Prevention in Sleep Deprivation Attack in MANET

Surendra Kumar[1], Satish Alaria[2], Dr. Vijay Kumar[3]

[1]*Research Scholar, Kautilya Institute of Technology and Engineering, Jaipur, Rajasthan*
[2]*Assistant Professor, Kautilya Institute of Technology and Engineering, Jaipur, Rajasthan*
[3]*Professor, Kautilya Institute of Technology and Engineering, Jaipur, Rajasthan*

***Abstract*— MANET is a collection of mobile, decentralized, and self-organized nodes. Securing MANET is a problem which adds more challenges on the research. This is because MANET properties make it harder to be secured than the other types of static networks. It suffers from a variety of security attacks and threats such as: Denial of Service (DoS), flooding attack, impersonation attack, selfish node misbehaving, routing table overflow attack, wormhole attack, blackhole attack etc. MANET is open to vulnerabilities as a result of its basic characteristics like no point of network management; topology changes vigorously, resource restriction, no certificate authority or centralized authority. This paper objective is to summarize different types of attacks over MANET, and concerns with studying sleep deprivation attack. Our objective is to design an artificial immune system to secure from sleep deprivation attack and is based on biological Danger Theory and we imply the concept of using two thresholds on the basis of throughput. In this paper we count on the number of requests sent by a particular node in a given interval of time twice, once for minor threshold and later for major threshold.**

Keywords—MANET, AODV, HIS, Route Discovery, Sleep Deprivation Attack, NS 2.35

I. INTRODUCTION

MANET as a mobile, decentralized, limited power, and limited capacity wireless network requires securing its environment using robust, self organized, and self healing algorithms such as the artificial immune system (AIS) algorithms. Routing protocols for mobile ad hoc networks generate a large amount of control traffic when node mobility causes link states and the network topology to change frequently. On the other hand, resources such as bandwidth and battery power are usually severely constrained in such networks. Therefore, minimizing the control traffic to set up and maintain routing state is one of the main challenges in the design of scalable routing protocols for mobile ad hoc networks. One approach to limit control traffic is to establish routes on demand rather than proactively. On-demand routing protocols [1] only establish a route to a destination when it is necessary to send packets to that destination, and therefore incur less overhead at the expense of higher route setup latency. Hybrid routing protocols [1],[2] combine both on-demand and proactive elements for more edibility in the latency-overhead trade. On-demand routing overhead can be broken down into two components: route discovery and route maintenance. In AODV, whenever a source S needs to communicate with a destination D, it checks for an existing route to D in the routing table. If the route is not present, it initiates a route discovery by broadcasting a RREQ (Route Request) packet which is flooded [3] into the network in a controlled manner, until it reaches the destination or until it reaches a node, which knows a route to the destination. Then, the destination or an intermediate node sends back a Route Reply (RREP) message, which includes the number of hops in between. Each node receiving the RREP message records a forward route to the destination and, thus, knows only the next hop required for a given route.

In 2003, Aickelin et al [4] came up with a project called ―danger project‖ in order to support utilizing the danger theory in developing Danger theory-based AIS algorithms. Danger theory [5] implies that the concentration of the danger or safe signals which come from the body tissues and caused by specific antigens control the response of the Human Immune System (HIS) to either tolerate or fight those antigens.

Dendritic cell algorithm (DCA) [6] is one of the most well-known danger project contributions. It utilizes the functionality of the dendritic cells in the innate immunity of the HIS. DCA proved the capability of detecting port scanning attack which certifies its qualification as an anomaly detector algorithm. However, Abdelhaq et al. [7] and Kim et al. [8] showed the analogy between the characteristics of MANET and sensor networks environments respectively from one side, and the general properties of the innate immunity from another side. This opens the way of utilizing DCA to detect other types of attacks over frequently changed environments such as Mobile Ad hoc Network (MANET).

The Ad hoc On Demand Distance Vector (AODV) routing protocol builds on the DSDV algorithm. AODV is advancement on DSDV because it typically minimizes the number of required broadcasts by creating routes on a demand basis, as just opposed to maintaining a full list of routes as in the DSDV algorithm. AODV declare as a pure on-demand route receiving system, since nodes that are not on a selected way do not maintain routing information or participate in routing table exchanges. When a source node wants to send a message to the destination node and does not already have a valid route to that destination, it starts a path discovery process to locate the other node. It

broadcasts a route request (RREQ) packet to its neighbor nodes, which then forward the request to their neighbor nodes, and so on, until either the destination or an intermediate node with a fresh enough routes to the destination is found. AODV use destination sequence numbers to ensure all routes are loop free and contain the most recent route information. Every node maintains its own sequence code, as well as a broadcast ID. The broadcast ID is incremented for every RREQ the node starts, and together with the node's IP address, uniquely recognized an RREQ. Once the Route request reaches the destination node or an intermediate node with a fresh enough route, the destination intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the route request. As the route reply is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer that will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ, AODV supports the use of symmetric links only [3][4].

II. ATTACKS ON MANETS

There are many types of attacks that form a real threat when applied on MANET; each type of attack varies from the other ones in the way of applying the threat, the goal of attacking, and the stack layer that is targeted by the attacker. Some attacks are passive and others are active. Active attacks may be internal or external. In the internal type of attacking the attacker is located inside the attacked MANET so it is dangerous as the attacker is considered at the beginning as a trusted node. However, in the external type of attack the attacker comes from outside the MANET network so it is easier to be detected as it is not well trusted. Passive attacks have been only performed internally. Active and passive attacks are defined as follows [9], [10], and [11]:

1. Passive attack: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping and traffic analysis; each one is explained as in table 1:

 Eavesdropping: The intruder silently listens to the communication by tapping the wireless link.

 Traffic analysis: The intruder analyses the traffic communications in order to gain information about the network topology and hence inject the attack in a strategic place (e.g. near the cluster head) that help the threat succeed.

2. Active attack: in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed:

 Denial of Service: The intruder aims to overflow the link by fake packets in order to make a link jam and hence down the path to the intended server to stop the service. Also, it could deplete the nodes' energy such as, *sleep deprivation attack* or *resource consumption attack.*

 Black hole: The intruder injects the control routing packets with fake information in order to attract the node that requested the route and hence gain that route. After the intruder acquires the route, the intruder could apply different types of attacks.

 Dropping packets: The intruder simply drops a packet into the network destined for the target node. If it performs a selective dropping, it will be harder to be detected.

 Delaying packets: In this attack, the intruder does not forward the received packets directly even if the link is empty.

 Worm hole: In this attack, a cooperation between two intruders as a minimum is required to communicate through a high speed link to deceive the nodes that wrongly consider the malicious link as the shortest path to the destined node.

 Sink hole: In this attack, the intruder attracts the nodes to use its fake route and hence it could easily inject any type of attack.

 Exploiting node penalizing schemes: In this attack, the intruder broadcasts error messages about well performing nodes and causes jamming to consider these nodes to be put on the black list.

 Routing table overflow: In this attack, the intruder overflows the nodes' routing tables with fake routing information.

III. EXISTING FRAMEWORKS

Sarafijanovic and Boudec [12] 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. Kim et al [5] used a theoretical integration between the DCA and directed diffusion routing protocol to protect the sensor network from interest cache poisoning attack. Drozda et al [13] use the concept of co-stimulation and communication between the innate immune system and the adaptive immune system to introduce an AIS intrusion detection algorithm over MANET. This paper is concerned with the DCA proposed by Greensmith et al [3].

As mentioned in [7], 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 nature encourage utilizing the danger based AISs which are abstracted their functionality from the innate immunity and its cells. Dendritic cells are one of the innate immunity cells which

inspired developing a danger based AIS intrusion detection algorithm called DCA. The following subsections show how DCA could be effective in detecting sleep deprivation attack over MANET.

IV. OUR PROPOSAL

The basic protocol that we used in our work is AODV i.e Ad-Hoc On Demand Distance Vector protocol . It is one of the most basic protocols used in ad-hocnetworks. Since MANET is also a class of ad-hoc networks so AODV is an obvious choice. The best thing about AODV is that it uses on-demand routing approach which implies that the network is functional only when a connection is required, otherwise it is silent.

The node which needs a connection, broadcasts a request for connection. OtherAODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the needy node. When a node receives such a message and already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The needy
node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time.

The advantage of AODV is that it creates no extra traffic for communication along existing links. Also, distance vector routing is simple, and doesn't require
much memory or calculation. However AODV requires more time to establish a connection, and the initial communication to establish a route is heavier than some other approaches.

In the route discovery process of AODV routing protocol over MANET, the source node broadcasts the route request (RREQ) packet throughout MANET nodes -as shown in Figure 1- and set a timer waiting for the reply. Each intermediate node receives the RREQ packet checks if it has fresh enough route to the destination. If yes, it unicasts the route reply (RREP) packet to source node else, 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 Figure 2.

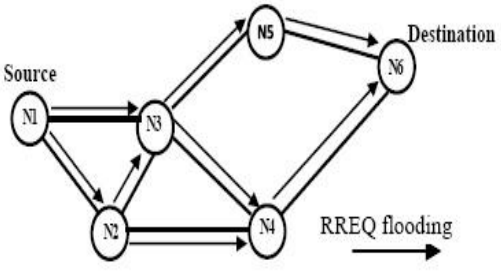

Figure 1. Propagation of RREQ packet

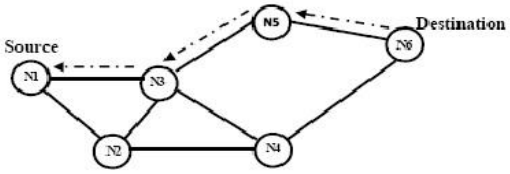

Figure 2. The path of RREP packet

In sleep deprivation attack the attacker exploits the route discovery process in AODV routing protocol as shown in Figure 3 the attacker keeps broadcasting the RREQ packet in order to notify each node continuously and consume its limited resource of energy, bandwidth, and memory. As shown in Figure 4, the attacker keeps overflowing the network with RREQ packets. When MANET links have been congested with malicious packets, the attacker could interrupt using the services of the available servers in the network. In Figure 4 if node N1 represents a server, then its service could be isolated by the attacker N3.

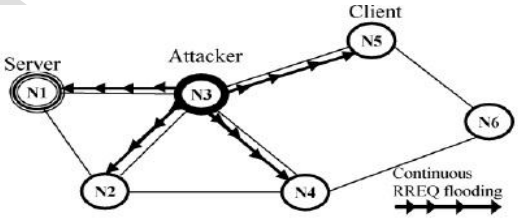

Figure 3. RREQ broadcasted by sleep deprivation attacker

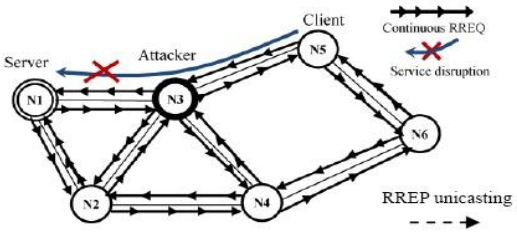

Figure 4. RREQ packets flooding by sleep deprivation attacker

ALGORITHM

Input: Queue of incoming packets
While (Queue not empty)

1. if sender belongs to black list
reject the packet;
fetch the next packet;

2. else if sender belongs to grey list
ifblackalarm()
reject the packet;
fetch the next packet;
else if whitealarm()
get the packets from queue;
serve the packets request;

fetch the next packet;
else put the packet into waiting queue;
fetch the next packet;

3. else if sender belongs to white list serve the packets request;
if (reqcnt<minorthreshold)
incrementminthrescntr;
else if (reqcnt<majorthreshold)
incrementmajthrescntr;

4. else if (minthrescntr _ minorthreshold)
put senders name to grey list;
sendgreyalarm() signal;
else if (majthrescntr _ majorthreshold)
put senders name to black list;
sendblackalarm() signal;
else put senders name to white list;
sendwhitealarm() signal;

V. SIMULATION

In the proposed scenario, we've taken 4 cases according to the drop out in thethroughputs. All the cases have a certain fixed value for the minor and major thresholds. The results of the 4 cases also vary according to these threshold values. The following are the screenshots of the various simulations carried out on the same 16 node structure:

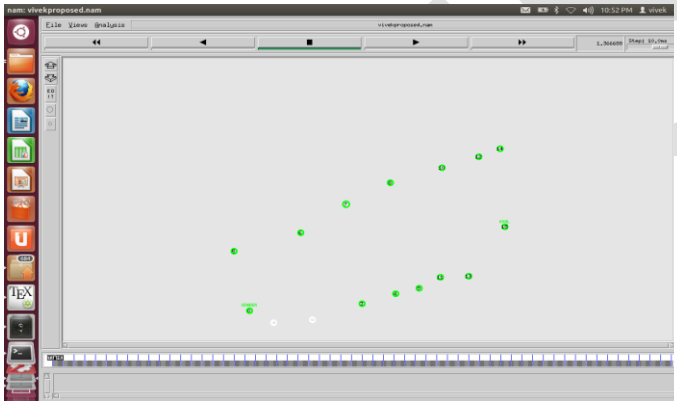

Figure 5. Proposed Scenario-1

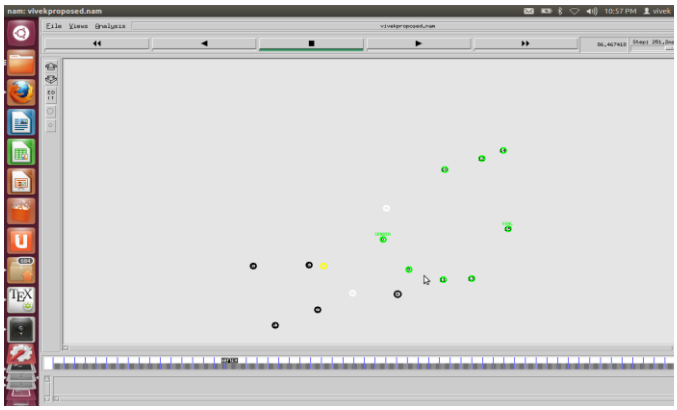

Figure 6.Proposed Scenario-2

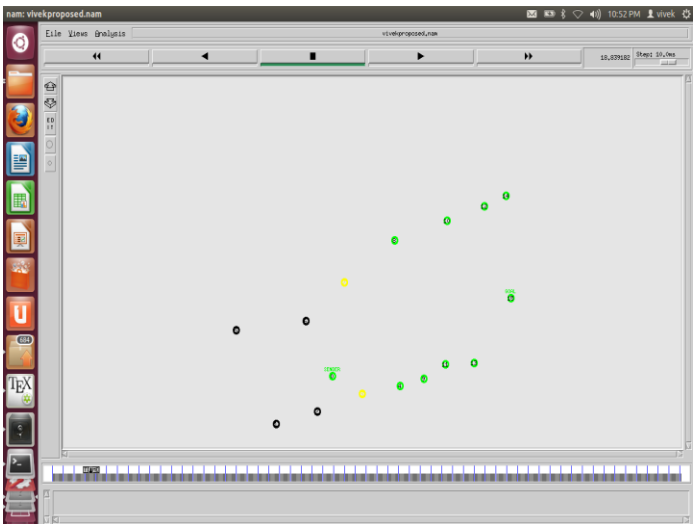

Figure 7.Proposed Scenario-3

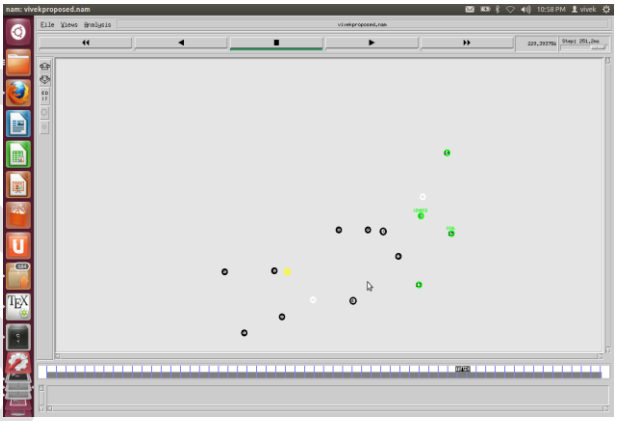

Figure 8.Proposed Scenario-4

The energy consumption under all the 4 cases is calculated by a suitable awk
file in which the parameters of energy are defined.
.

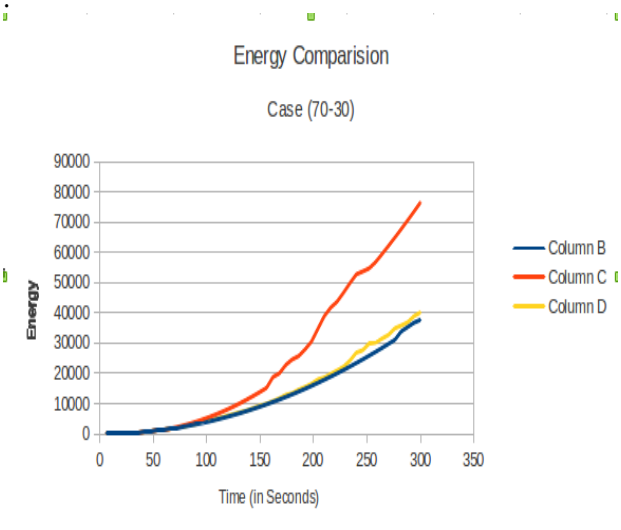

Figure 9. Energy Case-1

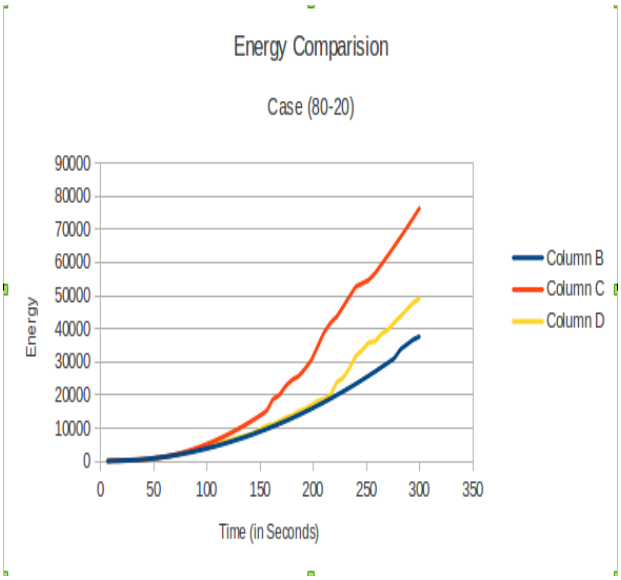

Figure 10.Energy Case-2

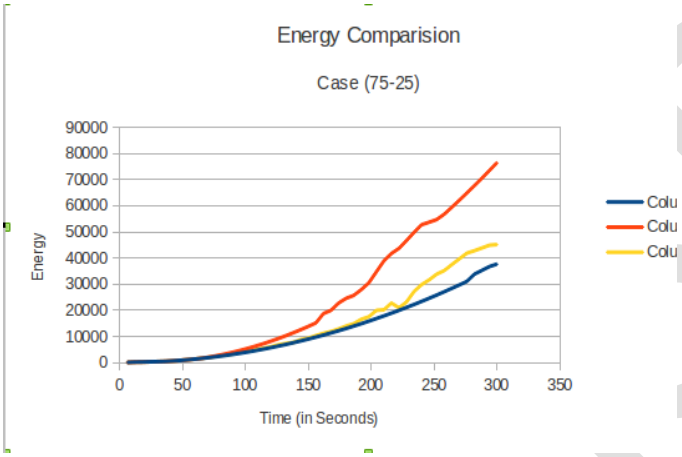

Figure 11.Energy Case-3

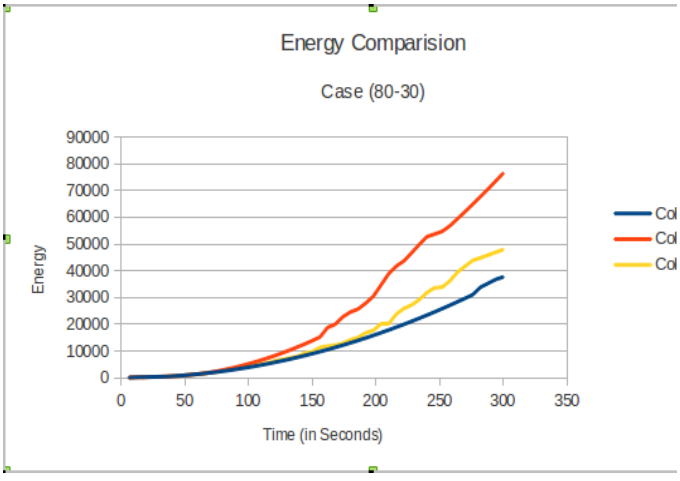

Figure 12. Energy Case-4

Finally when we compare all the 4 cases we find out that the energy values of all the 4 cases differ by good margins but the throughput is almost the same. The reason behind almost similar throughputs is that the packets are equally served in all the cases. But, if we look at the overall performance of the 4 cases, we found that the 80-20 case served as the worst because there was a huge gap between the 2 thresholds in this case. It pointed out an attacker much early and took a long time to finally take a call. The 70-30 case was the best case since it took time to declare a node as an attacker and then quickly adjudged it in considerable amount of time. The
energy consumption and throughput values both were optimized in this case.
Finally, the 75-25 and 80-30 cases were almost similar in nature. The 75-25 was good in throughput while 80-30 was good in terms of energy. The gap
between the thresholds was the same in both these cases but still 75-25 was better than 80-30 marginally.

VI. CONCLUSION AND FUTURE WORK

In our work we compared the energy consumption and throughput values under '4'various categories and used the concept of 2 thresholds instead of one. The use of 2 thresholds and inclusion of waiting queue caused a substantial overhead but still we was able to handle sleep deprivation attack to a great extent. We found out that the energy consumption to be varying under the 4 scenarios but the throughput values were almost the same for all 4 cases. But still the case where we considered 30-70 percent drop in throughput turned out to be our most efficient scenario since it handled most of the challenges very well.
In future work, we should test the practicality of using 2 thresholds to a higher level and take more and more scenarios to analyse the impact of my work
based on 2 thresholds. There is one more thing that instead of throughput we can take energy as the parameter to decide the values of the thresholds.

REFERENCES

[1] X. Hu, J. Wang, and C. Wang, ―Routing in Mobile AdHoc Networks,IEEE conference.
[2] P. Albers et al., ―Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing TrustBased Approaches,1st Int‘l. Wksp. WL Info. Sys. 4th Int‘l. Conf. Enterprise Info. Sys. 2002
[3] L. Venkatraman and D. P. Agrawal, ―Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks,‖ J. Parallel Distrib. Comp., 2002.
[4] Aickelin, U., Bentley, P., Cayzer, S., Kim, J., and McLeod, J.: Danger Theory: The Link between AIS and IDS? In: Timmis, J., Bentley, P.J., Hart, E. (eds.) ICARIS 2003. LNCS, vol. 2787, pp. 147–155. Springer, Heidelberg (2003).
[5] Matzinger, P.: Tolerance, Danger, and the Extended Family. Annual Review of Immunology 12, 991–1045 (1994).
[6] Greensmith, J., Aickelin, U., and Tedesco, G.: Information Fusion for Anomaly Detection with the Dendritic Cell Algorithm. Information Fusion. 11, 21--34. Elsevier (2010).
[7] Abdelhaq, M., Hassan, R., and Saqour, R.: Using Dendritic Cell Algorithm to detect the Resource Consumption Attack over MANET. In Proceedings of the 2nd international conference of software engineering and computer systems (ICSECS2011). LNCS, vol. 181, pp. 429-442, Springe-Verlag (2011).

[8] Kim, J., Bentley, P., Wallenta, C., Ahmed, M.,andHailes, S.: Danger Is Ubiquitous:Detecting Malicious Activities in Sensor Networks Using the Dendritic Cell Algorithm. In: Bersini, H., Carneiro, J. (eds.) ICARIS 2006. LNCS, vol. 4163, pp.390–403. Springer, Heidelberg (2006).
[9] Wang, D., Hu M., and Zhi, H.: A survey of Secure Routing in Ad Hoc Networks. In: 9th IEEE International Conference on Web Age Information Management, pp. 482-486. IEEE Press, Zhangjiajie Hunan (2008).
[10] Cayirci, E., and Rong, C.: Security in Wireless Ad Hoc and Sensor Networks.WILEY, United Kingdom (2009).
[11] Su, X.: Integrated prevention and detection of byzantine Attacks in mobile ad hoc networks. Phd. Thesis. The University of Texas at San Antonio.USA (2009).
[12] Sarafijanovic, S., and Le Boudec, J.Y.: An artificial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks. IEEE Transactions on Neural Networks 16(5), 1076–1087 (2005).
[13] Drozda, M., Schaust, S., and Szczerbicka, H.: Immuno-inspired Knowledge Management for Ad Hoc Wireless Networks. E. Szczerbicki& N.T. Nguyen (eds.). 260, 1—26. Springer, Heidelberg (2010).