Detecting Sleep Deprivation Attack over MANET Using a Danger Theory –Based Algorithm

[1]Maha Abdelhaq, [2]Rosilah Hassan, [3]Mahamod Ismail, [4] Raed Alsaqour, [5]Daud Israf

[1,2,4] School of Computer Science, Faculty of Information Science and Technology,
University Kebangsaan Malaysia, 43600, UKM Bangi, Selangor Darul Ehsan, Malaysia.

[3]Department of Electrical, Electronics and Systems Engineering, Faculty of Engineering,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, MALAYSIA

[5]Department of Biomedical Sciences, Faculty of Medicine & Healthy Sciences, UPM,
43400, Serdang, Selangor, Malaysia

[1]maha@ftsm.ukm.my, [2]rosilah@ftsm.ukm.my,[3]mahamod@eng.ukm.my
[4]raed.saqour@ftsm.ukm.my, [5]daud@medic.upm.edu.my

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. This paper objective is to summarize different types of attacks over MANET, and concerns with studying sleep deprivation attack. Therefore, this paper utilizes one of the danger theory intrusion detection algorithms, namely, the dendritic cell algorithm (DCA) to detect the sleep deprivation attack over MANET. In this paper, DCA is plugged in a proposed mobile dendritic cell algorithm called MDCA which represented through a proposed MDCA architecture.

KEYWORDS

Mobile Ad Hoc Networks (MANET), Human Immune System (HIS), Sleep deprivation attack, Danger Theory, Artificial Immune System (AIS), Dendritic Cell Algorithm (DCA).

1 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.

In 2003, Aickelin et al [1] 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 [2] 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) [3] 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. [4] and Kim et al. [5] 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 objective of this paper is to summarize different types of attacks over MANET, and concerns with studying sleep deprivation attack. Also, this paper explains the capability of the danger theory-based AIS intrusion detection algorithms, in particular DCA to detect sleep deprivation attack or called also, resource consumption attack (RCA) over MANET. In addition, the paper introduces a mobile dendritic cell algorithm (MDCA) architecture in which DCA plugged to be applied by each MANET node.

This paper is structured as follows: Section 2 introduces a background of MANET different types of attacks. Next, section 3 displays a review of both AIS-based and non AIS- based intrusion detection algorithms and techniques. Section 4 explains AODV routing protocol and its vulnerability to sleep deprivation attack. Next, section 5 explains how MDCA is capable to detect the sleep deprivation attack over MANET. Finally, section 6 represents a conclusion for this research with future work.

2 ATTACKS OVER MANET

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 [6], [7], and [8]:

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.
- *Sybil:* In this attack, the intruder masquerades under the identity of multiple nodes.
- *Rushing:* In this attack, the intruder broadcasts a route request and reply packets very quickly in order to make the nodes discard any other control packet in the network.
- *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.
- *Detour:* In this attack, the intruder creates virtual nodes on the optimal routes to appear longer and costlier than the other non-optimal routes; these forces the nodes to wrongly use the non-optimal route.
- *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.
- *Selfishness:* In this attack, the intruder does not relay the others' received packets, and suppresses the other nodes to sleep in along back offs on the MAC layer so it can use the link any time.
- *Hello flood:* In this attack, the intruder broadcasts hello messages to all the network nodes by using strong enough power to be wrongly considered as their neighbor.

3 THE APPLICATION OF SLEEP DEPRIVATION ATTACK OVER AODV ROUTING PROTOCOL

AODV routing protocol [9] is the underlying routing protocol used in this research. AODV is a reactive self-starting and large scale routing protocol. However, it is vulnerable to different types of attacks. This section explains AODV processes and how it is vulnerable to sleep deprivation attack over MANET. 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.

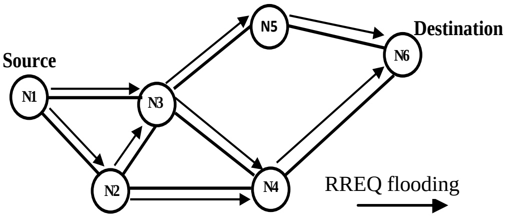

Figure 1. Propagation of RREQ packet

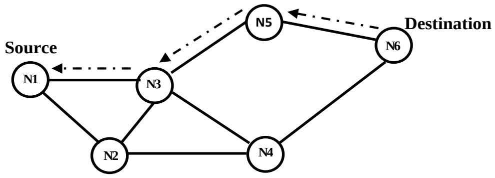

Figure 2. The path of RREP packet

In sleep deprivation attack [10, 11] 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.

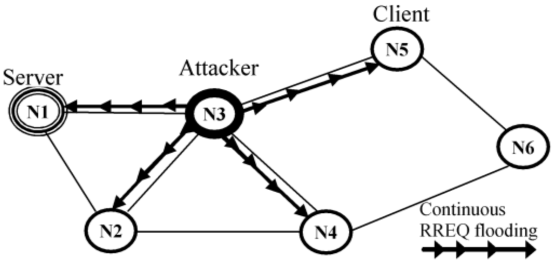

Figure 3. RREQ broadcasted by sleep deprivation attacker

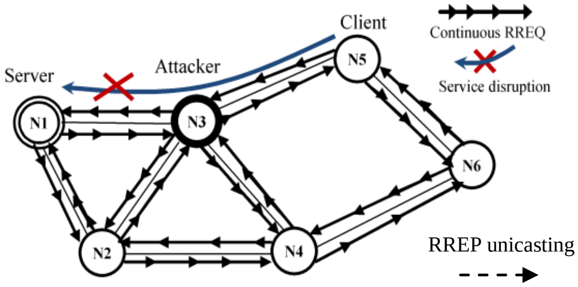

Figure 4. RREQ packets flooding by sleep deprivation attacker

4 DANGER THEORY-BASED AISs

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]. DCA is inspired from immunological researches on DCs because of their desired characteristics as mobile anomaly detectors in the human body. The algorithm was verified by applying it to detect port scanning attack over wired networks.

5 USING DCA TO DETECT SLEEP DEPRIVATION ATTACK

As mentioned in [4], 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.

5.1 The Proposed System Architecture

As shown in Figure 5, DCA has been plugged in a new architecture called MDCA architecture. The name shows that the proposed architecture will be performed by each MANET node since each node should protect itself from danger locally without using mobile agents. MDCA architecture consists of two main subsystems; the innate subsystem and the adaptive subsystem. The architecture represents a conceptual mapping of MDCA pseudo code algorithm shown in Figure 6.

At the beginning, the algorithm verifies each entered packet’s ID in the memory. If that packet ID found in the detected list, this means it comes from an attacker detected before, the algorithm rejects the packet directly, deletes its information from the routing table and sends an alarm message for the second time for that packet ID. Else if the packet ID is found in the alarmed list, this means the packet comes from an attacker detected by another node so it is rejected directly, deleted from the routing table but without sending alarm again. Else, the packet must be analyzed by the packet analyzer.

The packet analyzer extracts the required antigens from the routing table and generates the signals from the routing table, the availability of the bandwidth, and the power consumption rate. After that, the packet analyzer stores the antigens and signals in the antigens and signals stores respectively. The available antigens and signals formulate the main input for DCA to detect the sleep deprivation attack over MANET.

DCA utilizes the abstract functionality of DCs in biology, its outputs of antigens and their corresponding contexts as benign or malignant transfer to the packet classifier in the adaptive subsystem. The packet classifier plays the abstract role of T-helpers cells in the HIS therefore; if the output antigen context is benign it suppresses any fighting reaction against the antigen by transferring it to the packet acceptor same as the abstract role of T-suppressor cells.

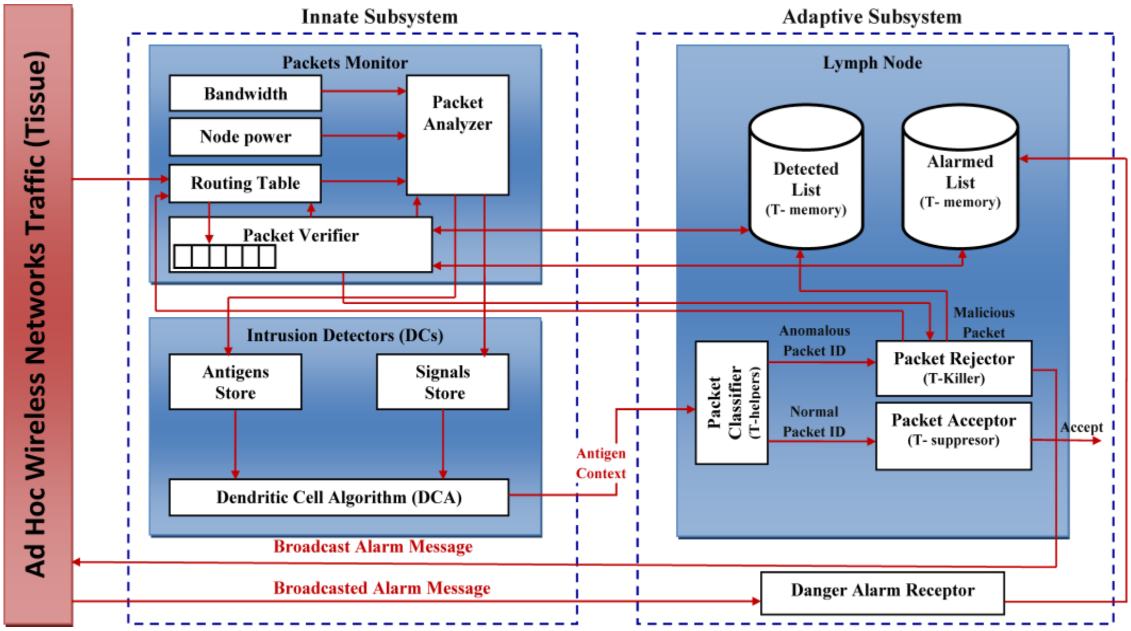

Figure 5. The Proposed MDCA architecture

Otherwise, if the output antigen context is malignant, the packet classifier stimulates fighting that antigen by transferring it to the packet rejecter unit which simulates the abstract role of T-killer cells in HIS.

Benign antigens represent the packet ID of normal nodes and vice versa, malignant antigens represent the packet ID of the malicious nodes.

The normal packets are accepted. But the anomalous packets treated differently, the packet rejecter rejects these packets, deletes them from the routing table, registers them in the detected list, and sends an alarm message for the whole neighbor nodes to inform them about the attacker.

Finally, MDCA architecture as shown in Figure 5 contains a danger alarm receptor that receives the alarms which come from the neighbor nodes and registers them in the alarmed list to isolate the attacker and prevent it after detecting its anomalous behaviors.

5.2 The Proposed Antigens

In HIS, antigens and tissue signals are two important inputs for DCs to control T-helpers 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 safe state.

According to MDCA over MANET, the resource of normal or anomalous behaviors is the mobile nodes themselves. Identifying the resource node of danger helps preventing it forever by isolating it from the network. Therefore; MDCA considers the antigen to be the IP address of the RREQ packet's originator. By this way, MDCA 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 in alarm messages throughout the network.

5.3 The Proposed 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, (iii) Safe signal, and the Inflammation input signal has not yet utilized in this paper. The details of MDCA 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 resource consumption attack. The routing table supports the packet verifier in MDCA 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 losses its power in abnormal rate, this indicates the success of sleep deprivation attack. However, this signal absence does not mean necessarily the absence of the attacker; since at the beginning of the attack the high rate of the received RREQ packets is only 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 flooded easily and quickly because of its limited bandwidth. This problem causes failure in both routing discovery and data packets delivery.

● Success in routing discovery and data packets delivery (safe signal): taking into consideration to process 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 improve mainly the absence of attack. If the node succeeded in initiating its routes and communicates with the other nodes freely, this means -in somehow- the failure of sleep deprivation attacker(s).

```
Input : traffic packets
Output: classified packets as
         normal or malicious.

Store input packet ID in Queue
While packet queue!=  null
      get packet ID
      verify packet ID in memory
  if packet ID exists in detected
     list
      reject packet
      delete the packet info
      from the routing table
      broadcast alarm message
  else if packet ID exist in
     alarmed list
      reject packet
      delete the packet info
      from the routing table
  else
      extract packet antigens
      transfer packet antigen to
      antigen store
      extract packet signals
      transfer packet signals to
      signal store
      call DCA
    if antigen is benign
      accept the packet
      start the routing
      algorithm
    else
      reject the packet
      delete the packet info
      from the routing table
      broadcast alarm message
      store packet ID in
      detected list
    end if
  end if
end while loop
```

Figure 6. The proposed MDCA pseudo code

6 CONCLUSIONS AND FUTURE WORK

This paper has utilized the benefits of one of the Danger Theory based AIS intrusion detection algorithms called DCA to detect the resource consumption attack over MANET. DCA has been plugged into a new mobile intrusion detection and prevention architecture called MDCA architecture. MDCA has to be performed by each node in MANET to detect the attack locally without any need for mobile agents.

MDCA will be verified and tested by performing simulation experiments in the future work. However, in the future experiments csm fuzzy threshold should be determined in a good way which avoids the research to fall into high false positive rates. Also, MCAV thresholds should be determined in order to determine the context of the tested antigen if it is benign or malignant. Finally, more signals and antigens will be added to enhance the intrusion detection precision and decrease the possible false positive rates.

7 REFERENCES

1. 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).
2. Matzinger, P.: Tolerance, Danger, and the Extended Family. Annual Review of Immunology 12, 991–1045 (1994).
3. Greensmith, J., Aickelin, U., and Tedesco, G.: Information Fusion for Anomaly Detection with the Dendritic Cell Algorithm. Information Fusion. 11, 21--34. Elsevier (2010).
4. 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).
5. Kim, J., Bentley, P., Wallenta, C., Ahmed, M., and Hailes, 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).
6. 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).
7. Cayirci, E., and Rong, C.: Security in Wireless Ad Hoc and Sensor Networks.WILEY, United Kingdom (2009).
8. 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).
9. Perkins, C.E., Royer, and E.M.: Ad hoc On-Demand Distance Vector Routing.. In: Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100 (1999).
10. Taneja, S., and Kush, A.: A Survey of routing protocols in mobile ad hoc networks. In international journal of innovation management and technology. 1,279—285 (2010).
11. Nadeem, A. and Howarth, M.: Adaptive Intrusion Detection & Prevention of Denial of Service Attacks in MANETs. In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing, pp. 926—930. ACM, New York (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).