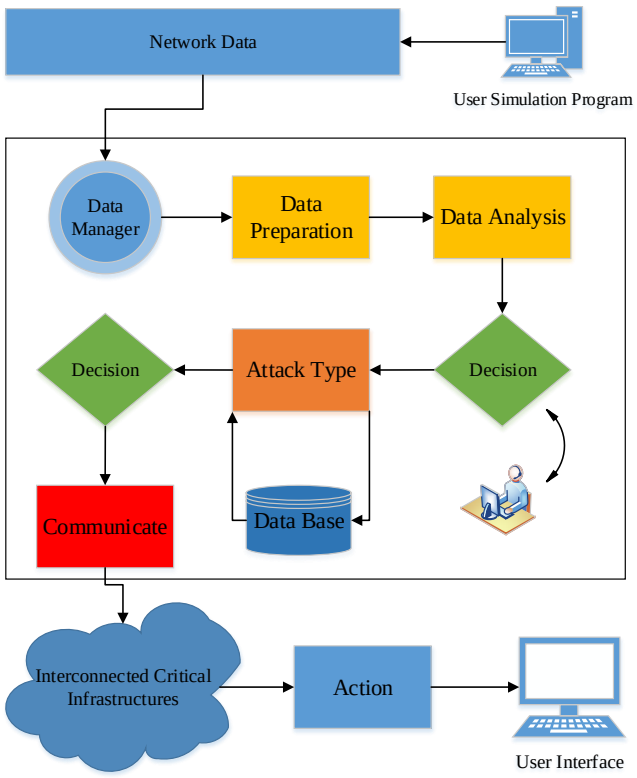

Figure 3 The System Framework.

The different components that form the system, and the flow between the components, are displayed above. The system starts with the collection of data from the network (provided by the simulation) and introduces it to Data Manager. At this point data is sent for analysis, involving a data classification process. Here machine learning algorithms, presented in the next subsection, detect behavioural changes which constitute abnormal behaviour. Once the abnormal signals are detected, a comparison with the previously stored behaviours is conducted in order to assess if the pattern is known. Depending on the network connectivity between the CIs, the system would then start share the new abnormal behavior with interconnected partners. This would help other CI plan for an emerging attack of cascading impact. At all times an administrator overviews the system functions.

4.3 Data Analysis

This sub-section details the process involved in detecting abnormal behaviour for sharing with other infrastructures. For the purpose of this paper, 48 records of data are used for the classification process consisting of 24 normal and 24 abnormal behaviour records. The records of data are comprised of 18 features.

Since the standard deviation is a valid measure that indicate the distance value from the mean. Both the mean and the standard division have been selected in order to give an accurate comparison in generating the classifiers. Table 3 presents the result of the classicisation process, which involved using 6 well-known machine learning algorithms. The best values are obtained by ParzenC and KNNC. In addition the Sensitivity and Specificity detection rates are also higher than other classifiers. This refers to the detection of normal and abnormal behaviours respectively.

Table 3. Classification Results

Classifiers	AUC%	Sensitivity	Specificity
LDC	79.17	0.706	1.000
UDC	50.00	0.500	0.500
QDC	50.00	0.500	0.500
SVC	75.00	0.667	1.000
Parzenc	87.50	0.800	1.000
KNNC	87.50	0.800	1.000

Using the above techniques to detect behaviour changes, patterns of behaviour would be developed and communicated to other infrastructures for mitigation and remediation planning.

5. Discussion

In this section, a discussion on the results is presented. Table 4 present 2x2 confusion matrix for the ParzenC classifier with 87.50% accuracy identifier and 3 incorrectly identified, as a demonstration of how the results for Table 3 are calculated.

Table 4. ParzenC Confusion Matrix

True Labels	Estimated Labels		
	1	2	Totals
1	12	0	12
2	3	9	12
Totals	15	9	24

Figure 4 displays a graph of the ParzenC classification for two of the eighteen features. The ellipses displayed, refer to likelihood contours, where the points inside the ellipse are most likely to belong to that grouping. The blue ellipses consist of data that comes from the normal behaviour dataset and the red referring to threat behaviour data. Threat behaviour can be identified as a result of one grouping clearly standing out from the other.

The process functions by creating a scatter plot of the values from both of the selected features then drawing the ellipses based on the division of the data. The ellipses, displayed, refer to likelihood contours, where the points inside the ellipse are most likely to belong to that grouping.

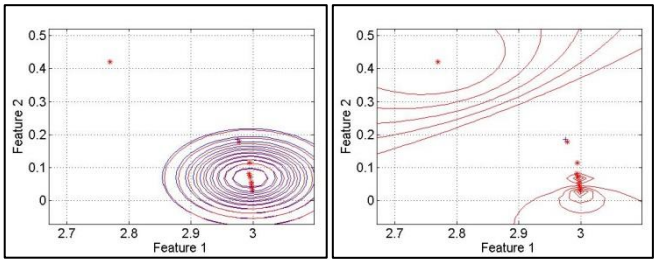

Figure 4. ParzenC Visualisation & Figure 5. KNNC Visualisation

The blue ellipses consist of data that comes from the normal behaviour dataset and the red ones referring to threat behaviour data. Threat behaviour can be identified as a result of one grouping clearly standing out from the other. Similarly, Figure 5 displays a visualisation of the classification results for the KNNC classification process. Feature 1, on the x-axis, refers to one of the dominant features and Feature 2, on the y-axis, and refers to one of the lesser dominant features from the dataset. Two features were used in each visual representation to demonstrate how the classifiers function. The graph displays that some changes in behaviour can be identified but often some are subtle and difficult to identify.

6. Conclusion

The growth which the Critical Infrastructure interconnectivity is one the main challenges when countering the growing cyber-threat. The research presented in this paper demonstrates a technique for the detection of abnormal behaviour within a CI and offers and approach for sharing the information with other infrastructures, using the human immune system as a reference model. A frame work was proposed, as was a simulation approach for constructing big

data sets for analysis. Using ParzenC and KNNC, two data classification techniques, we achieved high accuracy in the detection of abnormal behaviours. Our future work will involve automating the system to be able to offer a set of recommended changes to an administrator in response to a cyber-attack taking place. The recommendations will be shared within a network of interconnected critical infrastructures.

REFERENCES

[1] W. Hurst, M. Merabti, and P. Fergus, "A Survey of Critical Infrastructure Security," in Critical Infrastructure Protection VIII, A Survey of Critical Infrastructure Security ,8th IFIP WG 11.10 International Conference, 2014.

[2] T. Denis, "Managing Communications in Critical Infrastructures Protection," in 2010 Second International Conference on Computer Engineering and Applications, 2010, pp. 11–15.

[3] B. S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, Understanding, and Analyzing: Critical Infrastructure Interdependecies," Control Syst. IEEE, vol. 21, no. 6, pp. 11–25, 2001.

[4] A. Laugé, J. Hernantes, and J. Mari Sarriegi, "The Role of Critical Infrastructures' Interdependencies on the Impacts Caused by Natural Disasters," Crit. Inf. Infrastructures Secur., vol. 8328, pp. PP50–61, 2013.

[5] Novakovic. Jon, "The Impact Of Interdependence On Providing Protection For Critical Infrastructures," 2015. [Online]. Available: http://www.securitysolutionsmagazine.biz/2015/05/06/the-impact-of-interdependence-on-providing-protection-for-critical-infrastructures/. [Accessed: 11-Nov-2015].

[6] J. Moteff, P. Parfomak, and I. Ave, "CRS Report for Congress Received through the CRS Web Critical Infrastructure and Key Assets : Definition and Identification," 2004.

[7] D. Command and F. Leavenworth, "Critical Infrastructure Threats and Terrorism," in DCSINT handbook No. 1.02, 1st ed., no. 1, Distribution Unlimited, 2006.

[8] J. B. Camargo Jr. and L. F. Vismari, "Challenges in Safety Assessment of Complex Critical Infrastructures," in 2011 Fifth Latin-American Symposium on Dependable Computing Workshops, 2011, pp. 37–38.

[9] S. M. Rinaldi, "Modeling and Simulating Critical Infrastructures and Their Interdependencies," in System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on, 2004, vol. 00, no. C, pp. 1–8.

[10] A. Di Giorgio and F. Liberati, "Interdependency modeling and analysis of critical infrastructures based on Dynamic Bayesian Networks," in 2011 19th Mediterranean Conference on Control & Automation (MED), 2011, pp. 791–797.

[11] C. Han, L. Liu, and M. Rong, "Addressing Criticality Levels in Critical Infrastructure System," in Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on, 2009, no. October, pp. 3965 – 3970.

[12] J. P. Marchal, Gu., Marchel, G. and Heiken, Multidetector-Row Computed Tomography: Scanning and Contrast Protocols. Italia: Springer-Verlag, 2005.

[13] A. Kordon, Applying Computational Intelligence: How to Create Value. USA: Springer, 2010.

[14] J. Castro, L. and Timmis, Artificial Immune Systems: A New Computational Intelligence Approach, Illustrate. uk: Springer, 2002.

[15] L. Sompayrac, How the Immune System Works, 4th ed. John Witey and Sons, 2012.

[16] M. Elsadig and A. Abduallah, "Biological Intrusion Prevention and Self-Healing Model for Network Security," in 2010 Second International Conference on Future Networks, 2010, pp. 337–342.

[17] H. Province, "An Artificial Immune System Based Multi- Agent Model and its Application to Robot Cooperation Problem," in Intelligent Control and Automation, 2008. WCICA 2008. 7th World Congress on, 2008, pp. 3033–3039.

[18] K. Yeom and J. Park, "An Artificial Immune System Model for Multi Agents based Resource Discovery in Distributed Environments," in First International Conference on Innovative Computing, Information and Control - Volume I (ICICIC'06), 2006, vol. 1, pp. 234–239.