Research Journal of Applied Sciences, Engineering and Technology 3(9): 1026-1033, 2011
ISSN: 2040-7467

Submitted: July 26, 2011 Accepted: September 05, 2011 Published: September 20, 2011

Detecting Resource Consumption Attack over MANET using an Artificial Immune Algorithm

[1]Maha Abdelhaq, [1]Rosilah Hassan, [2]Mahamod Ismail and [3]Daud Israf
[1]School of Computer Science, Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600, UKM Bangi, Selangor Darul Ehsan, Malaysia
[2]Department of Electrical, Electronics and Systems Engineering, Faculty of Engineering, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia
[3]Department of Biomedical Sciences, Faculty of Medicine and Healthy Sciences, UPM, 43400, Serdang, Selangor, Malaysia

Abstract: The Human Immune System (HIS) is considered as a bank of models, functions, and concepts from where Artificial Immune algorithms are inspired. These algorithms are used to secure both host-based and network-based systems. However, it is not only important to utilize the HIS in producing AIS-based algorithms as much as it is important to introduce an algorithm with high performance. Therefore, creating a balance between utilizing HIS on one side and introducing the required AIS-based intrusion detection algorithm on the other side is a crucial issue which would be valuable to investigate. Securing the mobile ad hoc network (MANET) which is a collection of mobile, decentralized, and self organized nodes is another problem, which adds more challenges to the research. This is because MANET properties make it harder to be secured than the other types of static networks. We claim that AISs' properties such as being self-healing, self-defensive and self-organizing can meet the challenges of securing the MANET environment. This paper's objective is to utilize the biological model used in the dendritic cell algorithm (DCA) to introduce a Dendritic Cell Inspired Intrusion Detection Algorithm (DCIIDA). DCIIDA is introduced to detect the Resource Consumption Attack (RCA) over MANET. Furthermore, this study proposes a DCIIDA architecture which should be applied by each node in MANET.

Key words: Artificial immune system, attack, dendritic cell algorithm, denial of service attack, mobile ad hoc networks, resource consumption danger theory

INTRODUCTION

The Human Immune System (HIS) is one of the most powerful biological systems, which has attracted computer scientists to envision its utilization in Intrusion Detection Systems (IDSs) (Wu and Banzhaf, 2010). However, many Artificial Immune System (AIS) researches did not achieve the desired performance. Understanding the biology does not necessarily mean the ability to emulate it as it is, with all of its models and functions. Utilizing the concepts and principles of HIS that benefit the AIS environment is enough to gain the promised performance (Drozda *et al*., 2010). To improve the introduced AIS algorithms' performance, Uwi Aickelin *et al*. (2003) have established the "danger project" which is based mainly on the danger theory in immunology.

Danger theory (Matzinger, 1994) implies that the response type of the immune system to the incoming pathogens is based mainly on the existence of danger or safe signals from the body tissues caused by that pathogen. The Dendritic Cell Algorithm (DCA) is one of the most well-known danger project contributions. DCA utilizes the role of the Dendritic Cells (DCs) in HIS as forensic navigators and important anomaly detectors (Greensmith, 2007; Greensmith *et al*., 2005, 2010). DCs are defined as antigens presenting lymphocytes in the innate immunity; these lymphocytes play the main role in either stimulating or suppressing the adaptive immunity T-cells and hence controlling the immune system's type of response.

DCA's capability as an anomaly detector algorithm (Greensmith, 2007; Greensmith *et al*., 2005, 2010) inspires us to utilize its biological model to introduce a further DC inspired algorithm, which could detect another type of attack over Mobile Ad hoc Network (MANET). In addition, many of MANET's special characteristics and properties are similar to the innate immunity's abstract features; such as the openness and susceptibility of each to different types of danger attacks (Twycross and

Corresponding Author: Maha Abdelhaq, School of Computer Science, Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600, UKM Bangi, Selangor Darul Ehsan, Malaysia

Aickelin, 2005). Therefore, we argue that the proposed algorithm's features can also meet the security requirements of the MANET environment as a mobile, decentralized, limited power, and limited capacity wireless network.

The objective of this study is to explain the capability of the danger theory AIS intrusion detection algorithms, in particular, the introduced DC Inspired Intrusion Detection Algorithm (DCIIDA) in detecting the Resource Consumption Attack (RCA) over MANET. DCIIDA uses a different methodology in treating the incoming antigens and signals than that used in DCA. Furthermore, the paper proposes the DCIIDA architecture to be applied by each MANET node.

MATERIALS AND METHODS

This research has been conducted in the University Kebangsaan Malaysia, in the faculty of Information Science and Technology, Computer science Department between March and July 2011. This section sheds light on some of them and explains DCA in depth.

Related works:

Sarafijanovic and Boudec (2004, 2005) introduced the first researches that utilized AIS to be applied on MANET. The proposed AIS registered a detection rate of about 55% but the whole system could only detect a simple dropping packet attack over MANET. Kim *et al.* (2006) used a theoretical integration between the DCA and a directed diffusion routing protocol to protect the sensor network from interest cache poisoning attacks. Fanelli (2010) proposed The Network Threat Recognition with Immune Inspired Anomaly Detection (NetTRIIAD) model. The model consists of two main layers - the innate layer which emulates the innate immunity in HIS, and the adaptive layer which emulates the general abstract adaptive immunity in HIS. NetTRIIAD is used to detect DoS, dropping packets and delaying packets attacks over wired networks. Drozda *et al.* (2010) use the concept of co-stimulation to introduce an AIS algorithm over MANET. The algorithm detects three types of attacks over MANET, which are the wormhole attack, dropping packets attack, and packet delay attack. However, the algorithm depends mainly in one of its stages on the watchdog intrusion detection method which fails in two scenarios; when a collision occurs, or the malicious node changes its power to make it include the previous node but not the next one (Marti *et al*., 2005).

Dendritic cell algorithm: This study is concerned with the biological model used in DCA which was proposed by Greensmith (2007) Greensmith *et al.* (2005, 2010). DCA is inspired from immunological researches on DCs because of their desired biological role as mobile anomaly detectors. The algorithm was verified by applying it to detect a port scanning attack over the wired network

Table 1: Weights used to process the input signals in Eq. (1)

Wijp	PAMP J = 0	Danger signal J = 1	Safe signal J = 2
csm p = 1	2	1	2
semi p = 2	0	0	3
mat: p = 3	2	1	-3

(Greensmith *et al*., 2010). According to the biological model on which DCA based, each DC is exposed to a collection of input antigens and the available input signals which are in four main categories: (i) Pathogen Associated Molecular Pattern (PAMP) signals, (ii) Danger signals, (iii) Safe signals, and (iv) Inflammation signals. Each DC applies the concentration equation 1 using the input signals and empirically calculated weights in Table 1 to calculate the concentration of three main DC outputs; Costimulatory molecules (csm), smDC cytokines (semi), and mDC cytokines (mat). The main indices and data structures of Eq. (1) are as follows:

- Indices:
  = 0… i; input signal index;
  = 0… j; input signal category index;
  m = 0…. m; DC index;
  p = 0……p; DC output signal index;
- Data Structures:
  S = tissue signal matrix; (the concept of "tissue signal" is explained in (Greensmith, 2007; Greensmith *et al*., 2010)).
  S_{ij}= a signal type i, category j in the signal matrix S; (matrix S explanation Can be found in (Greensmith, 2007; Greensmith *et al*., 2010)).
  S(m) = signal matrix of DC(m);
  O_p(m) = output signal p of DC(m);
  W_{ijp} = transforming weight from S_{ij} O_p.

$$O_p(m) = \frac{\sum i \sum j \neq 3 \, WijpSij(m)}{\sum i \sum j \neq 3 \, |Wijp|} \forall P \qquad (1)$$

When csm exceeds a certain fuzzy threshold, the DC migrates, and the calculated concentrations of semi mature and mature output signals are compared to give the DC the context of the larger value. Hence, each DC context is given to the whole collection of antigens exposed to certain signals into that DC in a certain fuzzy threshold time. At the end of the algorithm, each antigen context value is registered in a log file. Therefore, the degree of maturation for each antigen is calculated as in Eq. (2):

Mature Context Antigen Value (MCAV) =
The no. of times the antigen appeared as mature /
The no. of times it appeared in the log file (2)

Table 2: The innate immunity properties and its corresponding MANET characteristics.

The innate immunity properties	MANET characteristics
The innate immunity environment is open to the outer pathogens	C1
Each phagocyte has a limited capacity to process the proteins	C2
The phagocytes move frequently throughout different types of body tissues in a flexible decentralized manner.	C3, C5 and C6
Phagocytes interact with each other through cytokinetic signals	C4
Phagocytes perform computational processing for the incoming proteins in parallel, i orde rto help th human body survive	C7

Although DCA is effective in real time IDSs, its results register high false positive alarm rates and low detection accuracy rates in some experiments (Greensmith, 2007). Therefore, this study utilizes the DC biological model in another way, and proposes a DC inspired algorithm, which promises to increase the accuracy of the detection rate and decrease the false positive rate.

Artificial Immune Systems and Manet: AIS intrusion detection algorithms aim at getting benefits from the HIS subsystems by mapping their functions and concepts in biology into abstract artificial frameworks. Mapping between HISs and AISs is a challenge which needs testing and verification. This section sheds light on introducing MANET as a technology capable of being an application for danger theory-based AIS algorithms.

Mobile ad hoc network overview: MANET is a rapidly deployable, self-organized, multi-hop wireless network, and is typically set up for a limited period of time and for particular applications such as for military, disaster areas, and medical applications. Nodes in MANET may move arbitrarily while communicating over wireless links. This network is typically used in situations where there is no centralized administration or support from networking infrastructure such as routers or base stations. Therefore, the mobile nodes should act as router end-systems, and organize themselves into a wireless network. Many up-to-date researches pay attention to work on MANET as a new technology with specific characteristics, which distinguish it from other types of networks. These characteristics are as shown in the following (Cayirci and Rong, 2009; Wang and Zhi, 2008).

C1-openness: MANET nodes communicate with each other through an open wireless medium. Hence the outer attackers can easily join the trusted node environment.
C2-Limited resources: MANET has limited power and bandwidth capacity.

C3-Mobility and dynamicity: MANET consists of highly frequently mobile nodes which cause high dynamicity in its topology changes and reconfiguration.
C4-Wireless medium signaling: The nodes in MANET interact with each other through wireless signaling.

C5-Flexibility: MANET could be deployed in any type of area, even if they are unstable such as military purposes areas, or the areas of frequent nature disasters.

C6-Decentralization and self-organizing: MANET is an infrastructure-less wireless network with no centralized management points, so every node manages itself by itself and can help in managing the other nodes but with no centralization such as necessary for sending alarm messages when an attacker is detected. C7-Distributed computation: Each node performs a routing processing and a security processing, and informs the other nodes to help the network survive.

The analogy between MANET and the innate immunity framework: The innate immunity in biology has an important role in detecting danger coming from outside to invade the human body. It consists of forensic navigator cells, which navigate throughout the body tissues to protect them from dangerous pathogens. The innate immunity cells as mobile, self-organizing, and flexible cells inspire the showing of the analogy between the MANET environment's special characteristics and the abstract properties of the innate immunity environment based on the work of Twycross and Aickelin (2005). In Table 2, the analogy between the general innate immunity properties and the corresponding MANET characteristics as mentioned in the previous subsection is shown clearly.

Aodv and its Vulnerability to Resource Consumption Attack: The AODV routing protocol (Perkins and Royer, 1999) is the underlying routing protocol used in this research. AODV is a reactive self-starting and large-scale routing protocol. The AODV routing protocol has been extensively studied and developed over many years, which proves its robustness and benefits. The main two advantages of the AODV protocol are: firstly, the connection setup delay with the destination is lower comparing with other MANET routing protocols. Secondly, AODV avoids the congested paths in comparison with the other ad hoc routing protocols (Taneja and Kush, 2010). However, AODV is vulnerable to different types of attacks. The following subsections explain AODV processes and how it is vulnerable to RCA over MANET.

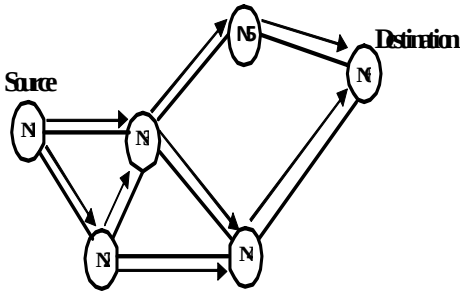

Fig. 1: Propagation of RREQ packet

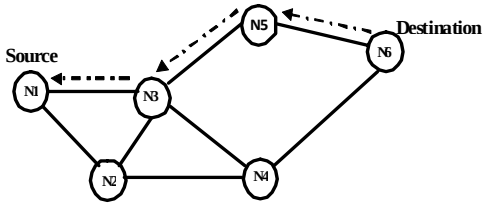

Fig. 2: The path of RREP packet

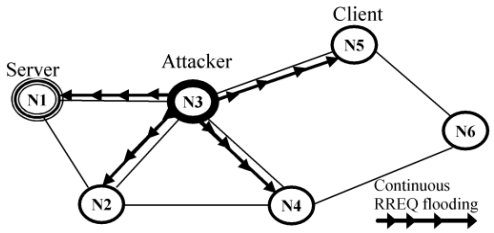

Fig. 3: RREQ broadcasted by RCA

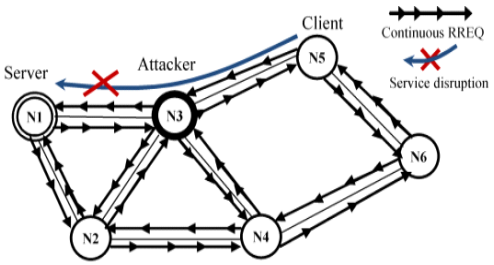

Fig. 4: RREQ packets flooding by RCA

AODV routing protocol and how it is vulnerable to RCA: In the route discovery process of the AODV routing protocol over MANET (Perkins and Royer, 1999), the source node broadcasts the route request (RREQ) packet throughout MANET nodes -as shown in Fig. 1 - and sets a timer waiting for the reply. The RREQ packet contains routing information such as: the originator IP address, the broadcast ID, and the destination sequence number. Each intermedate node receives the RREQ packet and keeps the reverse path to the source node besides performing two processes: firstly, it verifies if it has received the RREQ packet before with the same originator IP address and broadcast ID, then decides either to discard the RREQ packet or accept it. Secondly, if the RREQ packet is accepted, the intermediate node checks the destination sequence number stored in its routing table; if it is greater than or equal to the one stored in the RREQ packet it unicasts the route reply (RREP) packet to the source node. If no intermediate node has a fresh enough (fresh destination sequence number) route to the destination node, the RREQ packet keeps its navigation until it reaches the destination node itself which in turn unicasts the RREP packet towards the source node as shown in Fig. 2.

The attacker as shown in Fig. 3 keeps the RREQ packet with a different broadcast ID in order to notify each node broadcasting continuously and consume its limited resource of energy, bandwidth, and memory.

As noticed, the attacker does not follow AODV rules. Therefore, to achieve its attack successfully, it does not set a timer waiting for a reply but keeps overflowing the network with RREQ packets as shown in Fig. 4. MANET is very vulnerable to this type of attack since its limited bandwidth capacity simplifies overflowing of the link very easily and quickly. When MANET links have overflowed with malicious packets, the congested links will be jammed and congested which leads to interruption in accessing services of the available servers in the network. In Fig. 4 if node N1 represents a server, then its service could be isolated by the attacker N3.

RESULTS AND DISCUSSION

Using DCIIDA to detect the resource consumption attack: As mentioned early, many properties are shared between MANET and the innate immune system; one important property is that the two environments are open and vulnerable to danger either from outside or inside. All of the sharing features and the environment's nature encourage utilization of danger theory-based AISs which abstract their functionality from the innate immunity and its cells. Dendritic cells are one of the innate immunity cells which inspire the introduction of an intrusion detection algorithm in this study, called DCIIDA. The following subsections show how the proposed DCIIDA could be effective in detecting RCA over MANET.

The proposed system architecture: As shown in Fig. 5, a mapping between HIS and MANET is performed in general. For example, each message in MANET represents the entered pathogen to the human body. Also,

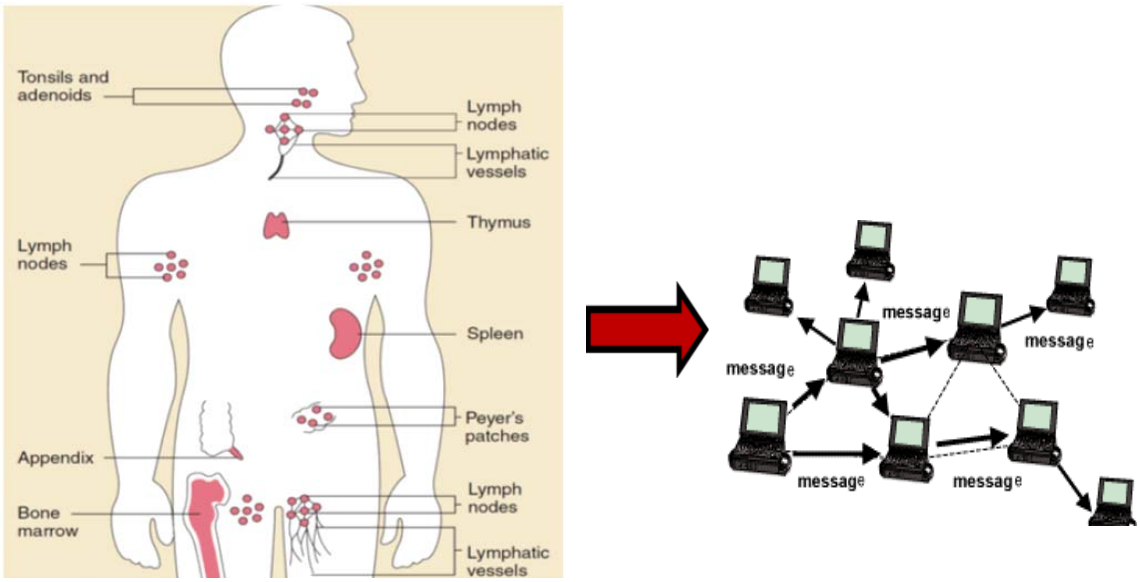

Fig. 5: Mapping HIS model into AIS algorithm over MANET (NIAIDS, 2003; UT, 2010)

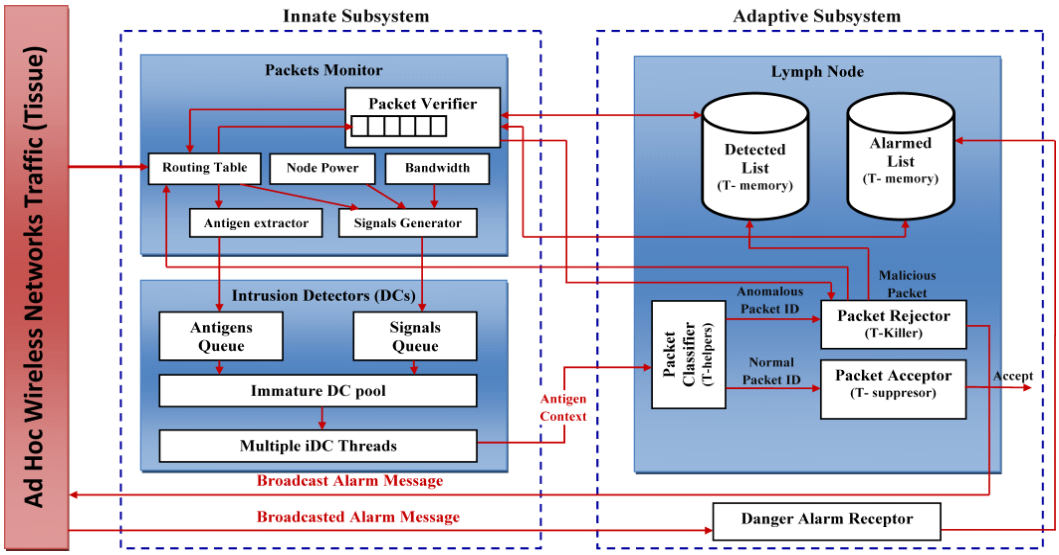

Fig. 6: The proposed DCIIDA architecture

each node represents the human body; therefore, each node must apply DCIIDA to protect itself from intrusions just as each human body contains the immune system to protect itself from dangerous pathogens.

According to Fig. 6 the proposed architecture consists of two main subsystems; the innate subsystem and the adaptive subsystem. The architecture represents a conceptual mapping of the proposed DCIIDA pseudocode in Fig. 7.

Each packet received by the routing table must be verified by the DCIIDA firstly before starting the AODV routing protocol. Therefore, each received packet's ID is checked by the packet verifier in the memory. If that packet ID is found in the detected list, this means that it comes from an attacker detected before. The algorithm rejects the packet directly, deletes it from the routing table and sends an alarm message for the second time for that packet ID. Otherwise, if the packet ID is found in the alarmed list, that means the packet comes from an attacker detected by another node, so it is rejected directly, and deleted from the routing table but without sending an alarm again. Otherwise, the packet must be verified by

```
Input: traffic packets.
Output: extracted antigens and signals.

store input packet in queue.
While queue != null
get packet ID;
verify packet ID in memory;
    If packet ID exists in detected list
reject packet;
delete the packet information from the routing table;
broadcast alarm message;
 else if packet ID exist in alarmed list
reject packet;
delete the packet information from the routing table;
 else
extract packet antigen;
store packet antigen in antigen queue;
extract packet signal;
store packet signal in signal queue;
 end if
end while
While antigens queue != null & iDCThread < thread threshold
start iDCThread;
end while
// iDC Thread
While iDC == true
While csm < output signal migration threshold
search antigens queue for same antigens ID;
get same antigens ID;
search signals queue for corresponding signals;
get corresponding signals;
compute the output;
compute the cumulating output;
end while
If semi-mature output > mature output then
packet ID is normal;
accept the packet;
start the routing algorithm;
else packet ID is attacker
reject the packet;
delete the packet information from the routing table
broadcast alarm message;
store packet ID in detected list;
end if
```

Fig. 7: The pseudo code of the proposed DCIIDA

DCIIDA. Hence, if the packet verifier does not delete the packet routing information from the routing table, then the antigen extractor starts extracting the packet antigens from the routing table and stores them in the antigens queue. At the same time, the signals extractor starts extracting the packet signals from the routing table and other resources concerned with evaluating the node battery power and the available bandwidth. The extracted signals then are stored in the signals queue.

Unlike DCA, DCIIDA utilizes the abstract functionality of the DCs in HIS as intrusion detectors in a different way; for each available antigen with a new ID, the algorithm initiates an immature DC (iDC) object from the iDC pool that plays in one thread. Each iDC object searches the antigens queue for new antigens with the same ID, and then it searches the signals queue for signals related to the collected antigens which come from the behavior of the same node. Therefore, each DC will

represent the context of one type of antigen only. In this way, DCIIDA decreases the high false positive rate drawback in DCA in which the context of one mature DC is given to its different types of antigens, which may include benign antigens; also the same drawback of high false negative is raised when the context of semi mature DC is given to all of its antigens, even if they include malignant antigens. After that, each iDC calculates the output signals which resulted from the input entities. The iDC continues in this operation in iteration and does not stop until the iDC transfers to the maturation state which means becoming either semi-mature or fully mature. In each iteration, iDC adds the value of calculated output signals to the value of updated cumulating output signals that indicates the maturation state as in DCA (Greensmith, 2007; Greensmith *et al*., 2005, 2010). DCIIDA operates multiple iDCs in multiple threads for each different antigen's new ID. When the iDC reaches the maturation state, it migrates from the innate sub-system to the adaptive sub-system. Specifically, to the classifier that plays the abstract role of T-helpers semi-mature cells. If DC is in the semi-mature state, it will suppress any fighting reaction and therefore, the classifier will transfer the DC to the packet acceptor. On the other hand, if the DC is a fully matured DC, it will stimulate the classifier to transfer it to the packet rejecter unit that plays the abstract role of T-killers. The maturation state of each DC represents the state of the antigens it holds. So, the antigens collected by semi-mature DC are considered as benign and its source node packets considered as normal. Also, the antigens collected by fully mature DC are considered as malignant and its source node packets considered as malicious. The normal packets are accepted, and the AODV routing protocol as a result is allowed to process these normal packets. But the anomalous packets are treated differently; the packet rejecter rejects these packets, deletes their routing information from the routing table, registers them in the detected list, and sends an alarm for the all neighbor nodes to inform them about the attacker. Finally, the proposed DCIIDA architecture contains a danger alarm receptor that receives the alarms which come from the neighbor nodes and registers them in the alarmed list. It is of value to mention that DCIIDA promises less false positive and more detection rates than DCA since it uses multiple threads to process the same antigen types.

Antigens: In HIS, antigens and tissue signals are two important inputs for DCs to control T-helper response; either to fight the malignant antigens or suppress fighting the benign ones. Signals represent the symptoms of danger or safe state existence. However, antigens represent the resource of danger or a safe state.

According to DCIIDA over MANET, the resource of normal or anomalous behaviors is the mobile nodes themselves. Identifying the resource node of danger helps to preclude it forever by isolating it from the network. Therefore; DCIIDA considers the antigen to be the IP address of the RREQ packet originator. In this way, DCIIDA could perform two types of responses: firstly, it detects the danger very early especially when the same attacker comes again. Secondly, it prevents the attack in the whole network by broadcasting the IP address of the malicious node via alarm messages throughout the network.

Signals: DCA includes four main input signals that specify the behavior of the input antigens. This paper utilizes three input signals only: (i) PAMP signal, (ii) Danger signal, and (iii) Safe signal. The Inflammation input signal has not yet been utilized in this paper. The details of DCIIDA signals are as follows:

- High rate of the received RREQ control packets by the routing table (PAMP): the abnormal increase in the received rate of RREQ control packets by the routing table indicates strongly the existence of a resource consumption attack. The routing table supports the packet verifier in the DCIIDA architecture with this information as a PAMP signal to the available antigens.
- Abnormal rate of the battery power consumption (danger signal): if the node's battery loses its power at an abnormal rate, this indicates the success of the RCA. However, this signal absence does not necessarily mean the absence of the attacker; since it is only at the beginning of the attack that the high rate of thereceived RREQ packets is noticed.
- Failure in routing discovery and data packets delivery (danger signal): when the attacker overflows the wireless links with bogus RREQ packets, it becomes congested and floods easily and quickly because of its limited bandwidth. This problem causes failure in both routing discovery and data packet delivery.
- Success in routing discovery and data packet delivery (safe signal): taking into consideration that the processing of the safe signals in parallel with the other signals decreases the false positive rate in the intrusion detection algorithm. However, the existence of these signals does not mainly prove the absence of attack. If the node had succeeded in initiating its routes and communicates with the other nodes freely, this means, somehow, the failure of RCA attacker(s).

CONCLUSION

This study has utilized the benefits of the dendritic cell model used by the DCA algorithm to develop a

danger theory-based AIS over MANET. The proposed DCIIDA has been supported by a proposed architecture which represents a conceptual mapping of the DCIIDA pseudo code. DCIIDA promises less false positive and more detection rates than DCA since it uses multiple threads to process the same antigen types.

DCIIDA will be verified and tested by performing simulation experiments in the future work. However, in the future experiments, the csm fuzzy threshold should be determined in a superior way which would avoid the drawback of high false positive rates. Furthermore, the number of operated iDC will be determined to get the required benefit balanced with the required performance. Finally, more signals and antigens will be added to enhance the intrusion detection precision and decrease the possible false positive rates.

ACKNOWLEDGMENT

This research is supported by Network Communication Technology Group (NCT) http:// www.ftsm.ukm. my/network/. University Kebangsaan Malaysia (UKM), 2011.

REFERENCES

Aickelin, U., P. Bentley, S. Cayzer, J. Kim and J. McLeod, 2003. Danger theory: The link between AIS and IDS? Proceedings of the 2003 International Conferenceon Artificial Immune Systems (ICARIS). LNCS, Springer Heidelberg, 2787: 147-155.

Cayirci, E. and C. Rong, 2009. Security in Wireless Ad Hoc and Sensor Networks. WILEY, United Kingdom.

Perkins, C.E. and E.M. Royer, 1999. Ad hoc on-demand distance vector routing. Proceedings of the 1999 IEEE Workshop on Mobile Computing Systems and Applications, pp: 90-100.

Drozda, M., S. Schaust and H. Szczerbicka, 2010. Immuno-inspired Knowledge Management for Ad Hoc Wireless Networks Springer, Heidelberg, 260: 1-26.

Fanelli, R., 2010. Further experimentation with hybrid immune inspired network intrusion detection. Proceedings of the 2010 International Conference on Artificial Immune Systems (ICARIS), LNCS 6209, Springer, Heidelberg. pp: 264-275.

Greensmith, J., U. Aickelin and S. Cayzer, 2005. Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection. Proceedings of the 2005 International Conference on Artificial Immune Systems (ICARIS). LNCS, Springer, Heidelberg, 3627: 153-167.

Greensmith, J., 2007. The dendritic cell algorithm, Ph.D. Thesis, The University of Nottingham. UK.

Greensmith, J., U. Aickelin and G. Tedesco, 2010. Information fusion for anomaly detection with the dendritic cell algorithm. Inf. Fusion, 11: 2134.

Kim, J., P. Bentley, C. Wallenta, M. Ahmed and S. Hailes, 2006. Danger is ubiquitous: Detecting malicious activities in sensor networks using the dendritic cell algorithm. Proceedings of the 2006 International Conference on Artificial Immune Systems (ICARIS). LNCS, Springer, Heidelberg, 4163: 390-403.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2005. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 2005 International Conference on Mobile Computing and Networking, pp: 255-265.

Matzinger, P., 1994. Tolerance, danger, and the extended family. Annual Rev. Immunol., 12: 991-1045.

Sarafijanovic, S. and J.Y. Le Boudec, 2004. An artificial immune system for misbehavior detection in mobile ad-hoc networks with virtual thymus, clustering, danger signal and memory detectors. Proceedings of the 2004 International Conference on Artificial Immune Systems (ICARIS), pp: 342-356.

Sarafijanovic, S. and J.Y. Le Boudec, 2005. An artificial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks. IEEE Trans. Neural Networks, 16(5): 1076-1087.

Taneja, S. and A. Kush, 2010. A Survey of routing protocols in mobile ad hoc networks. Int. J. Innov. Manag. Technol., 1: 279-285.

Twycross, J. and U. Aickelin, 2005. Towards a conceptual framework for innate immunity. Proceedings of the 2004 International Conference on Artificial Immune Systems (ICARIS). LNCS,. Springer, Heidelberg, 3627: 112-125.

United States Government. 2003. NIAIDS. Understanding the Immune System, How It Works. NIH Publication No. 03-5423. U.S. National Institutes of Health.

University of Tokyo (UT), 2010. Retrieved from: http:// www.mcl.iis.u-tokyo.ac.jp/eng_version/index. html.

Wang, D., M. Hu and H. Zhi, 2008. A survey of secure routing in ad hoc networks. Proceedings of the 2008 IEEE International Conference on Web Age Information Management, pp: 482-486.

Wu, S.X. and W. Banzhaf, 2010. The use of computational intelligence in intrusion detection systems. Appl. Soft Comput., 10: 1-35. Elsevier.