BIO INSPIRED SECURE ROUTING IN WIRELESS MESH NETWORKS

MOHAMED MOWJOON, M. & AGBINYA, J.

Abstract: *This chapter is the extension of my previous work (Mahira et al., 2009) and introduces the novel concept of implementing biological phenomena in communication system especially in the wireless world. In spite of recent advances and the move towards bio inspired systems, this chapter proposes the notion of applying Human Immune System concept and the Artificial Immune System theory to model the presence of danger in the Wireless Mesh Network and provide counter measures to protect WMN. For this purpose, the concept of biological cytokines model has been studied and set up in the research.*

Key words: *wireless mesh network, human immune system, artificial immune systems, cytokines*

Authors´ data: Dr. **Mohamed Mowjoon**, M[ahira]; **Agbinya**, J[ohnson], Centre for Real time Information Networks, School of Computing and Communications, Faculty of Engineering and Information Technology, University of Technology, Sydney, Australia, mathamle@eng.uts.edu.au, mahira.mowjoon@yahoo.com.au

This Publication has to be referred as: Mohamed Mowjoon, M[ahira] & Agbinya, J[ohnson] (2010). Bio Inspired Secure Routing in Wireless Mesh Networks, Chapter 57 in DAAAM International Scientific Book 2010, pp. 655-668, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-74-2, ISSN 1726-9687, Vienna, Austria
DOI: 10.2507/daaam.scibook.2010.57

1. Introduction

Wireless Mesh Networks (WMNs) are self organizing and self configuring wireless networks implemented with IEEE 802.11 hardware (Mahira et al., 2008a). Recently, these networks have promising applications in battle fields (soldier networks), global parking industry, mobile public safety communication, intelligent highway infra structure, rural networks, medical systems, disaster networking and many more. Even though WMN has attracted critical applications, security of WMN has not been addressed prominently. This case leads to some reluctance in deploying these networks in safety concerned environments therefore there is an urgent need to research safety measures which offer security to the wireless mesh network system. This feature will lead to provide more confidence to various users of the system. The security aspect can be viewed from various points such as 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 in order to achieve the expected secure WMN in various applications boomed in the recent past, present and looking in to grow in the future of efficient and successful deployment of WMN.

2. Routing in WMN

Researchers have developed array of new routing protocols for wireless mesh networks, an extensive list can be found at (Karol & David, 2006). Very frequently number of routing protocols emerge and characterise the functionality of WMN. The key reasons for the continuing emergence of these routing protocols are the lack of standards which define the operation of WMN and the diverse application scenarios in which WMN is deployed. IEEE 802.11s task group is the main body working on the formation of standards for WMN and the standard is still under development. Further, user demands varies from one application to another, for example a home network should offer user friendliness, minimum power consumption, efficient scalability etc. ; soldiers should be provided with high security mobility and ease of use in a Soldier network. Thus the protocol designer for a specific scenario is responsible to consider critical aspects of the application when designing routing protocols.

2.1 Classification of routing protocols

Routing protocols can be divided in to three categories, reactive, proactive, and hybrid. Reactive protocols present routing information when required, proactive systems provide up to date state information when it is ready and, hybrid protocols take advantages of both reactive and proactive schemes. In the literature there are

number of reactive protocols, proactive protocols and hybrid protocols reported. The following table shows the most popular examples for each of these protocol types.

Reactive Protocols	Proactive Protocols	Hybrid Protocols
Ad hoc On-Demand Distance Vector (AODV),	Optimized Link State Protocol (OLSR)	Hybrid Wireless Mesh Protocol (HWMP)
Dynamic Source Routing (DSR),	Destination-Sequenced Distance Vector routing (DSDV)	Hazy Sighted Link State routing protocol (HSLS),
		Zone Routing Protocol (ZRP)
		Hybrid Routing Protocol for Large Scale Mobile Ad Hoc Networks with Mobile Backbones (HRPLS)

Tab. 1. Classification of routing protocols

From the literature (Karol & David, 2006) it is found that reactive methods perform well in wireless environment due to the paucity of available bandwidth and the mobility of nodes. However, I believe that the hybrid protocols will achieve high performance, as they take advantages of both reactive and proactive schemes.

2.2 Hybrid Wireless Mesh Protocol (HWMP)

Hybrid Wireless Mesh Protocol takes advantages of both reactive protocol AODV and proactive protocol OLSR.This protocol has been proposed by 802.11s task group as a default and the standard is expected to be published by 2010 (Bahr, 2008). In addition to be the proposed standard, the following key benefits (Bahr, 2008) stimulated me to choose HWMP as the working protocol in my research

1. Flexibility to adapt to diverse scenarios
2. Mesh points learn and use the best-metric path to any destination in the mesh with low complexity
3. When a root node is configured in the mesh:
    a. Flooding of route discovery packets in the mesh is reduced if the destination falls outside the mesh
    b. The need to buffer messages at the source while on-demand route discovery is in progress is reduced
    c. Non-discovery broadcast traffic can be delivered along the tree topology
    d. On-demand routes have the topology tree to fall back during route re-discovery or when an on-demand route become engaged

2.3 Mode of operation of HWMP

In the reactive mode, firstly, the source MP transmits path request (PREQ) message to all intermediate MPs, then the request is processed and forwarded by all intermediate MPs and the reverse path from destination to source is established, afterwards the node with the path to the destination unicast path reply (PREP) message to the source MP. A tree structured network is formed by assigning a mesh point as a root node and other mesh points in the network proactively maintain paths to the root node and distance vector routing tree will be created and maintained. If the root node is not configured, reactive path discovery will be used for all routing in mesh network. If the root node is constructed a candidate path to the root node can be identified. The proactive component of HWMP works as the extension of proactive routing tree specially designed for MPs. Any MP that is configured as the route MP periodically broadcast proactive Path Request (PREQ) messages or route announcement (RANN) messages in to the wireless mesh network which will create and maintain a tree of paths to the root MP.

3. Human Immune System (HIS)

Human Immune System is a network of cells and organs that work together to defend the body against foreign invaders. A healthy immune system is capable of recognizing diverse enemies by differentiating self cells from non-self cells. (David Dugdale, 2009) Fig.1. shows the structure of the HIS.

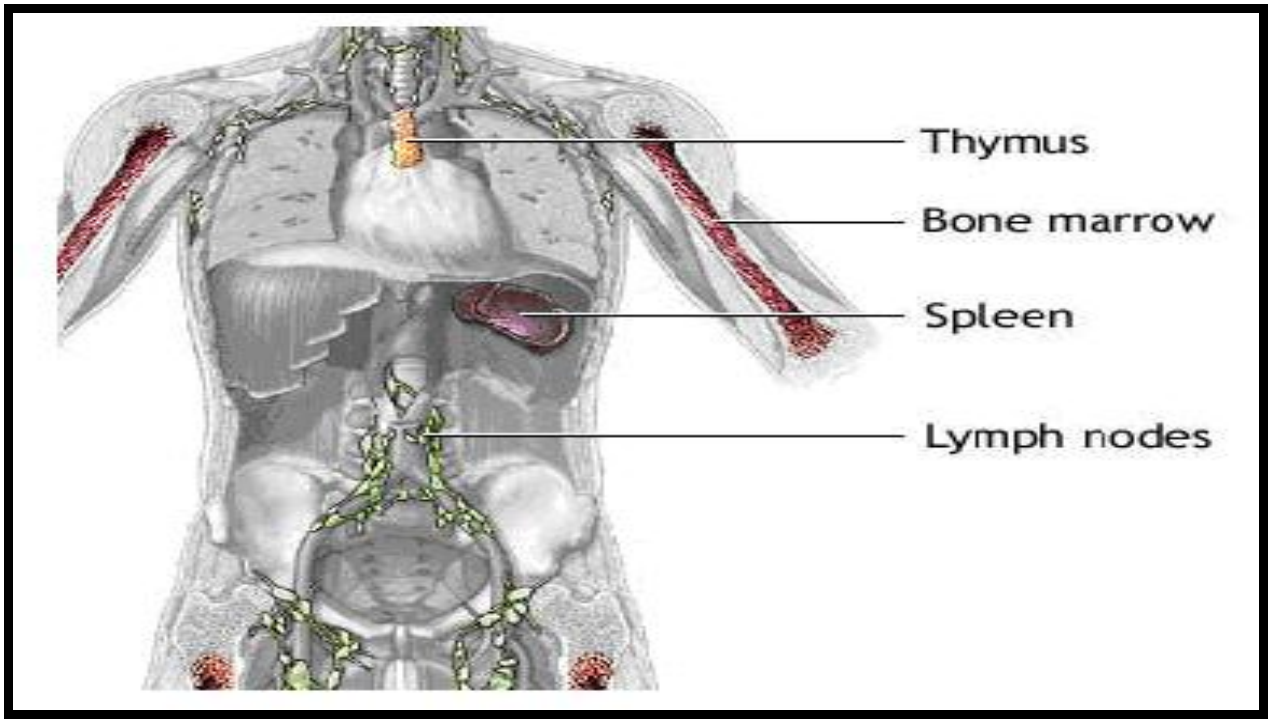

Fig. 1. Structure of HIS

Cells in HIS operate freely and create sequence of events leading to the destruction of pathogens. Immune cells can be broadly categorized in to two groups namely detectors and effectors (Sanjay & Stephen, 2004), 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 (Sanjay & Stephen, 2004).

4. Introduction to Artificial Immune System (AIS) and the Artificial Immune System Models

4.1 Introduction

The concept of AIS is still under debate and authors define the term Artificial Immune System differently. Some example definitions gathered in the literature are:

(i). (Timmis & Neal, 2000) states that "An Artificial Immune System is a computational system based upon metaphors of the natural immune system"

(ii). (Dasgupta, 1999) describes "Artificial immune systems are intelligent methodologies inspired by the immune system toward real-world problem solving"

(iii). (De Castro & Timmis, 2002b) explains "Artificial Immune Systems (AIS) are adaptive systems, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving"

4.2 AIS Models

In the literature authors discussed four Artificial Immune System models namely negative selection model, clonal selection model, immune network model and danger model.

(i). Negative Selection Model

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

(ii). Clonal Selection model

The basis for the clonal selection algorithm is the natural B-cell mechanism (Sabine, 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 (Sabine, 2007). Leandro N. de Castro and Fernando J. Von Zuben proposed an algorithm called CLONALG which is based on the natural clonal selection mechanism and represents the computational implementation of clonal selection and

affinity maturation principles accountable for behaviour of B-cells during adaptive immune responses. Fig.2. depicts the clonal selection process.

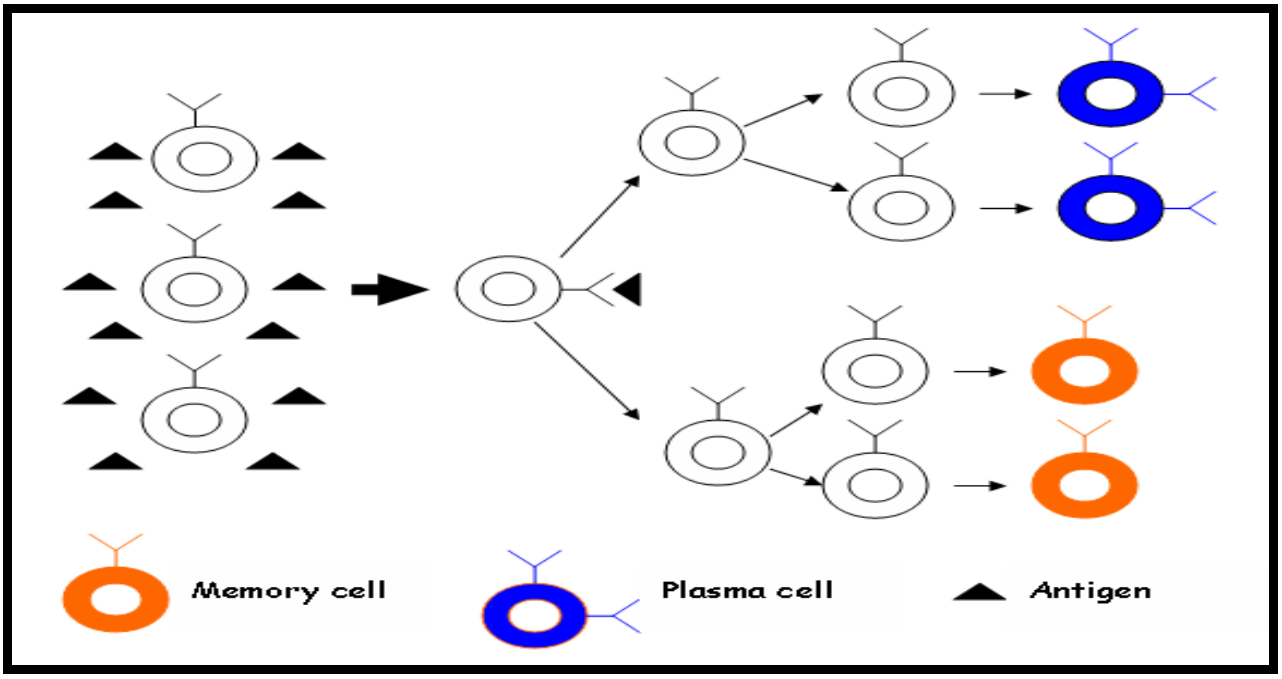

Fig. 2. Clonal Selection Process (Mahira et al., 2009)

(iii) Immune Network Model

The immune network theory implies that the immune system has a dynamic behaviour even in the absence of external stimuli (de Castro & Timmis, 2002a). Further the immune cells and molecules are capable of recognizing each other, which leads to an eigen behaviour of the system that is independent of alien stimulation. The network is activated when an antibody (cell receptor) recognises antigen and the network is suppressed when an antibody recognises an idiotope. The immune network theory suggests that 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.

(iv) The Danger Theory

Classical immunology depends on the concept of "self" and "non-self" cells distinction and 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.3. illustrates 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.

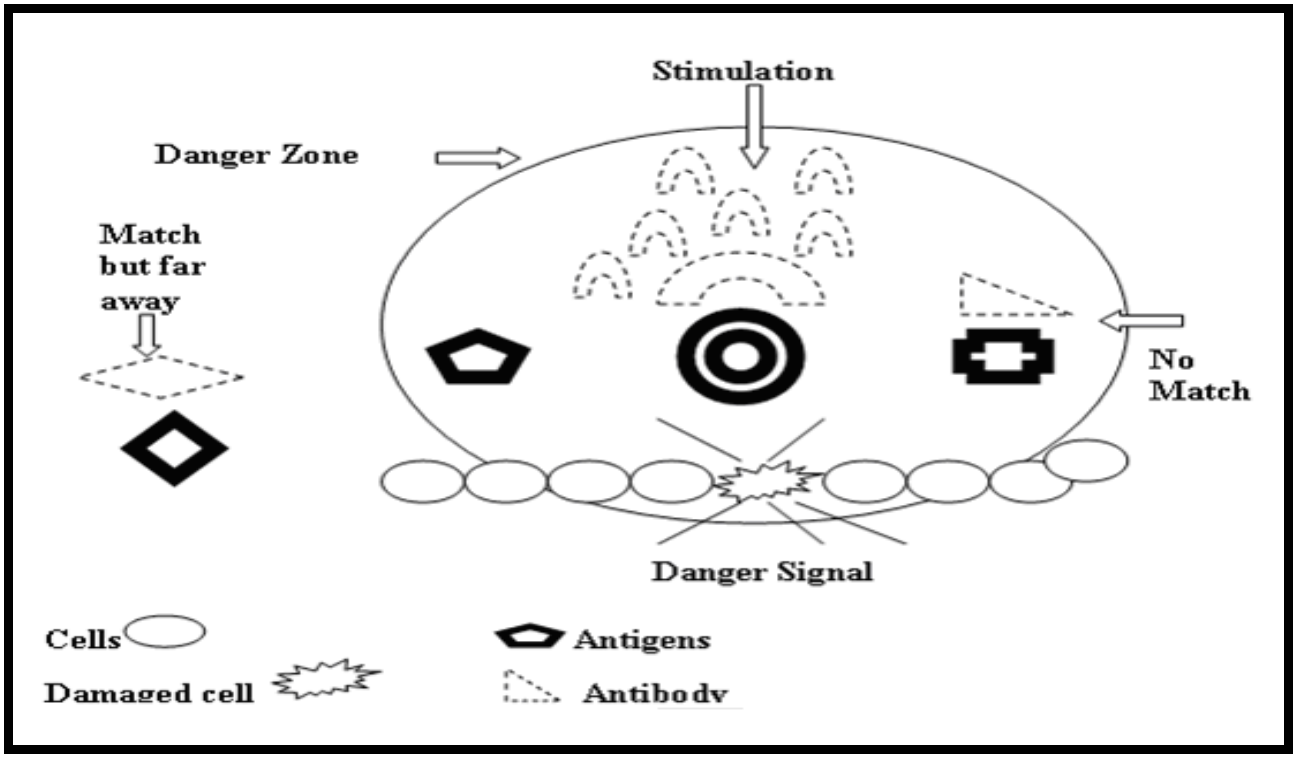

Fig. 3. Model of the Danger Theory (Mahira et al., 2008b)

5. Matching HIS elements with WMN devices

The human body is collection of billions of complex structures coordinate and operate systematically to accomplish necessary functions for sustainable life. Sustainability is the salient factor for living organisms and this concept is applicable for wireless mesh network where stability and sustainability is critical for expected functions of WMN which is deployed and designed for specific application in a specific environment and supports specific group of users intend to use the particular application. Even though the complexity of WMN system is not parallel to the complexity of the human body, the idea of coordination, sustainability, self defence mechanism and self organisation initiatives are critical in adapting HIS biological concepts in WMN operation. More over, the structure of the human body can be divided into four major categories, namely cells, tissues, organs and systems and the complexity increases from cells to systems, similarly, according to IEEE 802.11s standards the WMN structure is divided into four classes of nodes namely STA, MP, MAP and MPP. Self cells are the cells belong to the body itself, any thing out side the body is considered as non self cells. This notion can be mapped on to WMN system, where non self cells refer to Corrupted or well-behaving but unauthorized nodes inside the network or any external input either friendly or malicious, inactive or non participating nodes and well behaved network resource nodes refer to self cells in

human body. Antigen is usually a foreign substance which induces an immune response. When the body is exposed to antigens, body produces antibodies which neutralize those antigens this biological concept is mapped on to possible cause of interruption or anomalies or danger to the network in WMN environment. When anomalies and danger signals are produced in the WMN network, it is required to act accordingly in order to maintain the stability and the sustainability of the system so that the system takes necessary steps to recover or protect the system against antigen existing in the system. Cytokines play major role in communicating with cells in the body and there are various kinds of cytokines available in the system. Each cytokine performs different tasks and different cytokines communicate with different types of cells, this perception is analogous to the WMN system where various kinds of signals transferred between nodes or devices. Tab.2. depicts the matching 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

Tab. 2. Matching of HIS elements on to WMN devices

6. Linking Immune cell functions with WMN node functions

Natural cytokine network is very complicated, but in my research I take into account only the simplified version of natural cytokine network and mapped on to the WMN system that I am developing. In order to adapt the HIS concepts, in the first step nodes or devices in the WMN are mapped on to the cells in the cytokine network. According to IEEE 802.11s standard, nodes in WMN are classified in to four groups. Even though the cells in the cytokine network are classified into various categories, by grouping similar cells in to one category, the network of cells in the cytokine network is cut down in to four classes namely, T cell, B cell, Macrophage and Mast cell. Further, Immune cells identify antigens, this function is identical to the recognition of anomalous behaviours exist in the WMN system. Production of antibodies refers to the formulation of successful solutions to overcome the malicious attacks. Moreover, the T cell suppression is analogous to the wise choice of the best solution to overcome the threat exist or encountered in the WMN system. Mapping in table 3 has been derived from the analysis of immune cell functions and WMN node functions.

Immune Cells	WMN nodes
T- cell	MP
B-Cell	MAP
Macrophage	STA
Mast Cell	MPP
Recognition of Antigens	Identification of anomalous behaviors
Production of Antibodies	Formulating successful solution to overcome malicious attacks
T-Cell suppression	Eliminate redundant potential Solutions against anomalous behaviors

Tab. 3. Mapping Immune Cell function on to WMN node function

7. Cytokine network

The cytokine communication network is extremely complicated in nature. Fig.4. illustrates the simplified version of the natural cytokine network derived from Biocarta. The cytokines mentioned in most of the communication links are not complete.

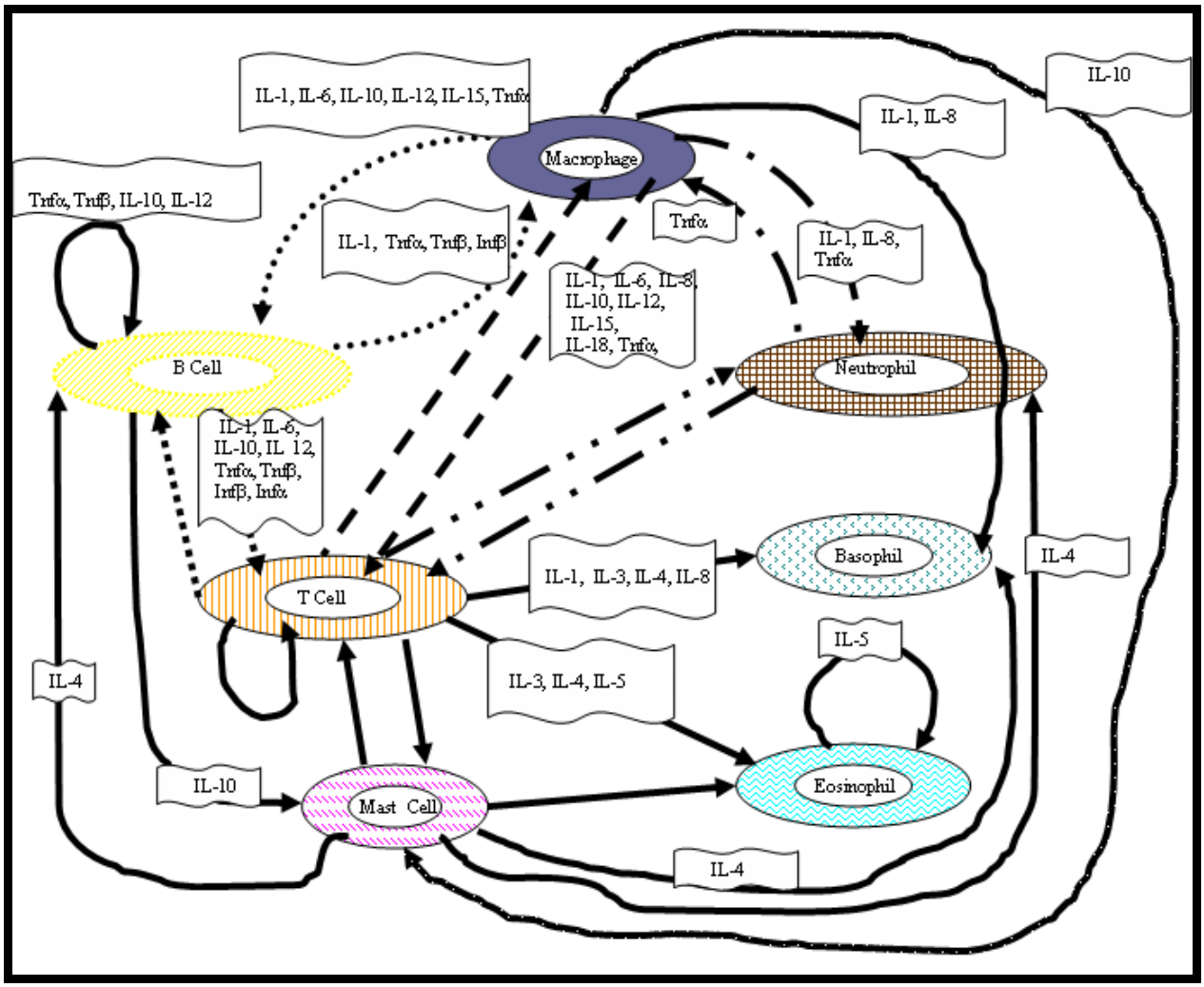

Fig. 4. Cytokine Communication Network (Mahira et al., 2009)

T-Cell in the network enhances immune responses by the secretion of specialised factors that activate other cells to fight against infection (Paul, 2008) The major function of B-Cell is the production of antibodies in response to foreign substance and identifies pathogens when antibodies on its surface bind to a specific foreign antigen (Paul, 2008).Further, B-cell signals other cells to kill or remove foreign substance from the body (Paul, 2008). Fig. illustrates the function of B-cell and T-cell mechanism, adapted from. Moreover, Macrophage is an Antigen Presenting Cell which activates adaptive immune response (Henry&Albert,2008),(Paul,2008),and Mast Cell belongs to the family of Basophil, Neutrophil and Eosinophil and present near the boundaries between the body and the outside world. Further, B-cell and T-cell mechanism is illustrated in Fig.5. and adapted from (Mahira et al., 2009).

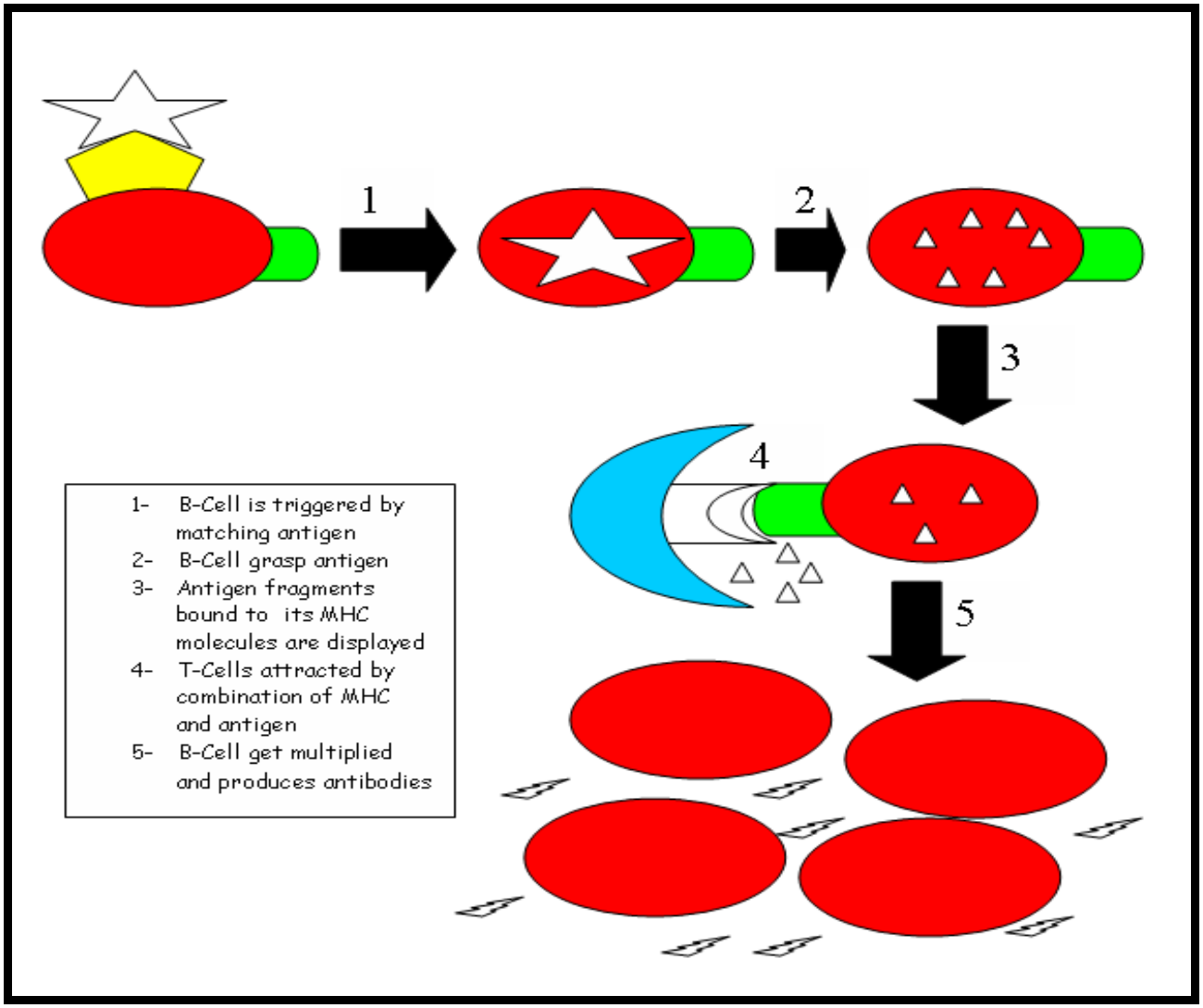

Fig. 5. B cell and T cell Mechanism

Matching antigen triggered B cell grasps antigen and shows antigen fragments bound to its MHC molecules where MHC is the major histocompatibility complex which is a large genomic region or gene family found in most vertebrates and plays an important role in the immune system, autoimmunity, and reproductive success. Then the antigen-MHC pair attracts the help of a mature matching cell. Subsequently, the cytokines secreted T cell help the B cell to multiply and mature in to antibody

producing plasma cells. These antibodies are released in to blood and lock onto matching antigens. Afterwards, the antigen antibody combination is cleared by the complement cascade or by the liver and spleen.

8. Algorithm for modelling safe WMN

The process of modelling WMN security based on danger theory consists of two steps. The first step is to recognize the danger signal and then to classify danger signals into different levels (Mahira et al., 2007). The defined danger levels are LOW (L), LOWMEDIUM (LM), MEDIUM (M), HIGHMEDIUM (HM) and HIGH (H) Further the Danger Theory runs on the following algorithm.

Receive signal
Evaluate received signal for its seriousness

If really dangerous
Perform signal classification

BEGIN

Case1: LOW
{
Trigger network
Observe the reaction
Revert to resting state after the time
}

Case2: LOWMEDIUM
{
Trigger network
Receive response from neighbours
Analyse responses
Perform actions based on the analysis
Revert to resting state after the time
}

Case3: MEDIUM
{
Trigger network
Receive response from neighbours
Analyse responses
Identify danger producing event
Perform actions based on the analysis
Revert to resting state after the time
}

Case4: HIGHMEDIUM

{
Trigger network
Receive response from neighbours
Identify signal producing element of the network
Interact with danger signal producing device
Analyse response
Perform actions based on the analysis
Revert to resting state after the time
}

Case5: HIGH

{
Trigger network
Identify danger signal producing element of the network
Interact with danger signal producing device
Produce lethal product
Perform counter measures
Revert to resting state after the time
}

END

Else
Take no counter actions
Record signal characteristics for future actions
End if
Else
Update database with new danger signal information
Use updated information for network training

End if

9. Conclusion

Further to the advancement in wireless communication networks, especially WMN, the necessity of secure WMN has been inherent by researchers in the field and the philosophy towards the application of HIS perception trigger off the novelty of the approach to attempt the challenge. The main limitation in this process is to choose the modelling parameters elegantly as the parameters vary based on the application and the generalization is meagre.

10. References

Dasgupta, D. (1999).Information Processing Mechanisms of the Immune System, in New Ideas in Optimisation, D. Corne, M. Dorigo and F. Glover (eds.), McGraw Hill, London, pp. 161-165.

Henry Y.K.Lau and Albert W.Y.Ko (2008). Coordination of Cooperative Search and Rescue Robots for Disaster Relief, Proceedings of the 17th World Congress, The International Federation of Automatic Control, seoul, Korea, 2008

Karol Kowalik and Mark Davis (2006). Why Are There So Many Routing Protocols for Wireless Mesh Networks? , Irish Signal and Systems Conference, Dublin, June 28–30, 2006

L. N. de Castro and J. Timmis (2002). Artificial Immune Systems: A Novel Paradigm to Pattern Recognition, in Artificial Networks in Pattern Recognition, J.M.Corchado, L.Alonson, and C.Fyfe (eds), SOCO-2002, University of Paisley,UK,pp.67-84.

L.N. de Castro; Timmis, Jonathan (2002). Artificial Immune Systems: A New Computational Intelligence Approach. Springer. pp. 57–58. ISBN 1852335947, 9781852335946

Mahira Atham Lebbe (Mahira M Mowjoon), Johnson I Agbinya, Zenon Chaczko (2008). Policy based danger management in Artificial Immune System inspired secure routing in Wireless Mesh Networks, *proceedings of International MultiConference of Engineers and Computer Scientists 2008*, 19-21 March, 2008, Hong Kong, China

Mahira M Mowjoon (Mahira Atham Lebbe), Johnson I Agbinya and Zenon Chaczko (2009), Replicating Cytokines in Modelling Signal Exchange between Nodes in Wireless Mesh Networks, *proceedings of the International MultiConference of Engineers and Computer Scientists 2009* , Vol I, ISBN:978-988-17012-2-0 , Hong Kong, March 2009,China.

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 2008*,May 13-15, 2008, Kuala Lumpur, Malaysia

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.

Nicholas R. Jennings (1999) Agent-Based Computing: Promise and Perils, http://dli.iiit.ac.in/ijcai/IJCAI-99%20VOL-2/PDF/107.pdf, available and verified on 12.02.2009

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

Sabine Bachmayer (2007), Artificial Immune Systems, from http://www.cs.helsinki.fi/u/niklande/opetus/SemK07/paper/bachmayer.pdf, accessed 2009-01-13

Sanjay Goel, Stephen Bush (2004). biological models of security for virus propagation in computer networks from *http://www.albany.edu/~goel/publications/goellogin12004.pdf,* accessed *2009-03-09*

Timmis, J. & Neal, M. (2000).Investigating the Evolution and Stability of a Resource Limited Artificial Immune System, *Proc. of the Genetic and Evolutionary Computation Conference, Workshop on Artificial Immune Systems and Their Application*, pp. 40-41

Bahr, (2008). from http://www.ikr.uni-stuttgart.de/Content/itg/fg524/Meetings/2008-10-27- Muenchen/01_ITG524_Muenchen_Bahr.pdf- accessed 2009-03-06

Dugdale David C. (2009). Immune system structures from *http://www.nlm.nih.gov/medlineplus/ency/imagepages/8932.htm, Accessed on* 2009-03-05

*** (2009) *http://training.seer.cancer.gov/module_anatomy/unit1_1_body_structure .html, Accessed* on: *2009-04-27*

Smith S.E. (2009). What is an Antigen?available from http://www.wisegeek.com/what-is-an-antigen.htm accessed 2009-04-27

Linnemeyer, Paul (2008). The Immune System -- An Overview available from *http://www.thebody.com/content/art1788.html* accessed *2009-01-31*

*** (2006) *http://en.wikipedia.org/wiki/Ad_hoc_protocol_list IEEE 802.11 TGs, "Joint SEE-Mesh/Wi-Mesh Proposal to 802.11 TGs,", Accessed on:2009-03-05*

*** (2009) *http://en.wikipedia.org/wiki/Immune_system, Accessed on*; *2009-01-31*

*** (2009) *http://en.wikipedia.org/wiki/File:B_cell_activation.png, Accessed on: 2009-01-31*

*** (2009) *http://en.wikipedia.org/wiki/mast_cell, Accessed on: 2009-01-29*

*** (2009) *http://en.wikipedia.org/wiki/B_cell, Accessed* on: *2009-04-28*