Secure Wireless Mesh Network based on Human Immune System and Self-Organizing Map

Mahira M. Mowjoon and Johnson I Agbinya
Centre for Real time Information Networks,
Faculty of Engineering and Information Technology,
University of Technology, Sydney
Australia

1. Introduction

Wireless Mesh Networks (WMNs) are evolving as a future generation wireless mobile networks and bring the dream of connected world into reality. According to 802.11s standard Nodes in a mesh network can be divided into four classes, Client or Station (STA), Mesh Point (MP), Mesh Access Point (MAP) and Mesh Portal Point (MPP). Client is a node that requests services but does not contribute in path discovery, Mesh Point (MP) is a node that participates in the mesh operations, Mesh Access Point (MAP) is a MP attached to an access point (AP) to provide services for clients (STA), and Mesh Portal Point (MPP) is a MP with additional functionality to act as a gateway between the mesh and an external network (Hidenori et al., 2006). Fig 1 shows WMN architecture according to 802.11s standard.

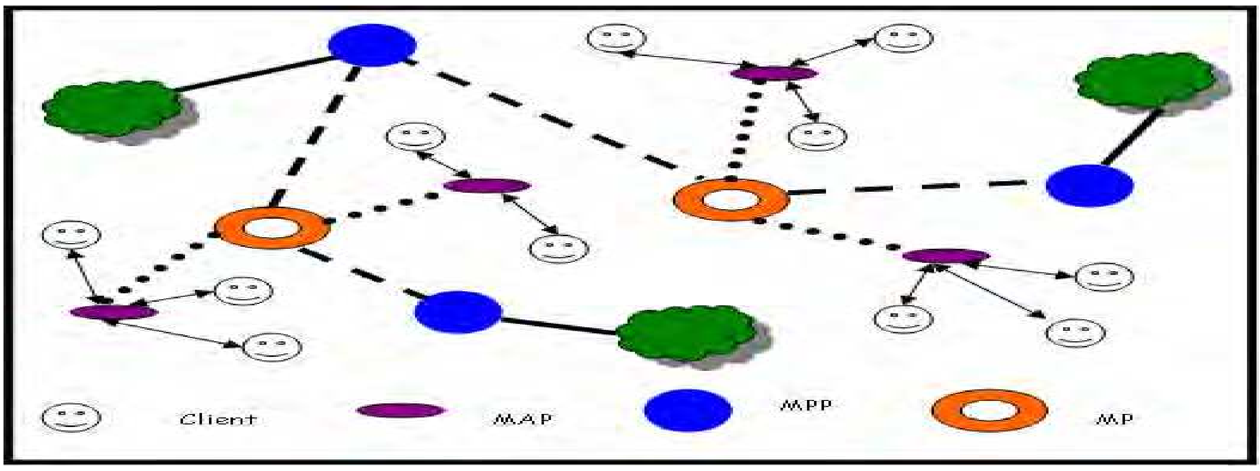


Fig. 1. WMN Architecture

Further, WMN is dynamically self-organized and self configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among them. Major principles of self-organization can be classified in to four categories specifically local state evaluation, interaction between individuals, negative feedback loop and positive feedback loop. This concept is common to both biological systems and communication systems and the figures 2 and 3 compare the concept of feedback loops for biological system and the feedback loop for WMN system respectively. Positive feedback loop amplifies an effect whereas negative feedback loop controls the system behaviour. Any dependencies and global control are prevented by acting upon local information. Moreover, direct and indirect information exchange is used to update local state and interact with the system environment. The self organizing nature of WMN brings many rewards such as low up-front cost, easy network maintenance, robustness, and reliable service coverage and delivers wireless services for extended applications namely real time intelligent transportation systems, spontaneous networks, rural networks, community and neighbourhood networks, broadband home networks, building automation, security surveillance systems, metropolitan area networks and health and medical systems.

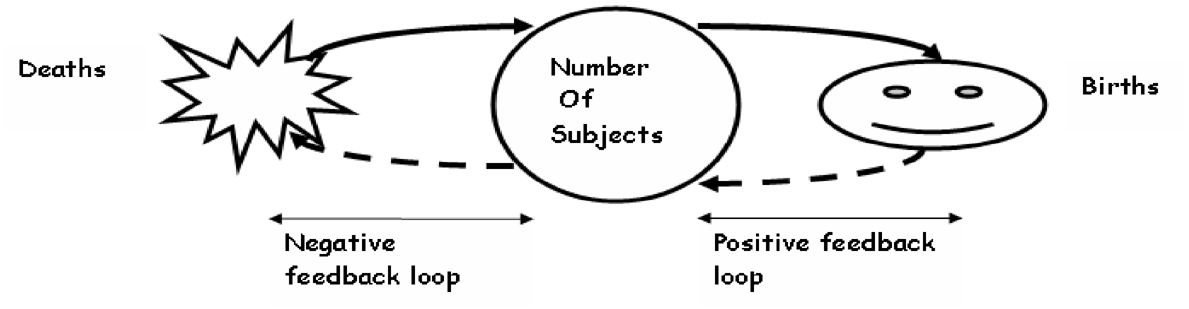


Fig. 2. Feedback loops in biological system

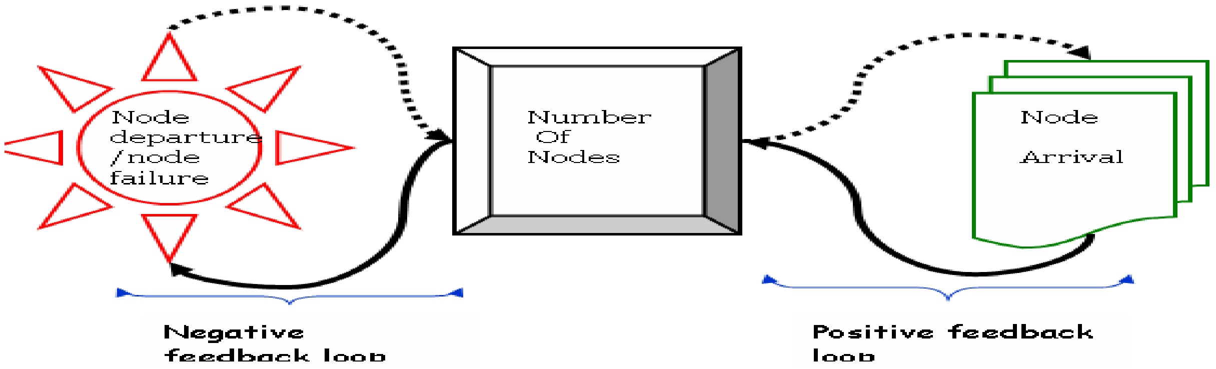


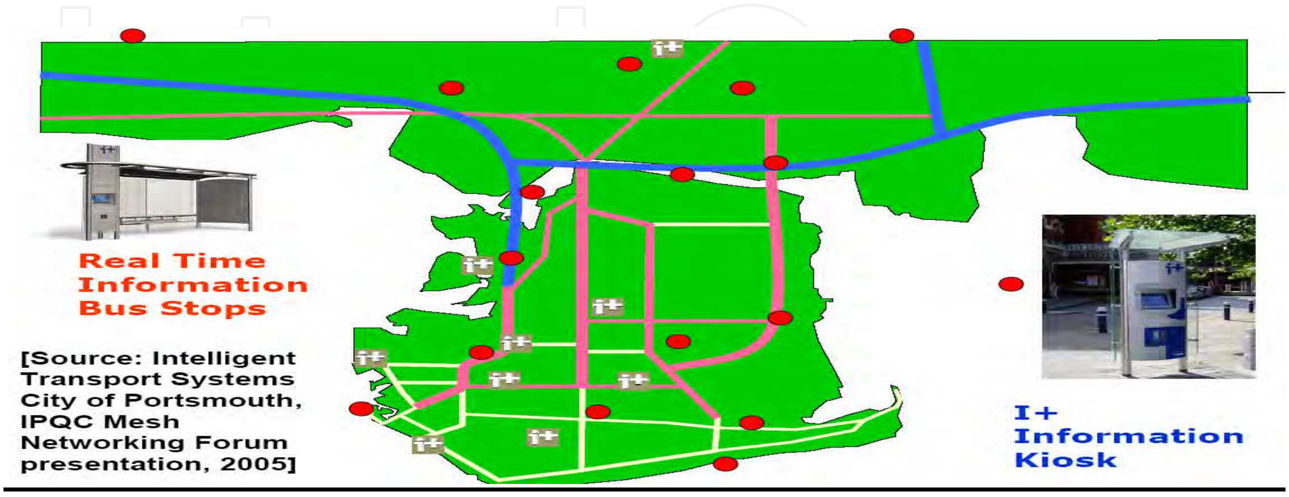
Fig. 3. Feedback loops in WMN system

Although there are some similarities between Mobile Ad-Hoc Networks and Wireless Mesh Networks there are also number of important differences. In contrast with Mobile Ad-Hoc Networks, static nodes, essentially Mesh Access Points in Mesh networks communicate with each other over wireless links.

1.1 Application scenarios of Wireless Mesh Networks

Real time intelligent transportation system

Mesh networking technology can be extensively used to provide useful passenger information services in buses, ferries, and trains and can support remote monitoring of in-vehicle security and driver communications. Fig. 4. shows real time intelligent transportation system.

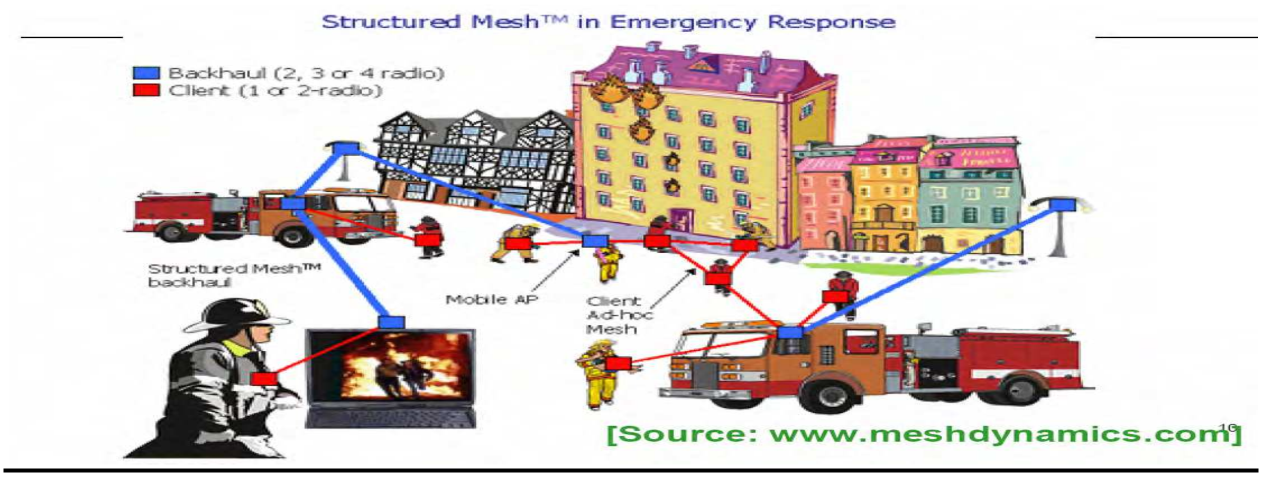


[Source: Intelligent Transport Systems City of Portsmouth, IPQC Mesh Networking Forum presentation, 2005]

Fig. 4. Real time intelligent transportation system

Spontaneous (emergency/disaster) network

WMNs facilitate group of people to establish group networks during an emergency situation, where the people involved have no knowledge about the environment. This service is offered by simply placing wireless mesh access points in desired locations. Fig. 5. illustrates emergency network.


Structured Mesh™ in Emergency Response
🟦 Backhaul (2, 3 or 4 radio)
🟥 Client (1 or 2-radio)
Structured Mesh™ backhaul
Mobile AP
Client Ad-hoc Mesh
10

[Source: www.meshdynamics.com]

Fig. 5. Emergency network

Rural network

Since the communication between nodes does not depend on the wired backbone, WMN is a cost effective option in under developed regions and covers vast area than the community networks.

Community and neighborhood network
WMNs resolve problem of resource utilization in community networks and covers large areas between houses while reducing the network access cost and provide multiple paths to access Internet and offer flexible connectivity with neighbours.
Broadband home network
In home networking, WMN offers location independent services and provides flexible and robust connectivity of the network.
Building automation
In large buildings controlling and monitoring of various electrical devices are very common. Currently, these tasks are executed through expensive wired networks, by deploying WMN controlling and monitoring can be performed at lower cost.
Security surveillance system
Security is becoming vital in critical environments and security surveillance systems become a necessity for enterprise buildings, shopping malls, grocery stores, etc. In order to setup such systems at locations as required, WMNs are a much more feasible solution than wired networks to connect all devices.
Health and medical system
Critical and bulk data processing and transmission are the key issues in medical centres and hospitals. While traditional wired networks provide only certain services wireless mesh technology offers efficient transmission of high resolution medical images and large volume of monitoring information.

2. Wireless Mesh Network security

Despite of hot move in WMN research, substantial investigation is needed to address the most challenging factors such as security, inter operability, Quality of service, connectivity, scalability and compatibility. Even though security is the major factor that affects the deployment of WMN it is often a secondary reflection in development, thus considerable research is still needed to address the security aspect. Recently, there has been a rapid boost in researching security of Wireless Mesh Networks, but still they lack efficient and scalable security solutions due to their dynamic and distributed nature of the system. The security factor can be explored with various key challenges includes secure routing, authentication, access control and authorization, key management and intrusion detection. Further, none of the existing key management based techniques are suitable for wireless mesh networks as they are inefficient on an arbitrary or unknown network topology, or not tolerant to a changing network topology or link failures.

In my research I focus on secure routing in WMN as the other aspects have been talked about in the literature and there has been urgent necessity of further exploration of secure routing in WMN.

3. Emerging concept, from nature to communication engineering

A great increase in studying biologically inspired systems, specifically the rising curiosity in Human Immune System (HIS) stimulates the applicability of HIS concepts in WMN security. Some of the attractive features analogous to the features of WMN include adaptability, distributability, diversity, autonomy and dynamic coverage. Moreover, secure routing functions can be mocked-up by analysing the reaction process of Human Immune System (HIS) against a foreign material.

4. Immune system

4.1 Human Immune System

Human Immune System is an extremely complex collection of cells and organs that work together to defend the body against foreign attacks. It has the capability of recognizing different enemies. Once the immune cells receive the distress they go through changes and start producing chemicals which regulates the growth and the behavior of the cells (NIH 2003). A healthy immune system is capable of distinguishing between self cells and non-self cells. The fig. 6. shows the structure of the HIS.

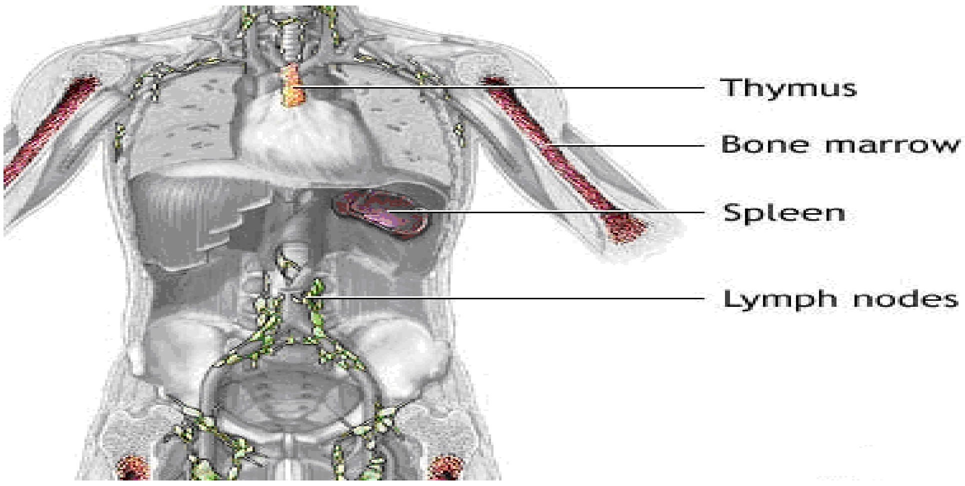


Fig. 6. Structure of HIS (Source Mediline)

4.2 How does Immune System respond to Antigen?

Human Immune System plays major role in protecting human body against pathogens and microbes. The large collection of cells in HIS operates autonomously and creates series of events leading to the destruction of pathogens. Immune cells can be broadly categorized in to two groups namely detectors and effectors (Mahira et al., 2007), detectors identify pathogens, and effectors neutralize them. Moreover, two kinds of immune responses are induced by the Immune system. They are innate response and adaptive response. During innate immune response process pathogens in the body are detected by phagocyte and antibodies are produced by the adaptive immune response to recognize specific pathogens. The lymphocytes that match antigen propagate by cloning and subsequently differentiate into B-cells, which generate antibodies, and T-cells, which destroy infected cells and activate other cells in the immune system (Mahira et al., 2007).

4.3 Artificial Immune System Models

There are four Artificial Immune System models discussed in the literature. They are negative selection model, clonal selection model, immune network model and danger model.

4.3.1 Negative Selection Model

This was introduced by Forrest in 1994 as a conceptual model of biological negative selection. Change detection is the basis of this algorithm and the generated detectors are intended to detect self strings which have changed from an ascertain norm.

In this process, firstly, set of self strings and a set of random strings are created. Secondly matching function is defined for random strings which do not strongly match as self string. This process iterates until detector strings are obtained.

4.3.2 Clonal Selection model

The basis for the clonal selection algorithm is the natural B-cell mechanism (Mahira et al., 2007). When the receptors of immature B-cells in the blood match to an antigen they propagate rapidly and modify to facilitate better matching. The B-cells with better matching proliferate continuously until the best matching B-cells are produced (Mahira et al., 2007) . Leandro N. de Castro and Fernando J. Von Zuben proposed natural clonal selection based algorithm, called CLONALG .This is a representation of computational implementation of clonal selection and affinity maturation principles accountable for behaviour of B-cells during adaptive immune responses .Fig.7. shows the clonal selection process.

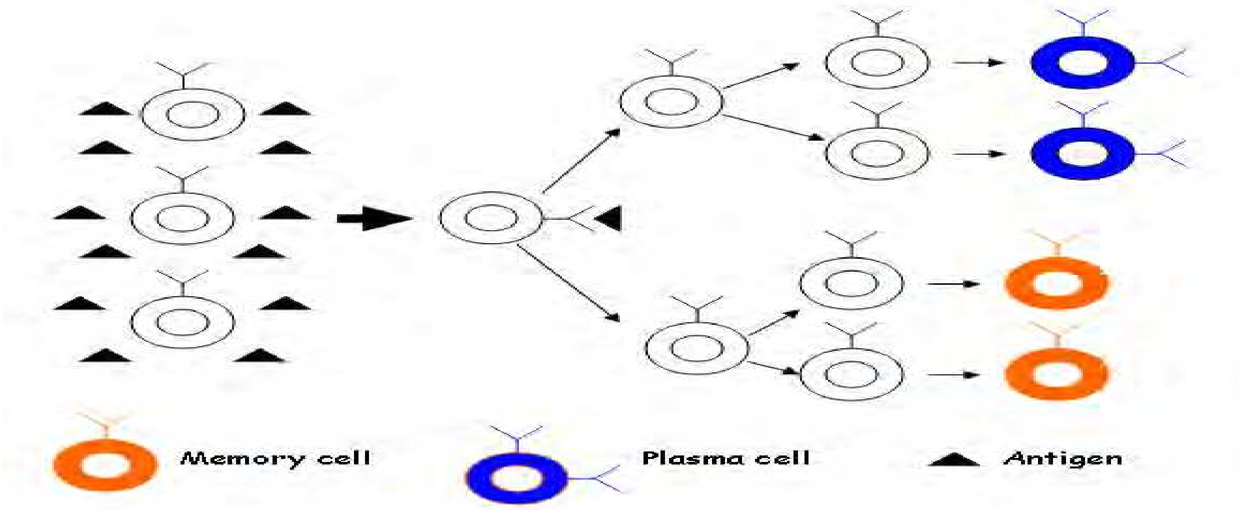


Fig. 7. Clonal Selection Process [Source (Mahira et al., 2007)]

4.3.3 Immune Network Model

The immune network theory suggests that the immune system has a dynamic behaviour even in the absence of external stimuli. Further the immune cells and molecules are capable of recognizing each other, which provides the system with an eigen behaviour that is independent of alien stimulation. The recognition of antigen by an antibody (cell receptor) leads to network activation, whereas the recognition of an idiotope by another antibody leads to network suppression. According to the immune network theory, the receptor molecules contained in the surface of the immune cells present idiotopes, and these idiotopes are displayed in and/or around the same portions of the receptors that recognize non-self antigens.

4.3.4 The Danger Theory

Classical immunology depends on the concept of "self" and "non-self" cells distinction. An immune response is triggered when the body encounters something "non-self", Matzinger pointed out that there is a bias in differentiating self and non-self cells because the HIS does not respond to useful bacteria in the food or air (Matzinger, 2002) . On the other hand, the central theme of Danger theory is that the immune system responds to danger but not to "non-self". The motive for this is that there is no need to attack everything that is foreign. This concept is very practical in WMN environment. The danger can be measured in terms of distress signal sent out by unexpectedly dying nodes/devices in the network. Fig.8 shows how an immune response can be pictured according to the danger theory. A cell that is in distress sends out danger signals and form danger zone around itself, then antigens in the neighborhood are captured by Antigen-presenting cells and they travel to the local lymph node and present the antigens to the lymphocytes. B-cells, which are within the danger zone, get stimulated to produce antibodies that match the antigens and to traverse the clonal expansion process. Those which do not match or are too far away do not get stimulated.

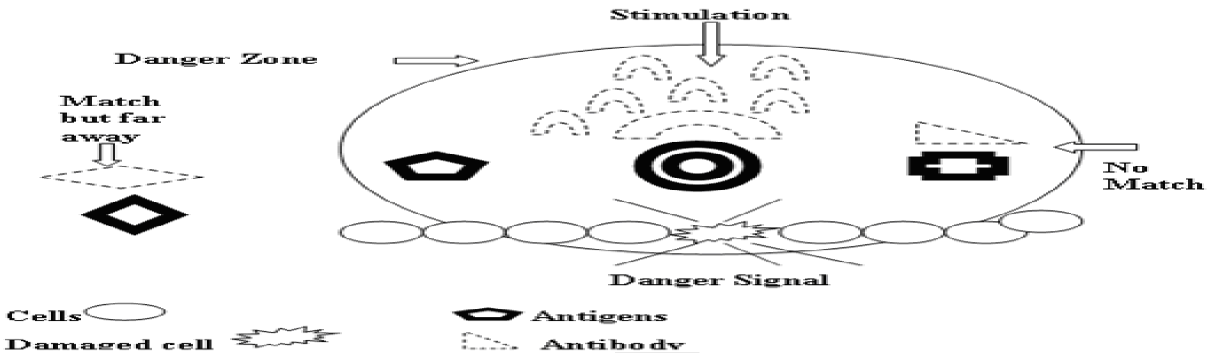


Fig. 8.Model of the Danger Theory [source (Mahira et al., 2008)]

Further, self and non-self classification against danger and non-danger distinction is illustrated in fig.9.

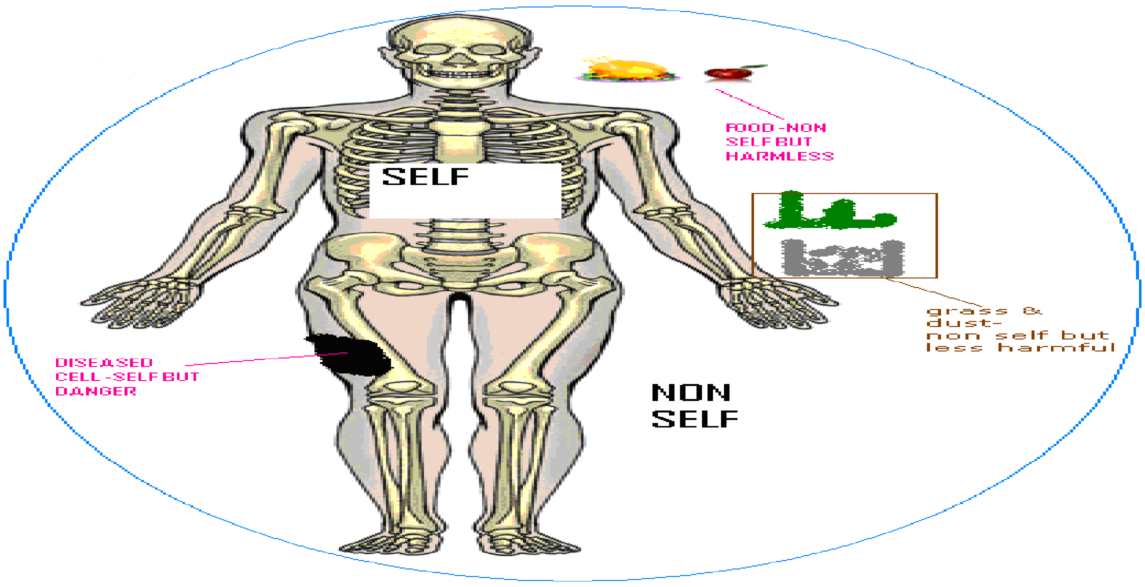

SELF
FOOD -NON SELF BUT HARMLESS
grass & dust- non self but less harmful
DISEASED CELL -SELF BUT DANGER
NON SELF

Fig. 9. Self and non-self classification against danger and non-danger distinction

5. Mapping of HIS elements on to WMN elements

As the first step in implementing HIS inspired secure routing, mapping of Human Immune System Elements onto Wireless Mesh Network has been carried out. The table 1 shows the mapping of HIS elements on to WMN devices.

HIS	WMN
Body	The entire WMN system
Self-Cells	Well behaved network resource nodes
Non-Self Cells	Corrupted or well-behaving but unauthorized nodes inside the network or any external input either friendly or malicious. Inactive or non participating nodes
Antigen	Possible cause of interruption or anomalies or danger to the network
Antibody	Recovery or protection actions for the node in danger possibly caused by antigen
Cytokines	Error messages or danger signals or events communicated between nodes

Table 1. Mapping of HIS elements on to WMN devices

6. Clustering methods

The main goal of clustering is to analyse and reduce the amount of data to work with by grouping related data elements together. Different clustering techniques are used in various application scenarios, for example clustering mechanisms used in web data grouping, spatial data clustering, in Biology and in marketing research. Taxonomy of clustering approaches is given in (Jain et al., 1999). The author has given an extremely detailed description of clustering mechanisms in his paper (Pavel). Partitional clustering and hierarchical clustering are the basic types of clustering mechanisms considered in (Ugur), (Samuel & Nick Theodosopoulos, 2006). Hierarchical algorithms can be performed as bottom up approach or top down approach. In this approach clusters are formed at the beginning of the process and then new clusters are produced based on the relationship of the data elements within the data set. On the other hand partitional algorithms form the clusters only once during the process. Then each element of the dataset is analysed and placed within the corresponding cluster.

7. Self-Organizing Map (SOM)

Self organizing map (SOM) is a computationally efficient neural network which is introduced by der Malsburg in 1973 and subsequently by Kohonen in 1982. SOM is also called as Self organizing feature maps (SOFM), topographic map and Kohonen feature maps. In the simplest form, SOM is a set of cells organised in different layers and each cell represents a piece of data which is usually a vector. Further, SOM admits N-dimensional input vectors and maps them to the Kohonen layer, in which neurons are usually arranged in a 1, 2 or 3 dimensional grid representing the feature space. Such a grid characterizes the topological properties of neurons rather than exact geometric locations. Fig.10 shows the basic structure of SOM and this architecture maps high dimensional data on to a two dimensional rectangular grid of output layer and the input layer is fully connected with the output layer and the output neurons have lateral connections to their neighbours.

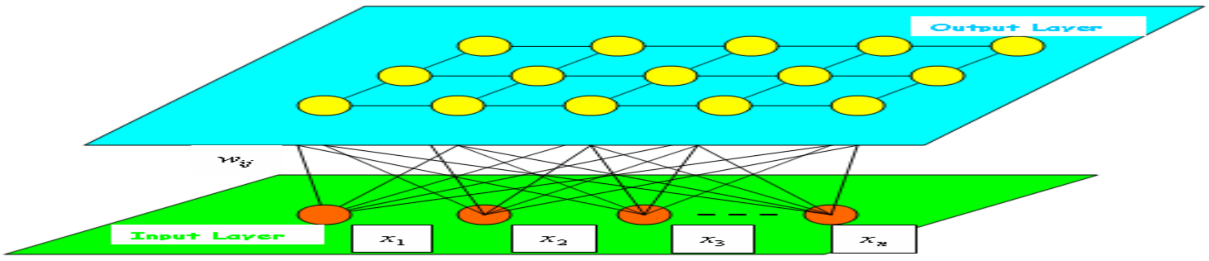


Fig. 10. The basic structure of SOM

In comparison with other commonly used clustering techniques, SOM has been broadly applied in data analysis and tremendous clustering and classification performance have been reported (Hashemi et al., 2005). Moreover, SOM provides comprehensible graphical illustration of the input data patterns, which has been applied to identify new vulnerability patterns while new threats or attacks amplify. The Growing Self-Organizing Map (GSOM) is a division of SOM with the growing map size. The motivation behind the GSOM is that the exact topology and the size of the map often have a large impact on the training process of the SOM and the map is determined by the statistical regularity not by the programmer. A detailed description of GSOM is given in (Hashemi et al., 2005).

8. Classification of Dangers using SOM

Mathematical Modelling

It is assumed that there is Q number of input patterns and the input vectors are of dimension N. Therefore the output for neuron j, from input pattern i, is denoted by $y_{i \to j}$ and depicted in Fig.11: Then the winning output neuron j, is determined by selecting the output neuron with the best weight vector that matches the input vector. This is achieved by calculating the distance between x_i and w_j. Where x_i and w_j are derived from the equations (1) and (2) and the distance $d_{i \rightarrow j}$ is manipulated using the equation (3).

$$\mathbf{x}_i = \begin{pmatrix} x_{i,1} \\ \\ x_{i,N} \end{pmatrix} \tag{1}$$

$$\mathbf{w}_j = \begin{pmatrix} w_{j,1} \\ \\ w_{j,N} \end{pmatrix} \tag{2}$$

$$d_{i \rightarrow j : x_i \rightarrow w_j} = \left[\sum \left(x_{i,k} - w_{j,k} \right) \right]^{1/2} \tag{3}$$

Moreover, x_{Total} and $y_{i \rightarrow j}$ are calculated using the formula (4) and (5) respectively.

$$\mathbf{x}_{Total} = \begin{bmatrix} \mathbf{x}_1 \\ \downarrow \\ \mathbf{x}_Q \end{bmatrix} = \begin{bmatrix} \left(x_{1,1} \quad \rightarrow \quad x_{1,N} \right)^T \\ . \\ \left(x_{Q,1} \quad \rightarrow \quad x_{Q,N} \right)^T \end{bmatrix} \tag{4}$$

$$y_{\mathrm{i} \rightarrow \mathrm{j}} = \sum_{k=1}^{\mathrm{N}} w_{\mathrm{j,k}} \; x_{\mathrm{i,k}} \tag{5}$$

where,

i = 1...Q (Q = number of input patterns)
j = 1....M (M = dimension of output neurons)
k = 1.....N (N = dimension of input vectors)

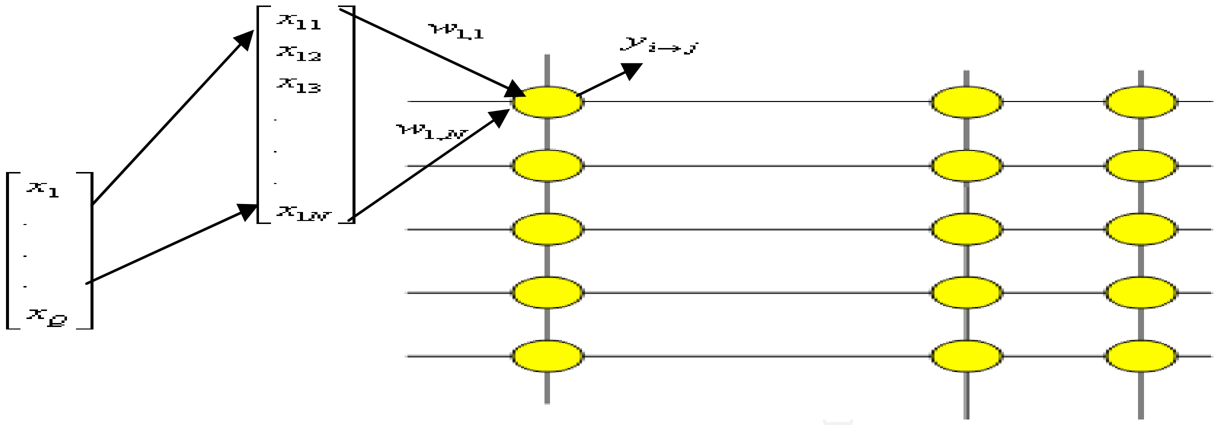


Fig. 11. The output for neuron j, from input pattern i

In addition, adjust weights of the winner neuron towards the input is given by the equation (6).

$$\mathbf{w}_j(t+1)=\begin{cases}\mathbf{w}_j(t)+\eta(t)\left[\mathbf{x}_i(t)-\mathbf{w}_j(t)\right] & j\in\Lambda_{winner}(t)\\ \mathbf{w}_j(t) & otherwise\end{cases} \tag{6}$$

Where, $\eta(t)$ is the decrease learning rate which is in a linear fashion or exponential decay; reduce the neighbourhood $\Lambda_{winner,neigh}(t)$ to update the weights of the neighbours,

$$\mathbf{w}_j(t+1)=\mathbf{w}_j(t)+\eta(t)\ \Lambda_{winner,neigh}(t)\ \left[\mathbf{x}_i(t)-\mathbf{w}_j(t)\right] \tag{7}$$

$\wedge_{winner,neigh}(t)$ is defined as follows,

$$\Lambda_{winner,neigh}(t)=e^{\left(\frac{-\left\|r_{neigh}-r_{winner}\right\|^2}{2\sigma^2}\right)} \tag{8}$$

Then the size of neighbourhood decreases over time to stabilize mapping, where σ represents width of neighbourhood function which is an exponential decay.
Based on these theoretical analyses, experiment was carried out and reported in section 9.

9. Experiment

In order to evaluate the performance of the proposed approach with DT, an experiment is conducted based on the process described in the previous sections. Self-Organizing Maps (SOMs) are applied as a danger level classifier in the experiments. To simplify the experiments, the input of SOMs in this simulation are limited to the following three categories: (1) Changes of Self-nonself information flow during a time interval, e.g., attack information and node failures; (2) Network traffic conditions, e.g., number of transmitted packets, bit error rate (BER) and packet delivery ratio (PDR). (3) Resource conditions, e.g., remaining bandwidth or memory, Link capacities.

9.1 Distributed Internet Traffic Generator (D-ITG)

The Distributed Traffic Generator (D-ITG) is used to generate artificial traffic data in order to train and test SOM network. The TCP traffic with Poisson distribution is adopted where packet size is 512 bytes, and average 1000 packets/sec. Beside, UDP traffic is also considered in the dataset. The bounds to identifying different level of traffic load are setup and the table 2 shows the details. These traffic conditions relates to the classification of danger levels.

Testbed Elements	Descriptions	Details
D-ITG	{UDP, TCP}	Poisson Distributions for TCP
	{Packet Size} byte	{64, 128, 256, 512, 1024, 1500}
	{Traffic Load}	Low ($\leq 1.5 Mbps$) Medium ($\leq 6 Mbps$) High ($\leq 8 Mbps$)

Table 2. Parameter Elements

Compared to the higher dimensionality of input data, the output of SOMs is a lower dimension space. When the network is fully trained, it is ready to get the data clustered on the map demonstrated in the Figure 14. After some tests by using the testing data, the 4 classified zones defined in the figure are found. In the simulation, a 2-dimensional space split into 4 classified zones, such as High danger, Medium danger, Low danger and Unacceptable zone, are the output of SOMs output neurons.

Figure 12 shows the process of training SOMs and testing SOMs with the testing data, which is part of the training dataset generated by the Distributed Traffic Generator - D-ITG and input dataset which is generated by Monte Carlo Simulation where random number generator produce all the dataset. Table3 shows the parameter setting of the SOMs for identifying danger levels. The following Figure 14 shows the simulation result. Input data is classified via SOM and visualized results are represented.

Number of Input Layer	3
Row of Output Layer	20
Column of Output Layer	20
Topology	Rectangular
Learning efficiency	0.9
Iteration Number	2000
Error_limit	5E-12

Table 3. Parameters of SOM for danger levels

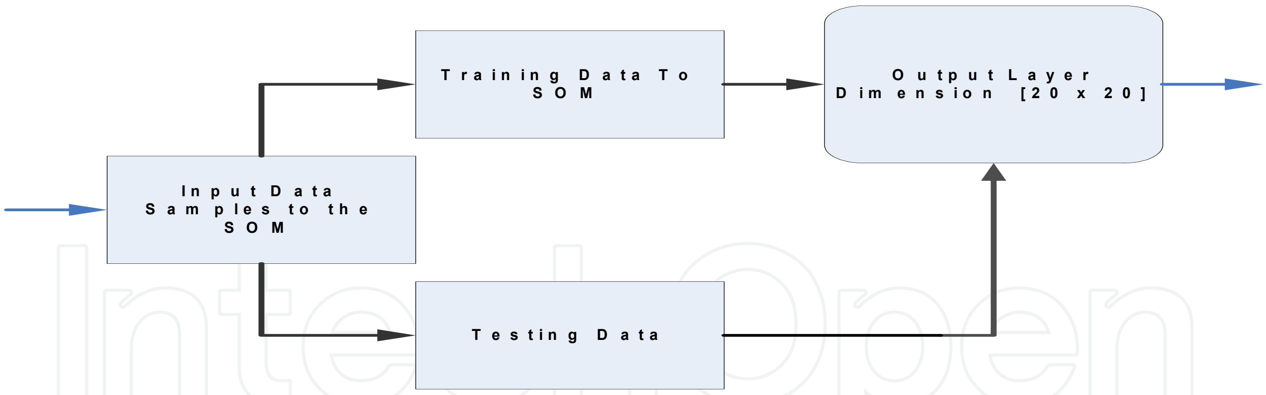

Training Data To SOM
Output Layer Dimension [20 x 20]
Input Data Samples to the SOM
Testing Data

Fig. 12. Simulation Structure

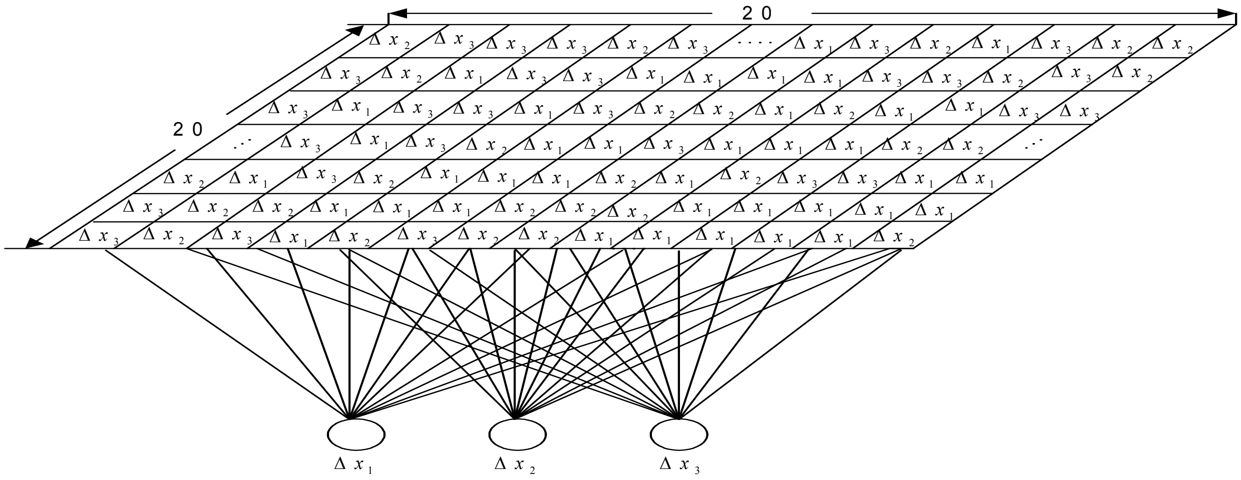


Fig. 13. Structure of SOM in the simulation

9.2 Simulation Results

According to the classified danger information from SOM, the methods and algorithms defined in this chapter will be invoked for secure routing protocol in the research. The simulation results of the algorithm are shown in Figure 14, as shown, the input data vectors involving three types of inputs are classified into 4 zones: (1) High Danger Level, (2) Medium Danger Level, (3) Low Danger Level (4) Unaccepted Danger Level. The darkest color shows zone (4). The lightest color represents zone (1) The other two zones (2) and (3) are depicted by the blue color. The lighter blue color zone represents zone (2). These zones stand for the danger levels.

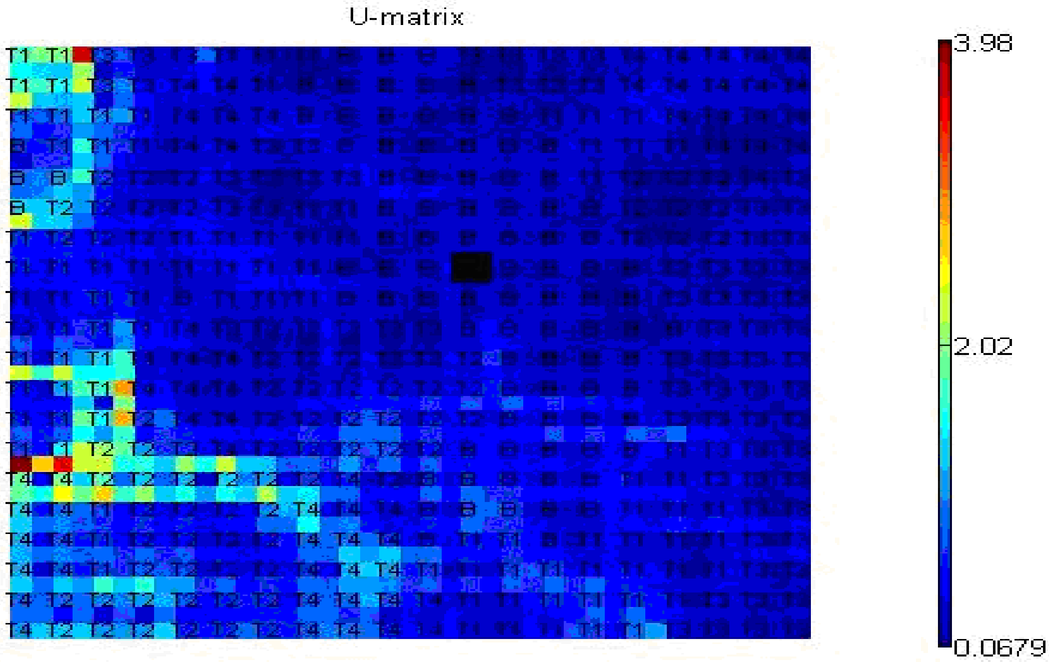


Fig. 14. Simulation Result

Acknowledgment

The authors wish to thank Zenon Chaczko and Frank Chiang for their contribution in preparing the paper, "Mahira Atham Lebbe, Johnson I Agbinya, Zenon Chaczko and Frank Chiang, Self-Organized Classification of Dangers for Secure Wireless Mesh Networks, 2007 Australasian Telecommunication Networks and Applications Conference, December 2nd – 5th 2007, Christchurch, New Zealand"

10. References

AK Jain , MN Murty and PJ Flynn (1999), Data Clustering: A Review, *in ACM Computing Surveys*, pp 264-323 Vol. 31, No. 3, September 1999.

Hashemi, R.R., M. Bahar, and S. De Agostino (2005). An extended self-organizing map (ESOM) for hierarchical clustering, *proceedings of IEEE International Conference on Systems, Man and Cybernetics*, pp 2856- 2860 Vol. 3, ISBN: 0-7803-9298-1, *Hilton, Las Vegas, August, 2005, IEEE, Nevada, USA.*

Hidenori Aoki,Shinji Takeda, Kengo Yagyu and Akira Yamada (2006) , IEEE 802.11s Wireless LAN Mesh Network technology, *NTT DoCoMo technical Journal*, Vol.8.No.2, pp 13-21.

Mahira Atham Lebbe, Johnson I Agbinya, Zenon Chaczko and Frank Chiang (2007), Self-Organized Classification of Dangers for Secure Wireless Mesh Networks, *proceedings of Australasian Telecommunication Networks and Applications Conference 2007*, pp 322-327, ISBN: 978-1-4244-1557-1, Christchurch December 2007,IEEE , New Zealand.

Mahira Atham Lebbe (Mahira M.Mowjoon), Johnson I Agbinya, Zenon Chaczko, Robin Braun (2008). Artificial Immune System inspired danger modelling in Wireless Mesh Networks, *proceedings of International Conference on Computer and Communication Engineering*, pp 984-988, ISBN: 978-1-4244-1691-2 , Kuala Lumpur , May 2008, IEEE, Malaysia.

Matzinger P (2002), The danger model: A renewed sense of self, *Science Magazine*, vol. 296, no. 5566, pp. 301–305.

Pavel Berkhin, Survey of Clustering Data Mining Techniques, *in Accrue Software, Inc*., pp 1-56, 1045 Forest Knoll Dr. San Jose, CA 95129, http://www.ee.ucr.edu/~barth/EE242/clustering_survey.pdf, available and validated on 31.03.2009

Samuel Sambasivam and Nick Theodosopoulos (2006), Advanced Data Clustering Methods of Mining Web Documents, *proceedings of Issues in Informing Science and Information Technology*, pp 563-579 Volume 3, Salford, June 2006, England.

Ugur Halici, Artificial Neural Networks, *In: Artificial Neural networks*, pp126-138, EE543 Lecture Notes, METU EEE Ankara.

Understanding the Immune System, How It Works, *US department of Health and Human services, National Institute of Health and National Institute of Allergy and infectious diseases National Cancer Institute*, NIH publication no.03-5423, September 2003,

http://www.niaid.nih.gov/Publications/immune/the_immune_system.pdf available and validated on 05.03.2009

Mediline plus Medical Encyclopedia: Immune system structures, http://www.nlm.nih.gov /medlineplus/ency/imagepages/8932.htm, available and validated on 05.03.2009

Self-Organizing Maps
Edited by George K Matsopoulos

ISBN 978-953-307-074-2
Hard cover, 430 pages
Publisher InTech
Published online 01, April, 2010
Published in print edition April, 2010

The Self-Organizing Map (SOM) is a neural network algorithm, which uses a competitive learning technique to train itself in an unsupervised manner. SOMs are different from other artificial neural networks in the sense that they use a neighborhood function to preserve the topological properties of the input space and they have been used to create an ordered representation of multi-dimensional data which simplifies complexity and reveals meaningful relationships. Prof. T. Kohonen in the early 1980s first established the relevant theory and explored possible applications of SOMs. Since then, a number of theoretical and practical applications of SOMs have been reported including clustering, prediction, data representation, classification, visualization, etc. This book was prompted by the desire to bring together some of the more recent theoretical and practical developments on SOMs and to provide the background for future developments in promising directions. The book comprises of 25 Chapters which can be categorized into three broad areas: methodology, visualization and practical applications.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Mahira M. Mowjoon and Johnson I Agbinya (2010). Secure Wireless Mesh Network based on Human Immune System and Self-Organizing Map, Self-Organizing Maps, George K Matsopoulos (Ed.), ISBN: 978-953-307-074-2, InTech, Available from: http://www.intechopen.com/books/self-organizing-maps/secure-wireless-mesh-network-based-on-human-immune-system-and-self-organizing-map

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821