Egyptian Computer Science Journal (ISSN-1110-2586)
Volume 41– Issue 1, January 2017

Solution for Black Hole and Cooperative Black Hole Attacks in Mobile Ad Hoc Networks

Khaled O.Basulaim, Shada Ali Aman
Department of Information Technology
Faculty of Engineering, University of Aden
khaled.basulaim@gmail.com, shadamit1@gmail.com

Abstract

Mobile ad hoc networks are formed by mobile nodes that communicate with each other through wireless medium. Packets are forwarded by intermediate nodes from source to destination node. Without having security mechanism, an intermediate node can behave maliciously to drop the packets going through it instead of forwarding them to the neighbor node. The main goal of this paper is to investigate the effect of single and cooperative black hole attack in AODV routing protocol in MANET and proposing a solution based on one-way hash chain to cope with black hole attack launched in a single or cooperative manner. Through simulation, the effect of black hole attack will be showed. Also, it is to accentuate the performance of the approach we propose in AODV routing protocol in terms of throughput, end-to-end delay and network load; and evaluating its efficiency. The obtained results show that the throughput of our proposed solution with single black hole attack is improved to 96.43 Kbps while in Cesar Cipher approach it was 88.14 Kbps, the average end-to-end delay of our proposed solution with single black hole attack is improved to 0.012 sec while in Merkle Tree approach with single black hole attack it was 0.13 sec and the average end-to-end delay of our proposed solution with cooperative black hole attack is improved to 0.0085 sec while in Merkle Tree approach with cooperative black hole attack it was 0.07 sec.

Keywords: *Mobile Ad Hoc Network, AODV routing protocol, Black Hole Attack, hash chain mechanism*.

1. Introduction

Mobile ad hoc networks, named also MANETs, are formed by devices (nodes) that communicate with each other through wireless physical medium without having to resort to preexisting network infrastructure. Nodes consist of some ordinary devices such as mobile phone, laptop, PDA and personal computer that are participating in the network and are moveable. These nodes can operate as host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network [1]. MANET have dynamic topology such that nodes can easily join or leave the network at any time. MANET have a large number of potential applications. Military uses such as connecting soldiers or other military units to each other on battlefields or establishing a new network in place of a network, which collapsed after a disaster like an earthquake. MANET is especially useful when conducting emergency and rescue operations [2].

MANET have special features such as open communication medium, changing network topology dynamically, cooperative algorithm and lack of central monitoring and management while these features make MANET more flexible; they make it vulnerable to various types of attacks [3]. AODV is an efficient reactive routing protocol used in MANET, which may be influenced by black hole attack, in which a malicious node sends a fake RREP message as it has a fresh and shortest route to destination node. Then, source node uses this route and sends the data packets to it. Black hole node drops all the data packets going to it instead of forwarding them to the following node [4,5].When multiple black hole nodes act in coordination with same aim of dropping or absorbing the packets these are known as cooperative black hole attack. To struggle against single and cooperative black hole attack, we propose a solution based on one-way hash chain in order to check the correct forwarding of packets by intermediate nodes, the RREQ and the RREP packets that holds the hop count and sequence number are protected by hash chain mechanism. One-way hash chain mechanism provide light calculations compared to other cryptographic techniques like the encryption methods. It also provide a fast and secure way as they do not involve heavy computations and hence are useful to be implemented in mobile ad hoc network for message integrity checks.

Through simulation using OPNET simulator, we show the effect of single and cooperative black hole attacks on AODV routing protocol and evaluate the performance of our approach in terms of throughput, end-to-end delay and network load. In addition, we compare the approach we propose with the Cesar Cipher [6] and the Merkle Tree approaches in terms of throughput and end-to-end delay [7].

The remainder of this paper is organized as follows: Section 2 summarizes the related works. Section 3describes how single and cooperative black hole attack are launched in AODV. Section 4 presents our proposed approach. Section 5 analyzes and discusses simulation results. Finally, Section 6 describes the conclusion and future work.

2. Related Works

The black hole attack causes a serious damage to mobile ad hoc network. Some research works were done for evaluating and defeating the negative effect of both single black hole attacks and cooperative black hole attacks.

Ibrahim and his research group, proposed a cryptography mechanism based on Cesar Cipher with pre-shared key of 3 to avoid single black hole attack. The RREQ message at the source node is encrypted before forwarding to the neighbors, Nodes, which know the pre-shared key can decrypt the RREQ correctly and generate the RREP message and send it to the source node. Therefore, the Black Hole node can't decrypt RREQ message [6].

Baadache and Belmehdi, have proposed a cryptography solution based on the principle of Merkle Tree, which checks for correct forwarding of packets by intermediate nodes, and hence avoiding the single black hole and cooperative black hole attacks [7].

Nishant Sitapara et.al, presented an intrusion detection system for AODV protocol (IDSAODV) for single Black Hole attack. They used an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals assuming that the first RREP message arrived from the black hole node [8].

While Raj and Swadas, proposed a solution in which the receiving node of RREP message compares the sequence number value with a dynamic updated threshold. If the sequence number value is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list [9].

Tarek and his team proposed an Intrusion Avoidance System for AODV(IASAODV), to detect and avoid the black hole node. Here, the source node must wait a time equals the double value of RREP-Wait-Time before sending any data. When the timer RREP_WAIT_TIME expires, it then checks the number of RREP arrives. If the sequence number of RREP is greater than the maximum sequence number value then it will be considered as black hole node and it will be inserted into black list table [10].

Lalit and his assistants have proposed a method to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of source node and intermediate node who has sent back first RREP or not. If more difference sexist between them, surely it is from the malicious node, and it will remove that entry from the RR-Table [11].

Deng et al. propose a routing security protocol where intermediate node sends back to the source node its next hop information with reply to check that the next hop has a link with the intermediate node, the source node sends a further request packet to the next hop. The next hop should send back a further reply message, which include the check result. If the next hop ensures that the intermediate node exists, the source start to establish a route to the destination through this intermediate node [12].

A cooperative black hole attack is defined when several malicious nodes work together as a group. To identify multiple black hole nodes acting in cooperation, Weerasinghe and Fu proposed slightly modified AODV protocol by introducing Data Routing Information (DRI) table that contains information on routing data packet from/through the node and cross checking process that determines the reliable nodes to discover secure paths from source to destination [13].

3. AODV and Black Hole Attack Model

Here, the AODV routing protocol will be described. Also, it is to discuss how a black hole attack can be launched in single or cooperative manner when using it.

3.1 AODV Routing Protocol

Ad hoc On-Demand Distance Vector AODV [4]is one of the best and popular routing protocols that used in MANET, it establishes route only on demand. In AODV when source node has to send data to destination node, but it doesn't have a valid route to it, it broadcasts a RREQ message containing information: source IP address, source sequence number, destination IP address, destination sequence number, hop count and broadcast ID. The neighbor nodes to the source node update their routing table accordingly and broadcast the RREQ. This process is repeated until the RREQ reach the destination node. The destination node uses the pre-establish reverse route to send back the RREP to the source node. It should be noted that source node can receive several RREPs, it chooses the one with highest sequence number for the intended destination. If several RREPs with the same highest sequence number for the same destination are received by the source node from more than one node, then the one with smaller hop count will be selected.

3.2 Single Black Hole Attack in AODV

The single black hole takes place when the malicious node acts separately to carry out its attack. First, the malicious node violates the routing protocol specification to advertise itself as having a valid and shortest route to a destination node. Then, it drops the intercepted packets without forwarding them. In order to explain this attack, we will summarize how the single black hole is conducted in AODV routing protocol.

1. When malicious node receives RREQ packet, it takes information about the destination address and it prepares RREP in which the destination address is set to the spoofed destination address, the sequence number is set to highest value and the hop count is set to smallest value.
2. The black hole node sends the RREP to the closest intermediate node that belong to the active route.
3. When RREP received by intermediate node, it will be forwarded through the reverse path towards the source node.
4. The source node receives the RREP, it will update its routing table according to the information in RREP packet and uses this new route to send data packets.
5. Black hole node drops all the data packets that passes through it.

Figure1 illustrates single black hole attack, when black hole node B receives the RREQ sent by source node S, it sends back to A "RREP" which contains a spoofed destination address with a relatively greater sequence number and a smaller hop count. A forwards this "RREP" to S and the source node S updates its routing table accordingly. The new route (S, A, B) will be used by S to send data packets, and when intercepted by B, these data packets will be dropped. Nodes S and D will not be able to communicate in the presence of the black hole node anymore.

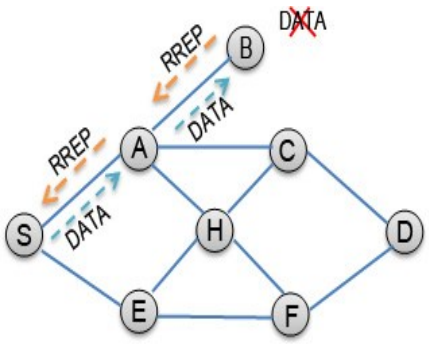

Figure1.Single black hole attack

3.3 Cooperative Black Hole Attack in AODV

In cooperative black hole attack, there are more than one black hole nodes working in group to violate the routing protocol specification or the implemented security mechanism. In order to explain this attack, the following paragraph describes the situation when multiple black hole nodes act in coordination to breach the security mechanism proposed by Deng et.al.[12] to identify single black hole attack. In Figure2, node B1 and B2 are working in group. Node B1 refers to B2 as its next hop. In the security mechanism proposed in [12], the

source node sends further request (FReq) to B2 through different route(S, E, F, B2) other than via B1. Node S asks B2if it is the next hop to B1 and if it has a valid route to the destination D.

B2 and B1 are working in coordination so the answer will be yes and with further Reply (FRep). Now, S starts sending data packets assuming that (S, B1, B2) is secure route but data packets are finally dropped by black hole node B1.

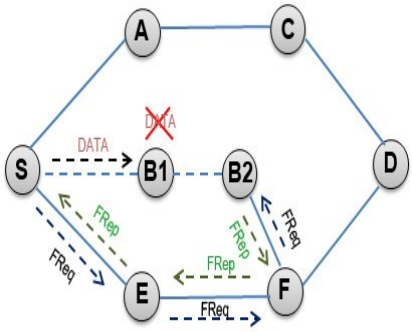

Figure2. Cooperative black hole attack

4. Proposed Solution

Here, the network assumption and details of our security approach against single and cooperative black hole attack will be explained.

4.1 Assumptions

We assume that wireless links are bidirectional i.e., if node S wants to transmit packets to node D, then node D is able to transmit packets to node S.

The destination node can only send RREP (route reply packet) and restricting intermediate node for the purpose.

4.2 Overview of the Proposed Solution

The AODV routing protocol has no security mechanism against malicious attack such as black hole attack where an attacker node absorbs all the packets to itself. In this paper, we propose a mechanism (solution) to struggle against black hole attack based on one-way hash chain. Black hole attack is based on the alteration on sequence number and hop count. We add additional field to the AODV routing protocol for RREQ packet we add the field HASHAODVRREQ and the same as for RREP packet we add the field HASHAODVRREP.

AODVRREQ	HASHAODVRREQ

So, each time a node receives RREQ packet or RREP packet it will check an additional field to verify the sequence number and hop count.

The one-way hash chain is a series of data generated from one-way hash function, which is easy to compute in one way while infeasible to do in reverse. Where $H^N(x)$ = H(H(….H(x)….)) and H is hash function.

Whenever a source node S wants to send data to destination node D, it initiates the route discovery process by sending new RREQ packet, which is:

AODVRREQ	HASHAODVRREQ

Where, AODVRREQ is the normal AODV RREQ and HASHAODVRREQ is the additional field that we add to the existing AODV RREQ. Source node S chooses maximum hop count MH based on the expected diameter of the network, then it generates a one-way hash chain:h_0,h_1,h_2,h_3,…,h_{MH} .

Source node in RREQ packets only can generate hash chain and intermediate node will verify the hash value and add the new hash value as will be explained.

A one-way hash chain is formed by applying the following actions:

- The source node selects random number X as a seed, which is generated by random number generator function.
- Then, the source node S set the initial value of hash by X,

$$\text{Hash} = h(X) \longrightarrow \tag{4.1}$$

Where h(') is a well-known one-way hash function and h_i = H(h_i – 1).

- Then, the source node S calculates the hash of x specific exactly r * v times,

$$h^{r*v}(X) \longrightarrow \tag{4.2}$$

Where h^{r*v}(X) means calculate hash of Xr * v times (r = MH) and v = n – u where n is the number that should be higher than max destination sequence number [14, 15] and u is the value of the destination sequence number.

So, source node S generates the hash of X using formula(1) and places its value in the HASHAODVRREQ field. Each time an intermediate node receives the RREQ, it verifies the validation of the hash value by calculating formula(3), which is the criterion formula:

$$h^{(MH-HC)*\,v}(\text{Hash}) \longrightarrow \tag{4.3}$$

(where MH = maximum hop count and HC = the current hop count value, i.e. HC = 0 for S) and compare the result value that must equal to the value contained in formula(2) if it is equal to the value in formula(2) an intermediate node will accept the routing packet and it will be forwarded to the next neighbor node. Otherwise, it will discard the packet. Then, intermediate node increments the hop count value by one in AODV RREQ header and calculate new hash chain value by hashing the previous hash value so that compute the hash of HASHAODVRREQ and places the new value in HASHAODVRREQ field before rebroadcasting the RREQ message to its neighbors. Process by intermediate node for handling the RREQ packet is illustrated in Figure 3.

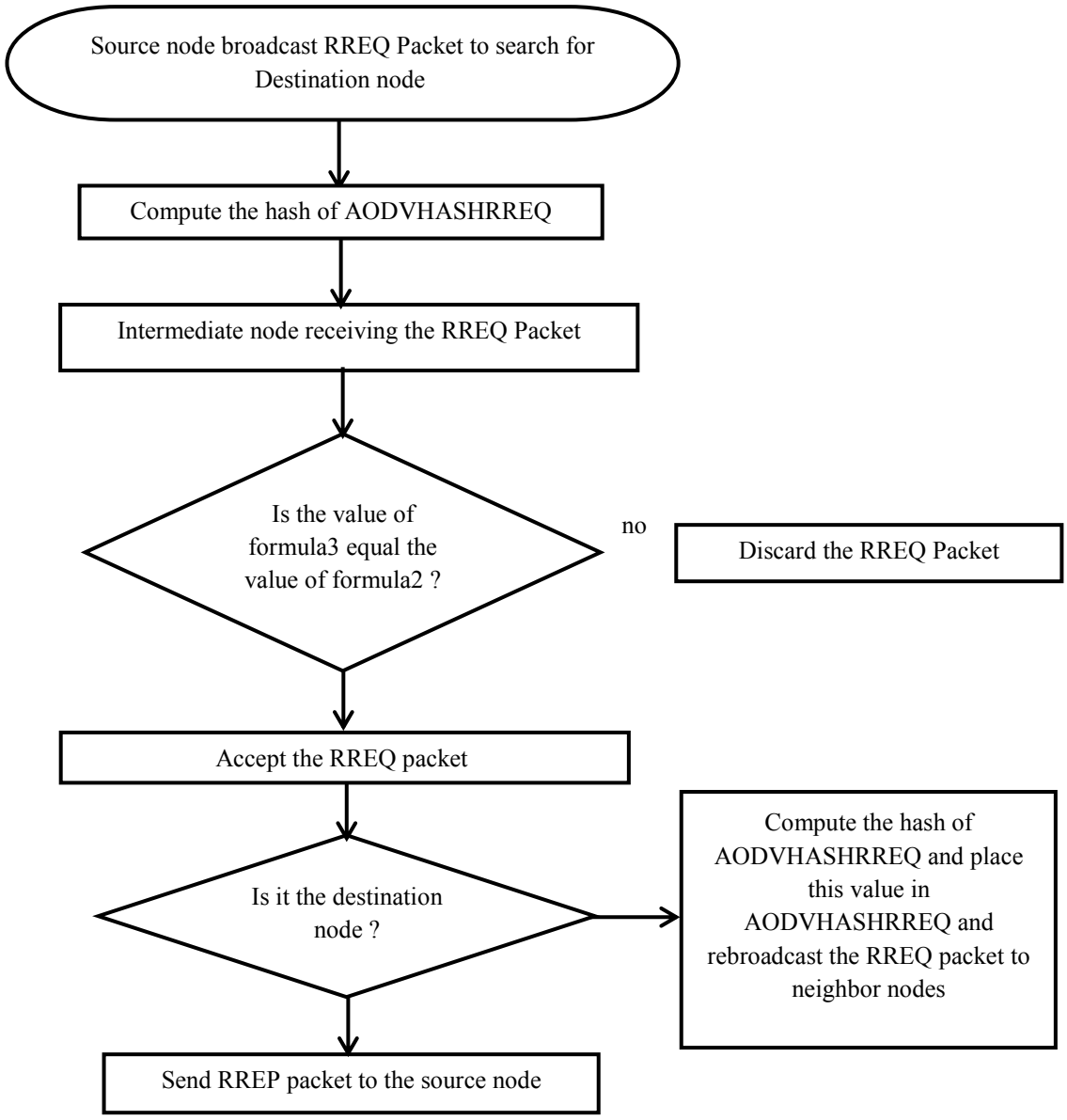

Figure3.Process at Intermediate node when it receives RREQ Packet

Similarly; for RREP, when destination node wants to send RREP packet, it does the same previous operation but it computes hash chain value in accordance with its own seed. Destination node puts the value of the hash in HASHAODVRREP.

- The new RREP will be :

AODVRREP	HASHAODVRREP

Process by intermediate node for handling the RREP packet is illustrated in figure 4.

Obviously, it is impossible to conduct single black hole attack if our proposed solution is used because black hole node should calculate the hash value in reverse (lower) order (i.e. in figure 1, node E must generate hash value in lower order which is impossible). In this way black hole node is not able to modify a route to some destination node with increasing in sequence number and lower hop count.

Also, it is impossible to conduct cooperative black hole attack i.e. in Figure 2, nodes E and F can cooperate to conduct cooperative black hole attack, this done if node E sends to F its hash value, but it is impossible to E and F to calculate any previous hash value.

In our approach, node identity is encoded in hash value. This way, an attacker cannot increase the sequence number and decrement the hop count in any RREQ or RREP of AODV routing packet this provides integrity to the routing packets of AODV.

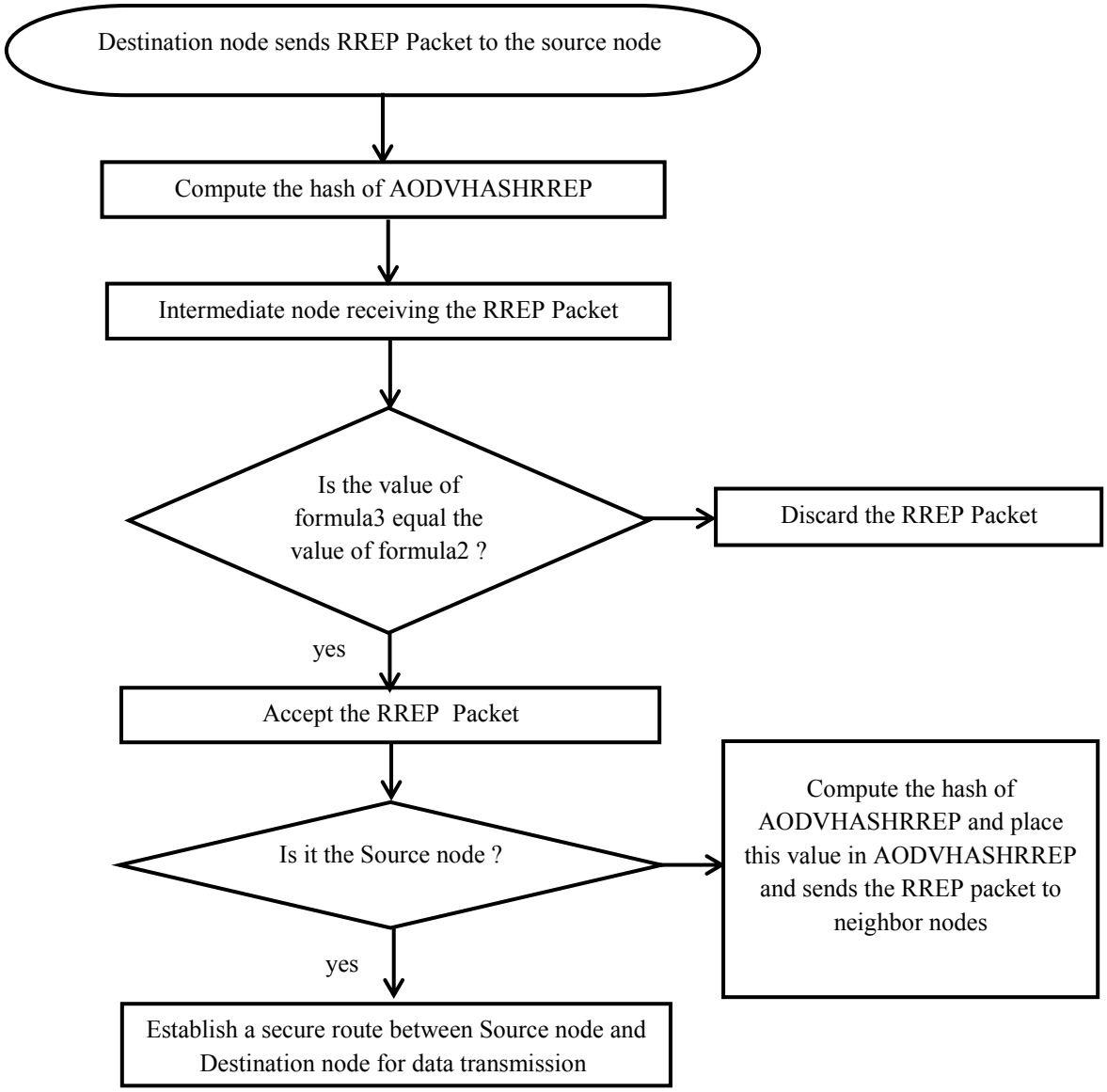

Figure4. Process at intermediate node when it receives RREP Packet

5. Simulation Results and Dissection

In this section, the performance of AODV routing protocol, the effects of black hole attack on the performance of AODV protocol and our solution to struggle against black hole attack launched in single or cooperative manner in AODV routing protocol using OPNET 14.5 simulator [16] will be evaluated.

5.1 Simulation Parameters and Setup

Simulation parameters are shown in Table 1**,** we set up a network with 20 wireless mobile nodes moving at random with Random Waypoint Model. This is a medium group that represents some of the typical scenarios, such as students workgroup in a university campus, a search and rescue team working in a disastrous or remote area, a squad of soldiers or armored vehicles in military operation. For simulation purposes, the network topology without black hole attack is shown in Figure 5.

Table 1. Simulation parameters.

Simulation Parameter	Value
Routing Protocol	AODV routing Protocol
Number of nodes	20
Network size	1000 m * 1000 m
Simulation duration	600 sec
Packet inter-arrival time	Exponential (1)
Packet Size (bits)	Exponential (1024)
Transmit power	0.001
Mobility Model	Random Way Point
Hash Function	SHA-1

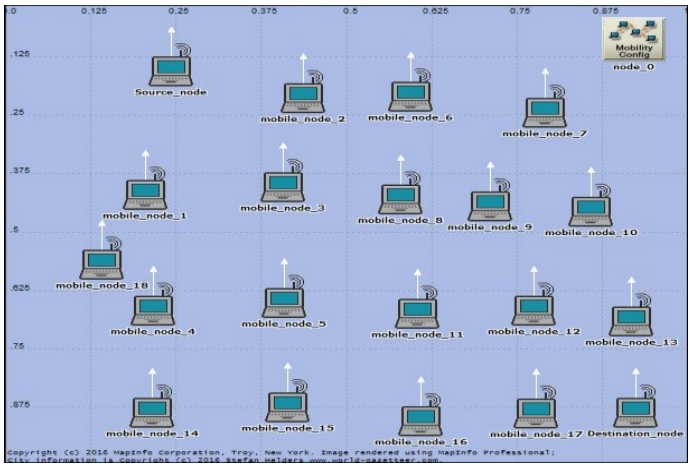

Figure5. Network Topology without Black Hole attack

Mobile_node_5 is selected to launch single black hole attack; the network topology with single black hole attack is shown in Figure 6.Mobile_node_4 and mobile_node_5 are selected to launch cooperative black hole attack; to conduct a cooperative black hole attack cooperation is supposed to be between the two black hole nodes, the network topology with cooperative black hole attack is shown in Figure 7.

Furthermore, the network topology with single black hole attack and solution is similar to the network topology in Figure 6 except that we modify the AODV routing protocol to support our proposed solution with hash chain mechanism and the network topology with cooperative black hole attack and solution is similar to the network topology in Figure 7 except that we modify the AODV routing protocol to support our proposed solution with hash chain mechanism.

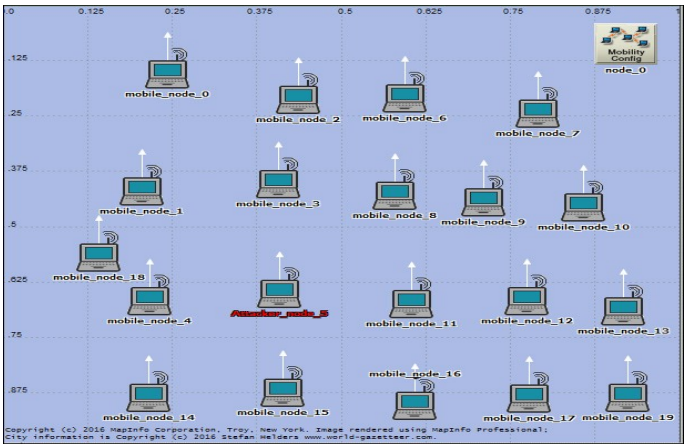

Figure 6. Network Topology with Single Black Hole attack

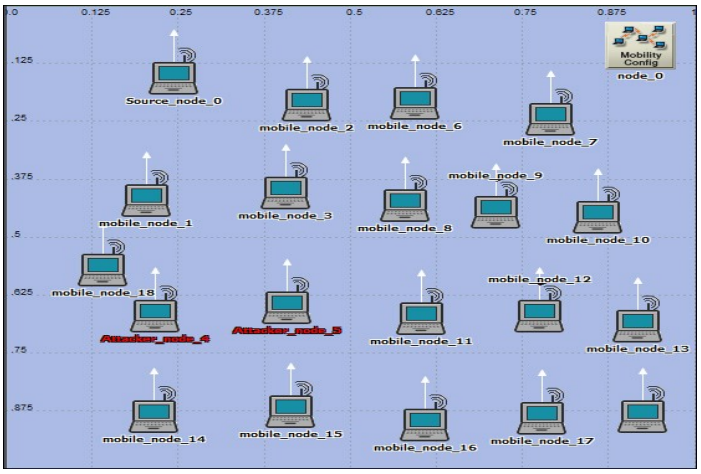

Figure 7. Network Topology with Cooperative Black Hole attack

5.2 Performance Evaluation

To evaluate the performance of AODV routing protocol without and with black hole attack as well as our proposed solution we have measured the following metrics:

1- Throughput

Throughput is a measure of successful delivery of packets in a given interval of time.

2- End-to-end Delay

This metric is defined as the average delay in transmission of a packet between two nodes. It represent the delay in seconds for sending a bit from source node to destination node.

3- Network Load

Indicates the traffic quantity, in bits/second, in the entire network.

Figure 8 shows the average throughput in cases: network without black hole attack, network with single black hole attack, network with cooperative black hole attack, network with single black hole attack and solution, and network with cooperative black hole attack and solution.

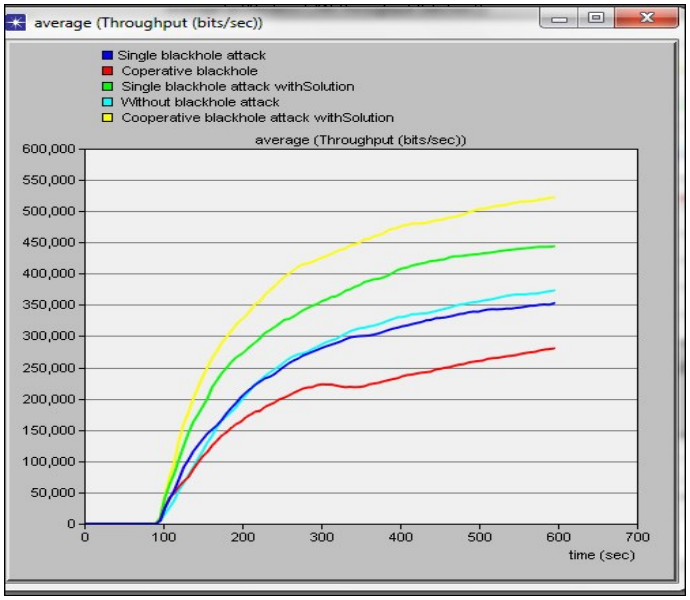

Figure 8.Average Throughput

It is found that the throughput is dramatically decreased as number of black hole nodes increased in the network because malicious node discard some of the packets. To avoid and minimize the effects of black hole attacks, we utilized our proposed solution, as it can be observed from the simulation results, the throughput is high in cases: network with single black hole attack and solution and network with cooperative black hole attack and solution than that in the case of network without attack, this throughput is the amount of data packets that successfully transmitted across the network in a given period of time, and also the hash control information we added to RREQ and RREP packet by our proposed solution. We note that the throughput in the cooperative black hole attack with solution case is larger than that in the single black hole attack with solution case, because more message exchange in cooperative black hole attack with solution than in single black hole attack with solution case.

Figure 9shows the average end-to-end delay in cases: network without black hole attack, network with single black hole attack, network with cooperative black hole attack, network with single black hole attack and solution, and network with cooperative black hole attack and solution.

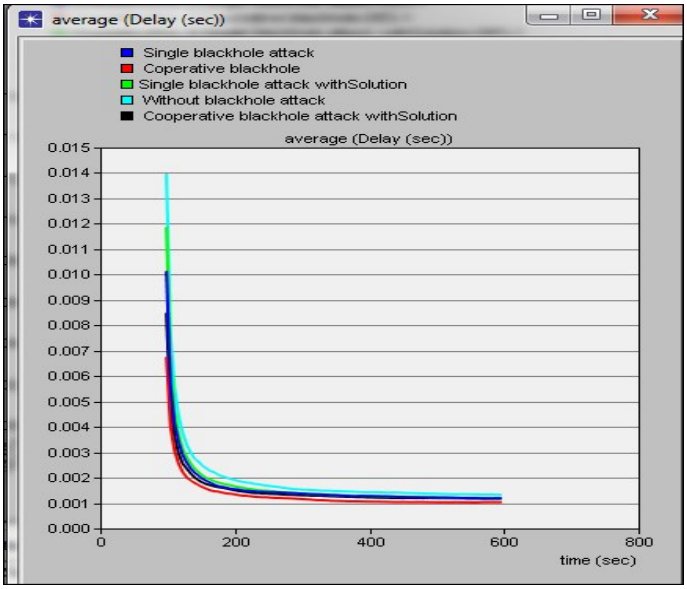

Figure 9. Average End-to-end Delay

From Figure 9, it is obvious that end-to-end delay decreased as the number of black hole nodes increased. If we utilize our proposed solution, we can see that the delay has a slight lag in cases network with single black hole attack and solution; and network with cooperative black hole attack and solution compared to the case of network without attack. This delay is the time taken by source node to send the packets from source node to destination node, thereafter the graphs become almost identical and converge to the normal case (without attack),which show that our proposed solution does not seriously affect network performance. We noted that, the delay at the beginning of simulation in case of cooperative black hole attack with solution has a time-lag than that in single black hole attack with solution case because more calculation is needed by nodes in cooperative black hole attack than in single black hole attack, consequently struggling against cooperative black hole attack takes more time than single black hole attack. Then, the end-to-end delay in our proposed approach converge to the normal case without attack.

Figure 10 shows the average network load for cases: network without black hole attack, network with single black hole attack, network with cooperative black hole attack, network with single black hole attack and solution, and network with cooperative black hole attack and solution.

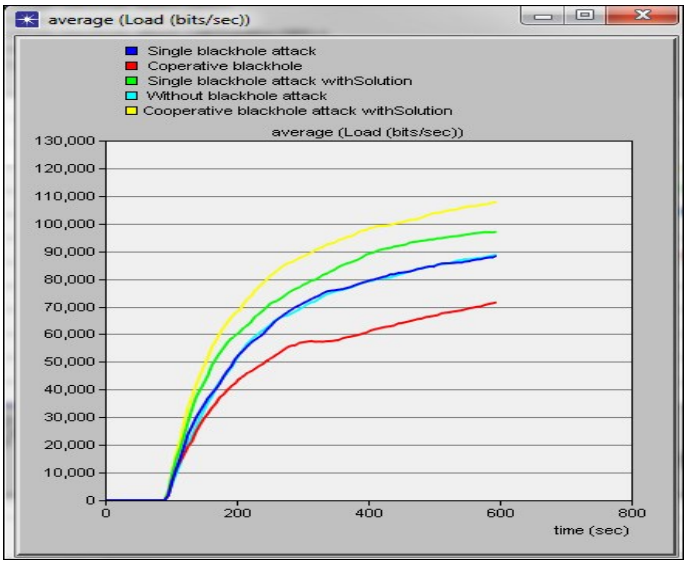

Figure 10. Average Network Load

It is found that the network load decreased as the number of black hole node increases, In our proposed solution the load in the case of network with black hole attack and solution has slight increase than that in the case of network without attack. This network load denotes the amount of traffic quantity in the network. In addition, the hash control information added by our proposed solution and exchange of message among nodes to communicate hash values. We can see that the average load in cooperative black hole attack with solution case is larger than that in single black hole attack with solution case, because there are more message exchange in cooperative black hole attack with solution compared to single black hole attack with solution case.

Figure 11 shows the throughput versus end-to-end delay for cases: network without black hole attack, network with single black hole attack, network with cooperative black hole attack, network with single black hole attack and solution, and network with cooperative black hole attack and solution.

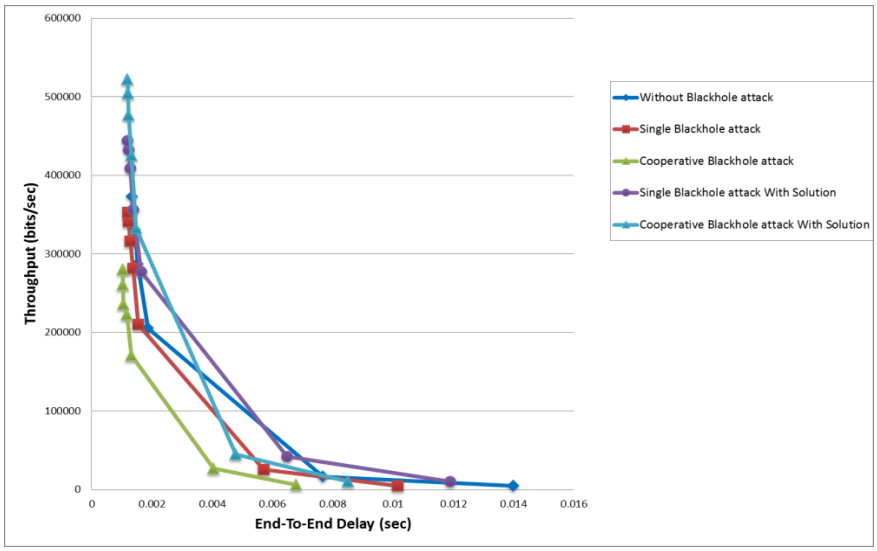

Figure 11.The Throughput VS. End-To-End Delay

From Figure 11, it is obvious that the proposed solution with single and cooperative black hole attack cases performs better than that in the case of network without attack. It has highest throughput and minimum end-to-end delay. The proposed solution has highest throughput, this throughput is the amount of data that successfully transmitted in a given period of time, added to the hash control information added to RREQ and RREP packet by our proposed solution.

Figure 12 shows the throughput vs. network load for cases: network without black hole attack, network with single black hole attack, network with cooperative black hole attack, network with single black hole attack and solution, and network with cooperative black hole attack and solution.

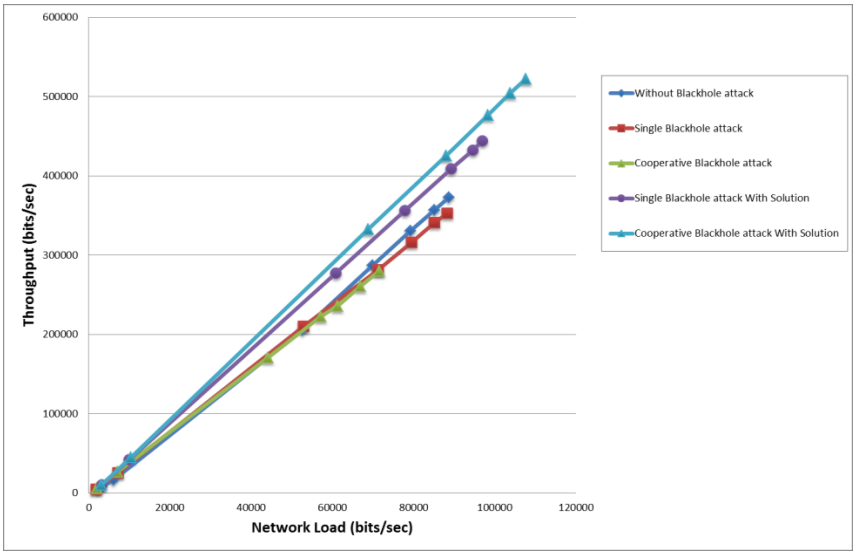

Figure 12. The Throughput VS. Network Load

From Figure 12, it is found that the proposed solution with single and cooperative black hole attack cases has a slightly higher throughput and slight increase in the network load than that in the case of the network without attack. This happens because of the hash control information added by our proposed solution and the exchange of message between nodes to communicate hash values.

As it is shown by these figures, the proposed solution effectively struggle single black hole attack and cooperative black hole attack in AODV routing protocol in MANET, in other words our approach protect MANET against single and cooperative black hole attack.

5.3 Comparison With Related Works

In order to compare our approach with other works focusing on the same subject, we have chosen the Cesar Cipher approach proposed in [6] and Merkle Tree approach proposed in [7], as comparison metrics we have measured the Throughput and end-to-end delay.

Figure 8that illustrates the throughput of our proposed approach, shows that the throughput of the proposed approach is better than the throughput in the Cesar Cipher approach. There are two reasons: first reason is that the Cesar Cipher approach is one of the simplest methods to use in cryptography and can provide minimum security to the information. Second, RREQ message can be decrypted by black hole node, so that source node can receive several RREP and it will choose the one with maximum destination

sequence number and minimum hop count that may belong to malicious node, so source node begins transmit data to it, But, in our approach we add extension to the RREQ packet and RREP packet using hash chain mechanism. This will ensure the integrity of data and guarantee that black hole attack cannot decrease the hop count and increase the sequence number, which effectively avoid black hole attack.

When analyzing the result it shows that throughput of AODV Encryption Decryption with black hole attack is by 88.14 Kbps, and the throughput of AODV with the proposed solution is by 96.43 Kbps. AODV with our proposed solution improves the throughput by 8.29 Kbps as compared to Cesar Cipher approach with single black hole attack and solution.

Figure 9illustrates the average end-to-end delay as it is measured by our proposed approach. As compared with end-to-end delay in Merkle Tree approach, the proposed approach has lower (better) end-to-end delay than that in Merkle Tree approach. The reason is that in the Merkle tree approach it takes more time for calculation of hash values carried out by nodes and sub nodes (parent and child node) such that computing the hash value of each sub node concatenates them and then hash the result to generate the hash value of parent node; while in our approach it takes less time for computations hash values and transmit the data packets to the destination.

In addition, the average end-to-end delay in the Merkle Tree solution with single black hole attack shows 0.13 sec and the average end-to-end delay in Merkle Tree solution with cooperative black hole attack shows 0.07 sec, while the end-to-end delay in the proposed solution with single black hole attack shows 0.012 sec and the end-to-end delay in the proposed solution with cooperative black hole attack shows 0.0085sec.AODV with our proposed approach has less (better) end-to-end delay by 0.118 sec in single black hole attack with solution and by 0.0615 sec in cooperative black hole attack with solution as compared to Merkle Tree approach.

6. Conclusion& Future Work

This paper focuses on black hole attacks when applying AODV routing protocol in MANET networks, where malicious node replies for any route request without having any active route to the specified destination. It then absorbs all the data packets and drops them so destination node will not be able to receive any data packets results in affecting the network performance. When two or more black hole nodes cooperate with each other with same aim of dropping or absorbing the packets these are known as cooperative black hole attack. In order to struggle against this attack we have proposed a solution based on the principles of hash chain mechanism, which that attacker cannot modify the packets thus insuring the packet forwarding by intermediate nodes. Our approach avoid black hole attack launched in single or cooperative manner. Simulation results shown the performance of our approach in AODV routing protocol. Compared to Cesar Cipher and Merkle Tree approaches, our approach has highest throughput and better end-to-end delay. Based on the simulation results, the proposed approach is able to avoid single and cooperative black hole attack in AODV routing protocol in MANET.As future work, it is mainly to analyze the performance of the proposed solution based on various security parameters like network density, node mobility and number of black hole nodes. Also it is intended to extend our mechanism to struggle against another type of attack like gray hole attack.

References

[1] David Remondo, "Wireless Ad Hoc Networks: An Overview", Springer, Vol. 5233, pp. 746-766.

[2] Jeroen Hoebeke.et.al, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", Department of Information Technology (INTEC), Ghent University – IMEC vzw, Belgium.

[3] Shivi Sharma.et.al, "Mobile Ad Hoc Network: Issues, Research Trend And Challenges", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN:2277 128X, Volume 5, Issue 5,pp. 1625-1630, May 2015.

[4] C. Perkins, E.B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC: 3561 (Experimental), IETF, July, 2003.

[5] F.H.Tesng.et.al, "A Survey Of Black Hole Attacks In Wireless Mobile Ad Hoc Networks", Human-centric Computing and Information Sciences, Vol.1, p.4,2011.(http://www.hcis-journal.com/content/1/1/4)

[6] Ahmed Ibrahim, Nagy E Zaki.et.al," Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol", Journal of Computer Sciences and Applications, Vol. 3, No. 4, pp.90-93,2015.

[7] Abderrahmane Baadache, Ali Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks", International Journal of Computer Science and Information Security (IJCSIS), Vol. 7, No. 1, 2010.

[8] Nishant Sitapara.et.al, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks", International Conference on Emerging Trends in Engineering ICETE-2010, Jasingpur, 2010.

[9] P. N. Raj and P. B. Swadas, "DPRAODV: A dyanamic learning system against black hole attack in aodv based manet", IJCSI International Journal of Computer Science Issues, vol. 2, pp. 54–59, 2009.

[10] Tarek. M. Mahmoud, Abdelmgeid A. Aly.et.al,"Avoiding Black Hole attack of AODV routing protocol in MANET", Int. J. on Network Security, Vol. 6, 2015.

[11] L. Himral, V. Vig, and N. Chand, "Preventing Aodv Routing Protocol From Black Hole Attack", International Journal of Engineering Science and Technology (IJEST), Vol.3, 2011.

[12] H. Deng, W. Li, D.P. Agrawal, "Routing security in wireless ad hoc networks", Communications Magazine, IEEE, 40(10) (2002) 70–75.

[13] H. Weerasinghe and H. Fu, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation", International Journal of Software Engineering and its application, vol. 2, no. 3, pp. 39–54, Jul. 2008.

[14] Nishu Kalia, Harpreet Sharma, "Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol", International Journal on Computer Science and Engineering (IJCSE), ISSN : 0975-3397, Vol. 8 No.5 May 2016.

[15] S.Thirumal,"Modified AODV to Prevent Black Hole Attacks in MANET", IJCSET, ISSN: 2231-0711, Vol 1, Issue 8, 447-450, September 2011.

[16] OPNET web site: </http://www.opnet.com/>.