J. Modern Technology & Engineering
Vol.2, No.3, 2017, pp.231-248

DEFENCE AGAINST BLACK HOLE ATTACKS IN MOBILE AD HOC NETWORKS USING ARTIFICIAL IMMUNE SYSTEMS

Sh. Behzad[1*], R. Fotohi[1], Arzu M. Guliyev[3]

[1]Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran
[3]Azerbaijan State Pedagogical University, Baku, Azerbaijan

Abstract. Mobile Ad-hoc Networks (MANET), don't have the basic and classic network devices, such as routers or access points. In these networks data transfer among the nodes are realized by the collaboration among multiple hops that rather than just serving as a single terminal, act also as a router to establish a route. But, such networks are vulnerable to a type of routing misbehaviour, called black hole attack. In this attack, an attacker cheats nodes, absorbs their packets and then deletes them. Hence, black hole disrupts communication, or even makes it impossible in some cases. In this paper, we employ Artificial Immune System (AIS) to defend against the black hole attack in DSR-based MANETs. The proposed protocol, called AIS-DSR (Artificial Immune System DSR) employs AIS (Artificial Immune System) to defend against black hole attacks. AIS-DSR is evaluated through extensive simulations in the ns-2 environment. The results show that AIS-DSR outperforms other existing solutions in terms of throughput, end-to-end delay, packets loss ratio and packets drop ratio.

Keywords: *Mobile Ad Hoc Networks, DSR routing protocol, Black hole attack, Artificial Immune System.*

Corresponding Author: *Shahram Behzad, Department of Computer Engineering, Germi branch, Islamic Azad University, Germi, Iran, e-mail: Sh.behzad173@gmail.com*

Manuscript received: *6 September 2017*

1. Introduction

Mobile Ad Hoc networks do not have any access point to network accessibility. Wireless devices such as notebooks, laptop and cell phones connect to similar equipment and form an Ad Hoc network. Since nodes are not controlled by any central entity, they have unrestricted mobility and connectivity to others. Routing and network management are done by each other nodes, cooperatively. In other words, the nodes' communications are formed based on the cooperation and some trust among them. In these networks, each node works as a host as well as a router that forwards packets for other nodes. The most important property of these networks is their dynamic and variable topologies that are the result of the nodes' mobility [16, 18, 24].

Availability of the fresh routes is irrespective of checking its routing table. In the attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [17]. In the protocol based on flooding, the black hole node reply will be received by the requesting node before the reception of reply from actual node; hence a black hole and forged route is created. When this route is established, it's up to the node whether to drop

all the packets or forward it to the unknown address [24]. In addition, in black Hole, attacker nodes tend to advertise and spread fake routes, absorb network traffic towards their selves and drop packets. Figure 1.Shows an example of black hole attack.

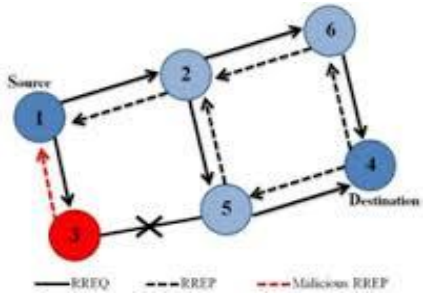

Figure 1. Problems of black hole attacks

basic concepts and preliminaries including DSR routing protocol, black hole attack and artificial immune system. We implement the proposed scheme over DSR routing protocol in ns-2 environment. Rest of this paper is organized as follows. In the second the related works are given. Section 3 brings Dynamic Source Routing (DSR) and its vulnerabilities.In section 4 the artificial immune system is illustrated and section 5 proposes a novel defense scheme based on AIS concepts. Simulation results and analysis can be found in section 6 and concluding remarks are given in section 7.

2. Related work

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalable. Despite the fact of popularity of MANET, these networks are very much exposed to attacks [16]. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [13]. Different kinds of attacks have been analyzed in MANET and their effect on the network. Attack such as gray hole, where the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [6]. MANETs routing protocols are also being exploited by the attackers in the form of flooding attack, which is done by the attacker either by using RREQ[1] or data flooding [17]. Design and presentation of different security obstacles and attacks in mobile ad hoc networks as well as finding appropriate solutions against them is a challenging research area for researchers. Black hole attack is one of the famous related attacks. In [7], black hole attack is evaluated in DSR based networks and a solution is proposed to mitigate it, as well. In such papers, fake routes are only suggested in response to RREQ packets. In [14], and [10] Black hole attack is assessed in DSR based networks and in [4], is considered

[1] Rout Request

in AODV based networks. In such works, fake RREP suggestions are just offered based upon received RREQs, too. Black hole attack operates in [25] in two different phases. It works by both propagating fake RREQs, and generating RREQ based false RREPs. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to separate. This malicious node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [8, 21]. This thesis focuses on the study the impact of black hole attack in MANET using both Reactive and Proactive protocols and to compare the vulnerability of both these protocols against the attack. Many approaches to detect the black hole attack and to defend the MANET from the attack have been proposed [12, 23]. According to the algorithm by Deng et al. [3], every node crosses check with its next hop node on the route to the destination on receiving or overhearing a RREP packet. If the next hop node does not have a link to the node that sent the RREP, then the node that sent the RREP is considered as malicious. This solution assumes that there exists at most one malicious node and thus cannot cover the case with two or more malicious nodes, which is quite possible in real situations. An algorithm presented in [26] claims to detect the black Hole attack in a MANET which is based on relationships of a trust level among the nodes. However, in the real network, it is very difficult to set an appropriate value for the trust level. In the method [26], every node has a function of learning the traffic flow in the network and evaluating the possibility criterion of black hole attack based on such learning results in order to detect the malicious node. If the value of the criterion is larger than a predetermined threshold, the node judges that there exists a black hole attacker. This method only provides detection of a single black hole attacker and cannot detect a chain ofmalicious nodes which cooperate with each other. The method [20] provides a data learning scheme to detect a black hole attacker. In this scheme, every node has knowledge of the current value of SN by the exchange of route messages such as RREQ and RREP. If a node receives a RREP message with a SN that is much larger than a threshold plus the current SN value, this node will believe that the RREP message is generated by a malicious node. Obviously, this method depends on the value of the threshold and may lead to a high rate of misjudgment. A. Bala proposes a trust based approach [5] using AODV [15] protocol. But they do not consider the data packets. Instead they consider only control packets like RREQ, RRER and RREP and network layer acknowledgement. A black hole can even drop data packets by perfectly transmitting control packets. There the system fails by thinking there is no black hole as the control packets are transmitted without any delayor drop. Satoshi has proposed a method [20] based on the number of RREQ messages sent and RREP messages received. It calculated the average sequence number and try to find out the malicious node, as the malicious node will send RREP messages with extremely higher sequence number. There are chances of getting RREP packet with highest sequence number from a genuine node too. S. Marti, et al in [3] on

the values from this watchdog, trust value on the neighbor is being increased or decreased dynamically. The method is implemented onlyon DSR protocol.

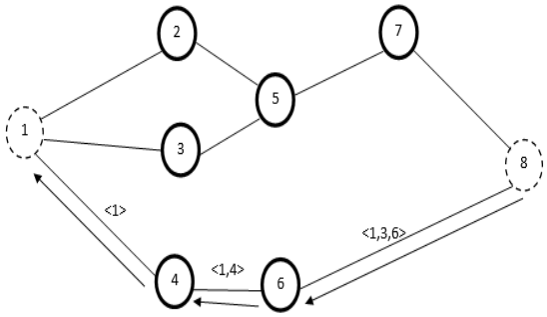

Figure 2. Depicts a discovery route in DSR protocol (All-over distribution)

3. Dynamic source routing (DSR) and its vulnerabilities

DSR protocol is a reactive routing algorithm designed for mobile Ad Hoc Network. The process of routing in DSR is composed of two main phases known as route discovery and route maintenance. Routing in DSR[2] is completely carried out in an on-demand method [18]. Route discovery phase is a process under which source node, in order to send data packets, obtains a valid route to the destination node. For this, source node creates a RREQ packet and relays it in the network. Such a packet will be received by all of the sources neighbor nodes. Each RREQ packet contains an identifier and a list of addresses of intermediate nodes which this packet has passed from them. Such a list is initially empty at the time of creating RREQ by the source node. When a node receives a RREQ packet, creates a RREP regarding information included in the list of addresses inside the packet and sends it back to the source node if only it be the destination node itself or have had a route to the destination. Once source node receives such a RREP packet, it first adds this route to its route cache and then starts to send data packets using the route included in the packet. If the receiver of RREQ has not had a route the destination and has not previously received this RREQ packet, appends its address to the list of nodes inside the packet and rebroadcasts that. When the destination node receives a RREQ[3], it can create and send back the RREP to the source node using the route which can be computed by inversing the list of addresses inside the RREQ packet. Route maintenance is a mechanism by which, as source node is using a route to send its data packets, can discover changes of topology and send remainder of its packets through an alternative route if it be convinced that the current route has been broken and not usable anymore [19].

[2] Dynamic Source Routing
[3] Route request

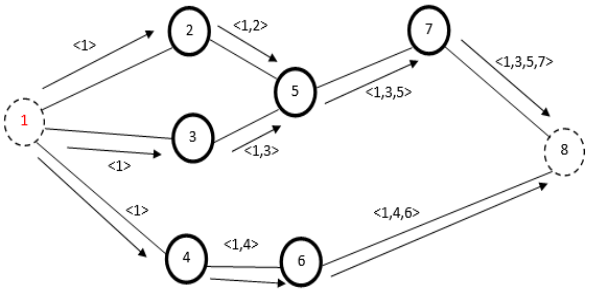

Figure 2-1. A sample of route discovery in DSR protocol

4. Artificial immune system over view

In this section we present the artificial immune system and explain principles we are going to use in this Paper We begin this section with presenting those characteristics of natural immune system which are a motivation for inspiration from and then we consider artificial immune algorithms the artificial immune system is a model for machine learning. The machine learning is a computer's ability to do a work by learning data or by experience. The artificial immune system is defined in this order: it is consisted of adaptive systems which have been emerged with an inspiration from theoretical immunology and functions, principles and observation immune models and would be used for solving problems [27].

DE Castro and Timmy's have chosen the above definition for AIS and specified three points individually which out to be taken into account in each artificial immune algorithm:

- In each individual artificial immune algorithm, should at least be an immune segment like lymphocyte.
- In each individual artificial immune algorithm, should be used idea which has been obtained from experimental or theoretical biology.
- The proposed artificial immune algorithm should be useful in the process of problem solving.

4.1. The artificial immune system: a model inspired by biology

In general, the artificial immune systems (AIS) are categorized on inspired algorithms from the biology. As the name would imply, these kinds of algorithms are computer based algorithms which their features and principles are the result of close examination in both adaptive characteristics 3 and the resistance of biological samples4. Samples of such algorithms arebrain-inspired neurotic networks, as well as artificial immune system which make use of principles and natural immune system processes to solve problems.

4.2. Immunity

In this section the immune principles would be insinuated in such a way that will facilitate understanding the rest of paper and we avoid giving excess details. This section is beginning with a short summery about intrinsic immune system. The intrinsic immune system has not been used extensively in artificial systems, however, due to assisting the performance of acquisitive immune system and

affecting it and also the usage of it in this Paper, having a short review regarding that seems necessary.

4.3. Intrinsic immunity

As the name would suggest, the intrinsic immune system would last not change over time and been adjusted for detecting a small number of common aggressors. The intrinsic immune system will diminish most of pathogens (which are the potential detrimental aggressors) at its first clash. The acquisitive immune system is in desperate needs of time to response against aggressors, so it is the intrinsic immune system responsibility to react against the aggressors immediately and bring the attack under its control so as to the acquisitive immune system could give an influential response [1, 2, 28].

4.4. The acquisitive immunity

When the intrinsic immunity is made active, its activity would last for several days while the time the acquisitive immunity is active, it would even endure for weeks. The acquisitive immunity is obliged to destroy the pathogens in case the intrinsic immunity has been defeated or is infeasible anyway. Inapplicability of the intrinsic immunity is due to its incapability to build a specific response for an aggressor pathogen; in this point it's the acquisitive immune system which takes the field. Unlike the intrinsic immunity, the acquisitive immunity is specific and has memory, according to figure 3, it can remember the pathogen which has attacked one time and system generated a response for it, therefore in future encounters it can respond quickly to oppose it.

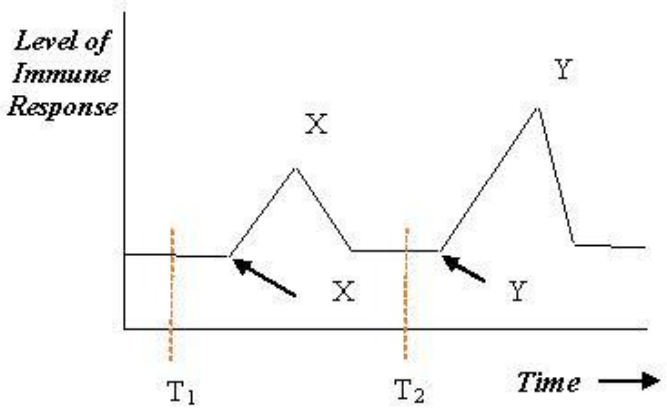

Figure 3. Primary and secondary immunity responses

Response of Y2 is stronger than X2. The first sign for existence of such unknown antigens in T1 produces X2 response. Nevertheless, notice the delay between T1 & X1. Nearly The same antigens been interred in the time of T2, almost immediately in produced response of Y1 for acquisitive system can be observed in vaccination experiments carried out by Jenner in 1970 [9].

4.5. B cell and antibodies and choosing colony

Like all immune cells, B cells are developed in bone marrow. A natural B cell contains 105 antibodies (receptor) on its surface. Each one of these antibodies has a unique shape that can be found in genetic structure of B cell and as a result they have a shape similar to B cell. Therefore all antibodies produced through a B cell are connected to a similar set of molecular models. According to figure 4, antibodies of B cell are dual- value and dual- performance. They are dual-value because of their capability for connecting to two antigens through two arms in Fab areas, and they are called dual- performance due to the fact that besides having the capability for connecting to antigen models using Fab areas, they can also be connected to certain receptors on surface of other immune cells using Fc portion [22].

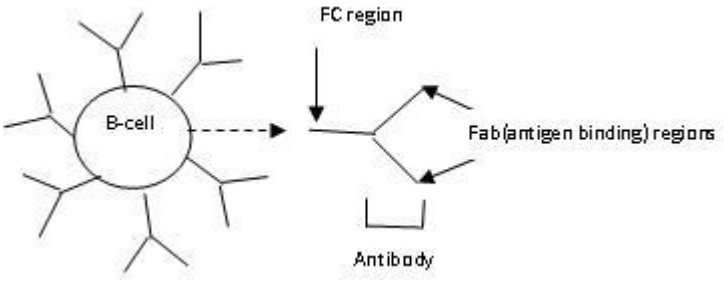

Figure 4. a diagram for B cell

There are copious antibodies on the surface of B Cell. In figure (4), an antibody (Ab), or an immunoglobulin (Ig), is consisted of two similar light chains (L) and also two similar heavy chains (H).

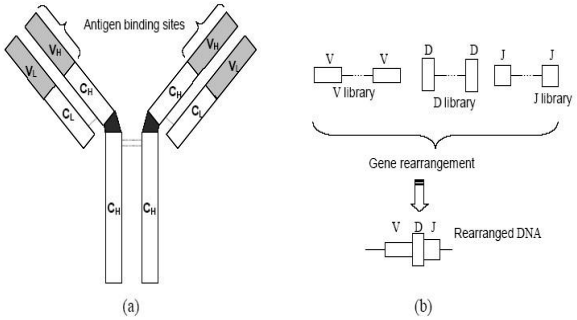

Figure 5. Antibody molecule and its genome

5. The proposed method

5.1. Over view of detection system

DSR routing protocol follows the basic, When RREQ process is sent, the node waits for RREP and once the RREPs come from the nodes, it responses to the first arrived RREP. The node sends packets with this RREP, which in turn leads to ignoring other REEPs. Such a process leads to ignoring the security or in security of the route, which in turn enhance the chance of malicious nodes (black

hole nodes) existence eliminating the transmitted packets. To avoid these types of attacks in the network, a method based on table and count hope, imitating the artificial immune system, is used. Through this process, we demand for a route and wait for the node response totransmit the packets. Once a large number of RREPs are received in a successive time period from a node, the packets are not transmitted with this RREP. Rather, information of the given node is recordedin a table and, to evaluate the immunity of the route, the hop counts transmitted by RREP are also analyzed. In the case RREP hop counts are less, for instance there exists a node with high RREPs and also less hop counts, the given node is labeled as suspicious in the table and its information is broadcasted to the neighboring nodes , that node is eliminated from operation cycle.

5.2. Proposed Method

Attacks of black holes have innumerable impacts on causing weakness in routıng and number of received packets to the destination and this leads to the rapid diminution of network's efficiency, and the number of dropped packets would increase and have a significant effect on other criteria in the network, such as operational potency, packet delivery rate, end to end delay and packet loss. Hence, to defense against the black hole attacks in mobıle ad hoc network, the artificial immune system of the body were inspired details and details of the proposed system are briefly described in the next section.

5.3. Exact correlation between human body and Mobile Ad Hoc network

The artificial immune system is a strong and complex system which protects human body against foreign factors. This system is also capable to identify and categorize cells in two groups, self and non self. In this paper for detection committed attack by black holes in mobile ad hoc networks we inspired by artificial immune system and regard conditions for limiting black holes attacks as (the RREP and repeat step) antibody and assume (the existing routes to destination) as antigen. We also consider mutation as the first delivered response to the source node, and then based on work situations in comparison stage, separate safe and other routes from that of unsafe.

5.4. Details of the proposed method for the defence against of black hole attacks

When requesting node in the routing path to the destination node, for sending the data packets, are fast the black hole attack in response to it’s a short path. Therefore a false route consist of the black hole node, forms And the normal route is longer and has a number of additional steps are deleted. Thus, the source node of the packet to the node sends a black hole. And node Blackholes could be deleted or altered to defense this Attacks) black hole (in the network, we approach the table and the number of hop count, Inspired by the artificial immune system was used. When the route's request is done, and RREQ is broadcasted to find the route, it waits to receive a response from all neighboring nods to send packets from this route. When the receives larger RREPs from an of a node in a sequential time period, ın the first stage it would not send packets to the destination with this

received RREPBut Its node table information and records for the safe path, the path is where malicious node or not the black hole.The number of hops sent by that specific RREP node should be compared too. If the hop number of Received RREPs many have hops lower, for an example a node sending excessive RREPs and having lower hops – we would identify that node as a suspicious node and black hole and mark it in the table and broadcast its information as black hole node to neighbors and then don't let that node participate in the navigation and so it would be removed from the operation cycle, as in Figure 6.

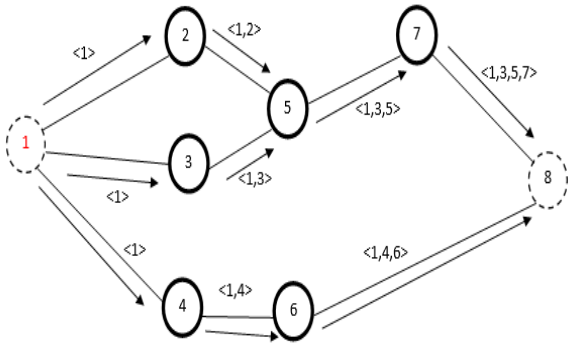

Figure 6. DSR Route Request (RREQ)

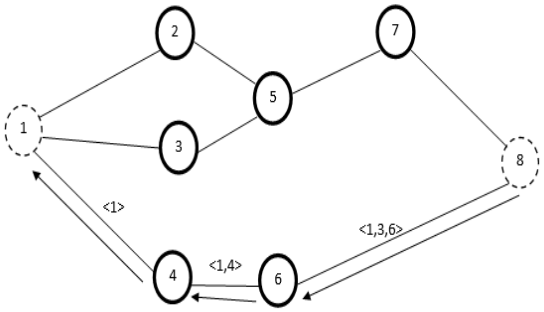

Figure 7. DSR Route Reply (RREP)

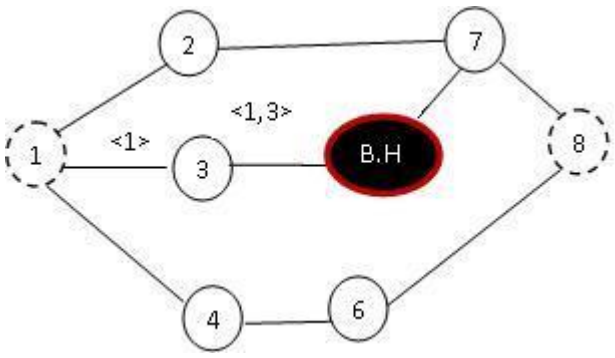

Figure 8. Single Black hole attack in DSR

The proposed system is composed of various stages: generating a population from antibodies, antigens, rejection, match, Save in the detector set, Hyper mutation of the detectors and Save in the immune memory.

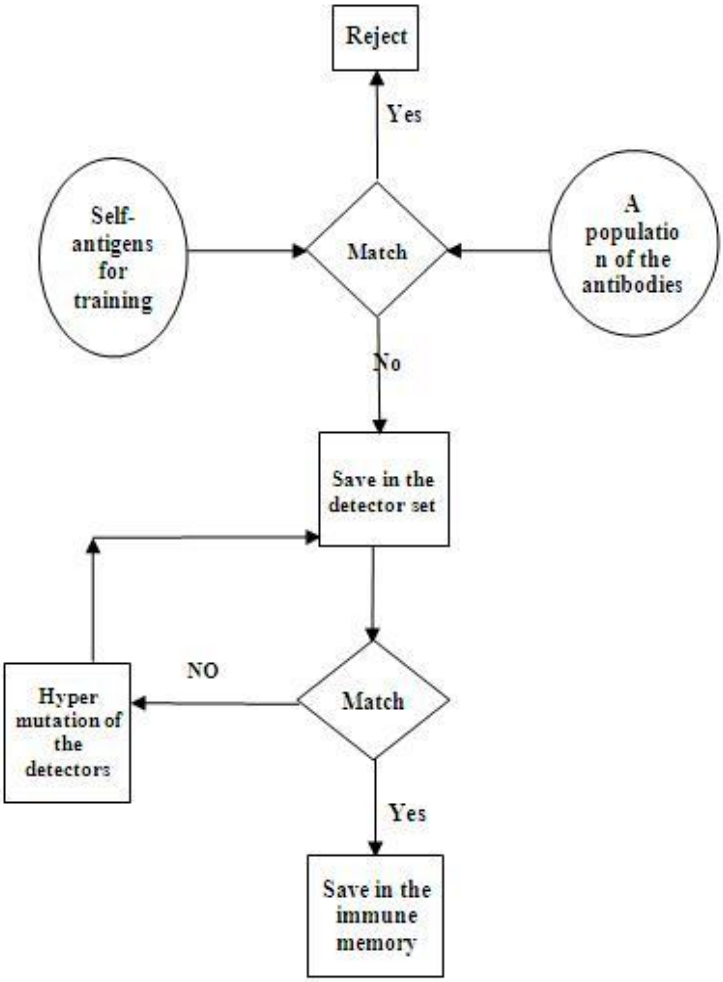

Figure 9. The flowchart of the proposed method.

Step 1. Population of antibodies) to cope with attacker features (at this stage All RREP are collected in the table with the features mentioned, i.e "RREP is of the highest repeating, and lower hop countAnd compare those with the features that interest RREP adapted to the RREP path to better evaluation to stepNext, the "complete set of detector" and we'll send you anAdaptive characteristics the applied not reject.

Step 2. Antigen population (All existing routes)
We consider the whole existing routes between the origin and destination loops as antigen. The algorithm in figure 10, instructs antibodies in comparison to relative elements and we would choose that antibody not being in accordance with relative elements.

```
1:   input  : S = set of patterns to be recognised, n the number of worst
     elements to select for removal
2:   output : M = set of memory detectors capable of classifying unseen
patterns

3:   begin
4:     Create an initial random set of antibodies, A
5:     forall patterns in S  do
6:       Determine the affinity with each antibody in A
7:       Generate clones of a subset of the antibodies in A  with the highest
affinity.
8:       The number of clones for an antibody is proportional to its affinity
9:       Mutate attributes of these clones to the set A , and place a copy of the
highest
affinity antibodies in A  into the memory set, M
11:      Replace the n lowest affinity antibodies in A with new randomly
generated antibodies
12:    end
13:  end
```

Figure 10. The identifier learning algorithm

Step 3. Match

At this stage after choosing all those appropriate RREPs which have been achieved in collating with imposed conditions, we store them in RREPs table, according to Figure 10. For instance, there is four routes in the RREPs table and they been assessed based on the mechanism, to do so we send a test packet to each one of these routes, if the ACK response didn't arrive from a route, we would add 20 units to Pm variable but if the ACK response arrives, we detract 50 units from Pm variable. In the course of time, if the Pm value exceeds 50, we remove that route otherwise we enter that route into next stages. Pm means the possibility of aggressiveness for a route.

Input: Pm for all routes

Output: An best immune route

Begin

R = number of routes

For r = 1 To R

If Pm > 0.5 Then reject

Else

$$F_r(\text{HOPCount, ITR}) = \frac{hop\ count}{Max\ hop\ count} + \frac{\max Iteration\ nod\ rrep}{Iteration\ Node\ RREP}$$

Select the route with maximum ROUTE i = (1 - Pm) * Fr (HOP COUNT ,ITR RREP)

End

Figure 11. The algorithm of choosing the best route

According to figure 11, Fr function is calculated for each individual i route and the route which has the greatest number is selected as the best route.

Step 4. Save to complete the detector
At this stage those amounts of RREPs which could be collated with imposed conditions are collected and sent to next stage which is the Match stage, i.e. they have the two specified characteristics.

Step 5. Match
between collative RREPs of the first stage, that RREP is chose as the best and securest RREP which has a higher FR amount.

Step 6. Mutation
only those sets of RREPs having the same characteristics
regarding step numbers and frequency are prioritized, the first reached RREP to the origin loop has the highest priority and returns back to the adding stage "identifier completion".

Step 7. Storingas the best identifier in the memory
Only those sets of RREPs are selected and registered in the immune memory as the best and safest RREPs which passed the imposed conditions in the beginning stages.

6. Simulation results and analysis

This section includes simulation and evaluation of Accurate Black hole attack, compared with artificial immune system. We compared the performance of DSR and DSR routing protocols with black hole attack against the performance of the routing protocols without Black hole attacks. With the help of the Network simulator ns-2 we were able to prove, ns is simulator project, Start 1989 as a variant of REAL (network simulator for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks). we run two simulation, one DSR under attacker node and other including the Defense Against Black hole Attacks ,we have repeated the experiments by changing the Several times. To, 100,120,140,160,180, And 200 to see the simulation parameter are show in table 1 the metrics used to evaluate the performance are given below.

6.1. Packet delivery ratio (%)

PDR is the number of packages that are delivered to the destination from the source, divided by the total number of packages in the network. This parameter is also called as success rate of the protocols:

PDR = (Number of seed Packet / Number of received Packet)* 100

Where PDR is the package delivery rate, Send Packet No is the number of sent packages, and Receive Packet No denotes the number of received packages.

Table 1. Simulation parameters

Simulator	**NS2.34**
Area	500m X500m
Number OF Mobile Node	50
Routing Protocol	(DSR)
Transmission Range	250m
Antenna	Omni Antenna
Simulation duration	100,120,140,160,180,200
MAC Layer	802_11
Traffic Type	CBR(UDP)
Buffer Size	50 Packet
Node placement	Random
Black hole Node	3 And 6 node

6.2. Packet loos (%)

Packet loss can be caused by a number of factors including attacker over the network medium due to multi-path fading, packet drop because of channel congestion, corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers, or normal routing routines (among DSR in mobile ad hoc networks),Packet loss can be caused by the black hole attack

Packet loss= (Send Packet - Received Packet)/Send Packet

6.3. End To End Delay

End-to-end delay refers to the time taken for a packet to be transmitted Around the Network from source to destination.

6.4. Throughput

A network can be measured by using the different tools that are available on the different operating systems. This page explains the theory, on which the adjustments of these tools for measurements are based, and the issues related to these measurements. The reason for measurement of the throughput in networks is that, the people often intend to know about the maximum operational power of data in a connection link or network access as expressed by the unit of bit per second. The measurement of this quantity is commonly carried out by transmitting a large size file from one system to another and calculating the required time for complete transmitting or copy of the file. Then, with dividing the file size by that

time, the throughput will be achieved in unit of megabit per second, kilobit per second or bit per second. The following formula shows how to calculate the throughput: [5]

$$X = C / T \quad (1)$$

where X is the throughput, C is the number of requests that are accomplished by the system, and T denotes the total time of system observation.

Packet Drop

In wireless mobile ad hoc network, a packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes, because, the packets are routinely dropped from the loss network.

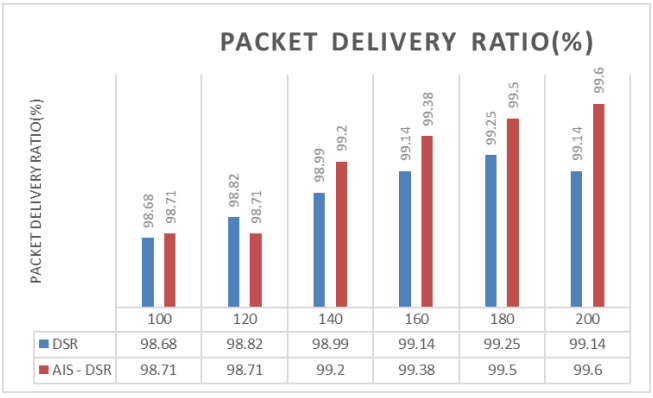

Figure12. PDR DSR under attack aand proposed method (AIS-DSR) Vs. Time

Figure 12 shows the packet delivery ratio of proposed method (AIS-DSR) at the different time Than the DSR under attack is better, the package delivery rate at the time of 140 to 200, is better because proposed method is well trained

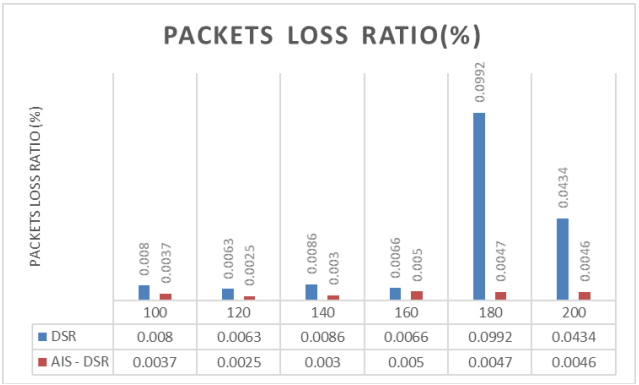

Figure 13. Packet loss DSR under attack and proposed method (AIS-DSR) VS Time

Figure 13 shows the packet loss ratio of proposed method (AIS-DSR) at the different time Than the DSR under attack is better, the package delivery rate at the time of 120 to 200, is better because proposed method is well trained. This result reflects that our detection method is valid for defense against black hole attack at different times.

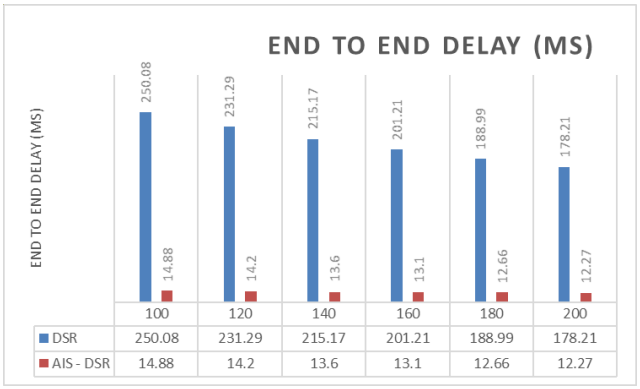

Figure 14. End to End Delay DSR under attack and proposed method (AIS-DSR) VS Time

Figure 14 shows that end-to-end delay is DSR under attack considerably higher, compared to the proposed method. This result reflects that our detection method is valid for defence against black hole attack at different times.

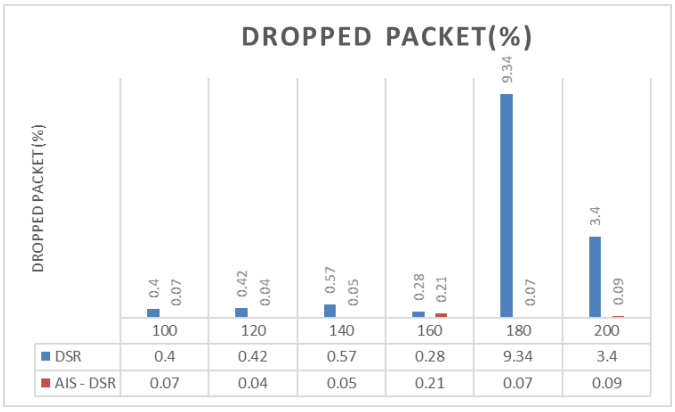

Figure 15. Dropped Packet DSR under attack and proposed method (AIS-DSR) VS Time

Figure 15 show that black hole has dramatically the drop packet, ratio compared to proposed method; show that in DSR under attack higher drop packet at different time. This proposes method (AIS-DSR) result reflects that our detection is valid for Defense against black hole attack at different times.

Figure 16 for 100 to 200 time, it is obvious that the throughput for propose method (AIS-DSR) is high compared to that of DSR under attack. As throughput is the ratio of the total data received from source to the time it takes till the receiver receives the last packet. The overall low throughput of DSR under attack is due to route reply. The black hole node immediately sends its RREP and the data is sent to the black hole node which cast off all the data. The network

throughput is much lower. This result reflects that propose method (AIS-DSR) our detection is valid for Defense against black hole attack.

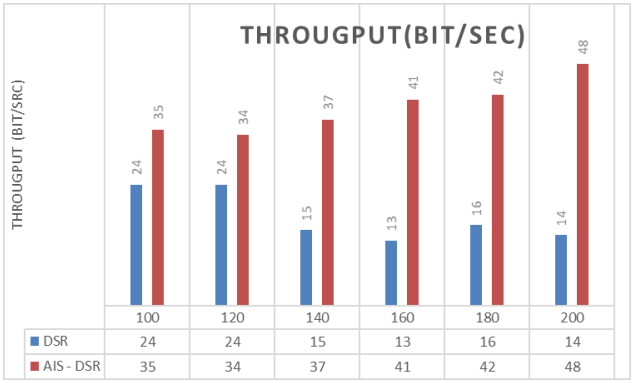

Figure 16. Throughput DSR under attack and proposed method (AIS-DSR) VS Time

7. Conclusion

Nowadays there are a lot of studies concerning defense against black holes attacks in occasionally portable networks MANT. Mobility of loops in this kind of network and not participation of some loops in navigation or destructiveness of loops in this kind of networks makes the network to face difficulties. In this Paper we used the artificial immune system or AIS to defense against the black holes attacks. In the proposed method for the first step the origin loop analyzes the step numbers and the arrived RREPs from each loop and with its strong learning modifies the route immediately and separates black hole loops from other existing loops in occasional networks and then chooses the best route among the current routes and conveys packets from an intact route and without black hole to the destination loop. The obtained results from the simulation of the proposed method in attack conditions show that the offered method AIS-DSR to some extent has a better performance against black hole attacks and has good results in respect of packet delivery, operational potency, end to end delay and number of omitted packets.

References

1. Aickelin U., Bentley P., (2003) Danger Theory: The Link between AIS and IDS, 2nd International Conference on Artificial Immune Systems,147-155.
2. Aickelin U., Cayzer S., (2002) The Danger Theory and Its Application to Artificial Immune Systems, 1st International Conference on Artificial Immune Systems, 141-148.
3. AI-Shurrnan M., Yoo S.M., Park S., (2004) Black Hole Attack in Mobile Ad Hoc Network, ACMSE' 04.
4. Bala A., Bansal M., Singh J., (2009) Performance Analysis of MANET under Blackhole Attack, First International Conference on Networks & Communications, India, 141-146.

5. Behzad Sh, Fotohi R., Jamali S.,(2013) Improvement over the OLSR Routing Protocol in Mobile Ad Hoc Networks by Eliminating the Unnecessary Loops, *International Journal of Information Technology and Computer Science (IJITCS)*, 5(6), 16.
6. Behzad Sh., Dadgar F., (2015) A hybrid method for detection and removal black hole attacks in mobile Ad-Hoc Networks, *Journal of Modern Technology and Engineering*, 2(1), 66-75.
7. Behzad Sh., Fotohi R., Effatparvar M., (2013) Queue based job scheduling algorithm for cloud computing , *International Research Journal of Applied and Basic Sciences*, 4(11), 3785-3790.
8. Biswas K., Ali M., (2007) Security threats in Mobile Ad-Hoc Network, Master Thesis, Blekinge Institute of Technology, Sweden, 22nd March.
9. Burnett F., (1959) The Clonal Selection Theory of Acquired Immunity, Cambridge University Press, 32-41.
10. Cai J., Yi P., Tian Y. et.al, (2009) The Simulation and Comparison of Routing Attacks on DSR Protocol, Proc. Int. Conf. on Wireless Communications, Networking and Mobile Computing, WiCom '09, China, 1-4.
11. Dadgar Arablu F., Guliyev A.M., (2017) Modeling and simulation for performance evaluation of models of queuing service systems with limited and unlimited buffer in distributed networks, *Journal of Modern Technology and Engineering*, 2(1), 90-105.
12. Deng H., Li W., Agrawal D.P., (2002) Routing security in wireless ad hoc network, *IEEE Communications Magazine*, 70- 75.
13. Elhoseny M., Farouk A., Zhou N. et al., (2017) Dynamic Multi-hop Clustering in a Wireless Sensor Network: Performance Improvement, *Wireless Personal Communications*, Springer US, 95, 4, 3733-3753 (DOI 10.1007/s11277-017-4023-8).
14. Fadlullah Z.M., Taleb T., Vasilakos A.V. et al., (2010) DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis, *IEEE/ACM Transactions on Networking (TON)*, 18(4), 1234-1247.
15. Fotohi R., Jamali S, Sarkohaki F., Behzad Sh., (2013) An Improvement over AODV Routing Protocol by Limiting Visited Hop Count, *IJITCS*, 5(9), 87-93, DOI: 10.5815/ijitcs.2013.09.09
16. Fotohi R., Ebazadeh Y., Geshlag M.S., (2016) A New Approach for Improvement Security against DoS Attacks in Vehicular Ad-hoc Network, *International Journal of Advanced Computer Science and Applications*, 7, 10-16.
17. Jamali S., Behzad Sh., (2015) A survey over black hole attack detection in mobile ad hoc network, *International Journal of Computer Science and Network Security (IJCSNS)* 15(3), 44.
18. Jamali S., Fotohi, R., (2016) Defending against Wormhole Attack in MANET Using an Artificial Immune System, *New Review of Information Networking*, 21(2), 79-100.
19. Johnson D., Hu Y., Maltz D., (2007) The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, RFC 4728.
20. Kurosawa S., Nakayama H., Kato N. et al,(2007)"Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Network by Dynamic Learning Method", *International Journal of Network Security*, 5, 338-346.
21. Pegueno G.A., Rivera J.R., (2006) Extension to MAC 802.11 for performance Improvement in MANET, Karlstads University, Sweden.

22. Reichardt P, Gunzer M., (2006) The Biophysics of T Lymphocyte Activation In Vitro and In Vivo, In Cell Communication in Nervous and Immune System, 199-218.
23. Rubin I., Behzad A., Zhang R. et al.,(2002) A mobile-backbone protocol for ad hoc wireless networks , In Proceedings of IEEE Aerospace Conference, 6, 2727-2740.
24. Sarkohaki F., Fotohi R., Ashrafian V., (2017) An Efficient Routing Protocol in Mobile Ad-hoc Networks by using Artificial Immune System, *International Journal of Advanced Computer Science and Applications (IJACSA)*, 8(4). http://dx.doi.org/10.14569/IJACSA.2017.080473.
25. Sharma Sh., Gupta R., (2009) Simulation study of Blackhole attack in the mobile ad hoc networks, *Journal of Engineering Science and Technology*, 4(2), 243-250,
26. Tamilselvan L., Sankaranarayanan V., (2007) Prevention of Black Hole Attack inMANEr", The 2nd international Conference on wireless, Broadband and Ultra Wideband Communications.
27. Timmis J., (2000) Artificial immune systems: a novel data analysis technique inspired by the immune network theory, Doctoral dissertation, Department of Computer Science, 21-30.
28. Twycross J, Aickelin U., (2005) Towards a Conceptual Framework for Innate Immunity", 4th International Conference on Artificial Immune Systems, 112-125.