Journal of Computer Sciences and Applications, 2015, Vol. 3, No. 4, 90-93
Available online at http://pubs.sciepub.com/jcsa/3/4/1

DOI:10.12691/jcsa-3-4-1

Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol

Ahmed Ibrahim[1], Nagy E Zaki[2,*]

[1]Department of Computer Science, Modern Academy, Cairo, Egypt
[2]Department of Computer, Science Arab Academy for Science, Technology & Maritime Transport, Cairo, Egypt
*Corresponding author: dr_nagy_ezzat@yahoo.com

Received August 13, 2015; Revised August 19, 2015; Accepted August 27, 2015

Abstract A Mobile Ad hoc Network is a collection of two or more devices connect with another nodes with flexibility and nodes can connect and leave the network easily. The unreliability of wireless networks lack on infrastructure and a lot of attacks can communicate with the wireless network. In the Black hole attack, the malicious node absorbs the data. MANET Disadvantages all packets and traffic in the network are dropped by Black hole node. Black hole node has the shortest path in the entire network by sending fake route reply. In this paper, propose the effect of the Black hole attack on the network performance using AODV protocol. The proposed process uses the AODV Encryption decryption to detect the Black hole attack. AODV Encryption decryption is modification of AODV protocol to reduce the effect of Black hole attack by adding Encrypt/Decrypt function in AODV protocol.

Keywords: *MANET Security, AODV Routing Protocol, ns-2, Wireless Ad hoc Networks, Attacks in Wireless Ad hoc Network, solution to black hole attack*

Cite This Article: Ahmed Ibrahim, and Nagy E Zaki, "Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol." *Journal of Computer Sciences and Applications*, vol. 3, no. 4 (2015): 90-93. doi: 10.12691/jcsa-3-4-1.

1. Introduction

The Ad hoc On-Demand Distance Vector [12] AODV algorithm is self-starting, dynamic, multi hop routing between mobile nodes to establish an Ad hoc network. AODV enable mobile nodes to quick routes to new destination. Nodes do not require maintained routes to destination that are not in active communication. AODV allow mobile nodes to re-establish broken links and changes in the network topology opportunely. AODV is uses destination sequence number for each route entry. The destination is including along with any route information it sends to requesting nodes. The choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number AODV routing protocol is intended for use by mobile nodes in an ad hoc network. A quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. AODV Challenge various kind of attacks such as a black hole attack [1], worm hole attack [2], gray hole attack [3] and so on.

2. Black Hole Attack

The active attack has effect in the network such as denial of service, editing in packets. It is aims of damaging other nodes by causing network outrage are considered as malicious. Active attacks involve actions such as the replication, modification and deletion of exchanged data.

Black Hole Attack is denial is service (DOS) Attack is easy to happen in Ad hoc network, in Black Hole node attacks all packets and fake valid route to the destination. The malicious node waits the neighboring node to send RREQ message, malicious node send fake RREP message to the source node that is the shortest route to the destination node, it has routing over the destination without checking routing table by high sequence number. So that route discovery process is done and start to send data packet over the malicious node instead of send data packets to the destination node. The source node unable to connect to with the real destination node, the Black Hole node received all packets from source node and dropping packets. Consequently malicious node always sends the RREP message having higher sequence number [4].

3. Related Work

S. Amutha and Kannan Balasubramanian [5] proposed novel algorithm has two steps such as checking the difference between the sequence number of source and destination node, and passes the packets in secure routing. If the first route reply will be from the malicious node with high destination sequence number, then that is stored as the first entry in the RR-Table. Compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table.

S.DOKURER [6] proposed IDSAODV this method modified in AODV protocol that implemented to minimize the effect of malicious node. This method implemented by modified in the routing update mechanism in AODV protocol. IDSAODV tries to eliminate the effect of the Black hole attack by ignore the first route in the routing update process. The first RREP message arrived with shortest route to the destination node from the malicious node. IDSAODV switched to the second route, The Black hole node increasing the date loss to 89% when used IDSAODV decreased the data loss to 67% this solution reduce the Black effect by 22% as packet loss.

AnkitaChaturvedi, Sanjiv Sharma [7] proposed IIDSAODV is based on checking the second RREP message and uses the sequence number is a 32 bit unsigned integer the Highest value (HSN). Check second RREP, the difference between the broadcasted and received destination sequence number is calculated and compared to the half of the highest possible sequence number (HSN). The difference should be less than or equal to (HSN/2). If second RREP pass then only the source node switches to this path. If checked fails the source node continue to send the data through the path by first RREP. In Black hole decrease the PDR of AODV by 83.79%, in case IDSAODV and IIDSAODV increase by 40.41% and 78.16%. Decrease throughput of AODV by 77.86%, in case IDSAODV and IIDSAODV increase by 20.66% and 73.59%. Decrease end-to-end delay of AODV by 88.74%, in case IDSAODV and IIDSAODV increase by 44.15% and 71.61%.

B.Sun et al. [8] proposed a neighbor set based approach to detect Black hole attack and a routing recovery protocol to mitigate the effect of black hole attacks. In detection phase collect neighbor set information and determine whether there exists a black hole attack. In response phase a routing recovery protocol is used to build the correct path to the destination. Detect Black hole attack without introduction much routing control overhead to the network. The packet throughput can be improved by least 15% and the false positive probability is usually less than 1.7%.

DPRAODV [9] proposed method that based authenticate the RREP sequence number. RREP_seq_no is higher than the threshold value. Threshold value is dynamically updated, the value of RREP_seq_no 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. It sends a new control packet, ALARM to its neighbors. The neighboring nodes know that RREP packet from the node is to be discarded. It simply ignores the node and does not receive reply from that node again.

EVM [10] Encryption Verification method minimize the multiple Black Hole nodes effectively by employing an encryption mechanism. Identify and verify of the suspicious node using an encrypted verification message. The messages or the sequence numbers contained in the messages cannot be modified by any malicious. EVM can reduce control overhead and increase the detection rate considerably compared to the SNV.

4. Background

Ad hoc network are consist a lot of mobile nodes with a lot of connections that join together. Any node act as router can communicate with any node in the same network if it with transmission range. In Black Hole attack one or more malicious node can intrude the network and start to attack. Any two nodes connect together used routing protocol to communicate. The routing protocol used in this model is the AODV.

5. Problem Identification

Black Hole Attack the malicious node intrude the Ad hoc network and wait the source node send RREQ message to the destination through the neighbors, when the malicious node receives the RREQ message send RREP with the highest sequence number to the source node before any node send RREP.

The source node are receives RREP message with the highest sequence number for the Black Hole node and source node start to establishes the rout to the Black Hole node checking routing table by high sequence number.

6. Proposed Work

In this paper we proposed a mechanism to modify the AODV protocol by adding encryption/decryption features to Overcome Black Hole attack using pre-shared key. For encryption and decryption feature we implement CESAR cipher with pre-shared key of 3.

These cryptographic functions take input as a string of plain text and shift the ASCII value of each character in the text three positions. Any encryption/decryption algorithm with symmetric key can be implemented here.

When using encryption we can be use any kind of algorithms like SHA-1, MD5, AES, DES, EAS and so on. Because the complexity of these algorithms we chose a simple polynomial algorithm to implement it.

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, the source node received the trusted RREP starts to establish route to destination.. Consequently the Black Hole node can't decrypt RREQ. We implemented the proposed mechanism using the Network Simulation program NS2.

7. Implementation

Encryption function:

```
voidSecurity_packetAgent::encryption(char out[])
{
        inti=0, key =3;
                for (i=0;i<strlen(out);i++)
        {
                out[i]=(out[i]+key)%128;
        }
}
```

Decryption function:

```
voidSecurity_packetAgent::decryption(char out[])
{
        inti=0, key =3;
                for (i=0;i<strlen(out);i++)
        {
                out[i]=(out[i]-key)%128;
        }
}
```

8. Simulation

NS2 [11] is very popular network simulation and open source, uses NS2 ver. (2.34). We have 19 nodes and one black hole. NS2 is simulator to evaluate the effect of Black hole attack on AODV Encryption decryption protocol in MANET.

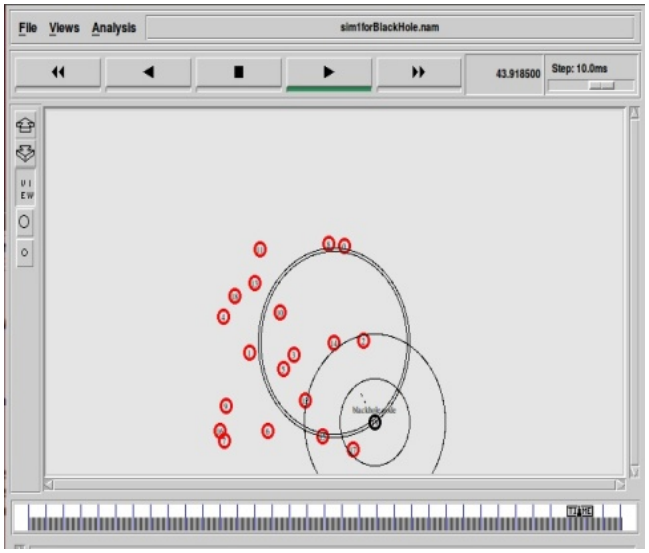

Figure 1. NAM for AODV Encryption decryption

Simulation environment

Table 1. NS-2 Simulation Parameter

Parameter	Value
Simulator	NS-2 (ver. -2.34)
Simulator time	450
Number of nodes	20
Routing Protocol	AODV
Traffic Model	CBR
Terrain Area	750m * 750m
Packet size	512
Maximum speed	20
Pause Time	1
No. of malicious node	1

Simulation result and discussion

Table 2. AODV without Attack

Time	Generated Packet	Received Packet	Packet Delivery Ratio	Throughput
50	1080	845	0.782407	70.93
100	1107	914	0.825655	74.88
150	1107	811	0.732611	66.44
200	1107	914	0.825655	74.88
250	1107	914	0.825655	74.88
300	1107	839	0.757904	68.74
350	1107	793	0.71635	64.96
400	1107	793	0.71635	64.96
450	1125	819	0.728	57.75

Table 3. AODV under Black Hole Attack

Time	Generated Packet	Received Packet	Packet Delivery Ratio	Throughput
50	1080	135	0.125	11.33
100	1107	399	0.360434	32.69
150	1107	122	0.110208	10.07
200	1107	443	0.400181	36.29
250	1107	443	0.400181	36.29
300	1107	443	0.400181	36.29
350	1107	636	0.574526	52.11
400	1107	636	0.574526	52.11
450	1125	649	0.576889	52.28

Table 4. IDS

Time	Generated Packet	Received Packet	Packet Delivery Ratio	Throughput
50	1080	345	0.319444	28.96
100	1107	637	0.575429	52.19
150	1107	467	0.421861	38.295
200	1107	645	0.582656	52.84
250	1107	645	0.582656	52.84
300	1107	645	0.582656	52.84
350	1107	730	0.65944	59.81
400	1107	730	0.65944	59.81
450	1125	745	0.662222	60.02

Table 5. AODV Encryption decryption

Time	Generated Packet	Received Packet	Packet Delivery Ratio	Throughput
50	1080	866	0.801852	72.7
100	1107	1008	0.910569	82.58
150	1107	1009	0.911472	82.66
200	1107	792	0.715447	64.89
250	1107	717	0.647696	58.74
300	1107	717	0.647696	58.74
350	1107	915	0.826558	74.96
400	1107	915	0.826558	74.96
450	1125	937	0.832889	75.48

To evaluate throughput and packet delivery ratio, using the AWK-scripts in NS2. The result is calculated with AWK-scripts and noted the result and draw graphs then analysis and comparison using a single Black Hole node.

Figure 2 show the graph for Throughput of AODV without Black Hole attack, AODV with Black Hole attack, IDSAODV and AODV Encryption Decryption. When analyzing the results show that the Throughput of AODV without Black Hole attack by 87.93 [kbps], AODV with Black Hole attack by 10.15 [kbps], IDSAODV with Black Hole attack by 29.89 [kbps], AODV Encryption

Decryption with Black Hole attack by 88.14 [kbps]. The Black Hole attack decrease the Throughput in AODV with Black Hole attack and IDSAODV with Black Hole attack77.78 and 58.04[kbps]. AODV Encryption Decryption improves the Throughput by 58.25[kbps] as compared to IDSAODV with Black Hole attack.

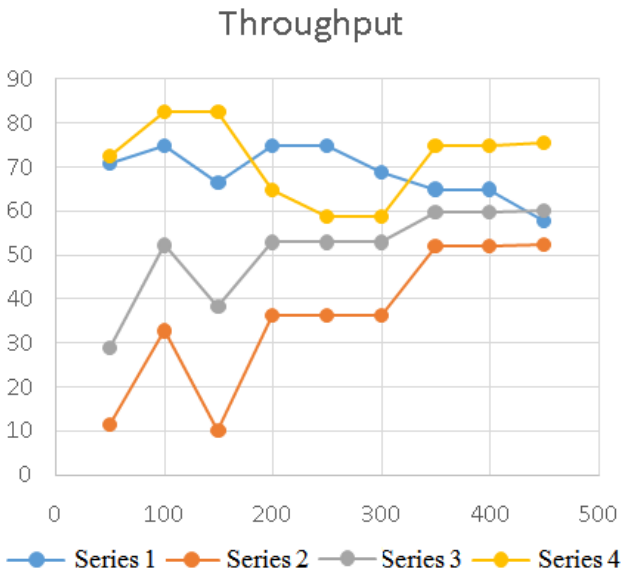

Figure 2. Throughput of AODV, Black Hole, IDS and AODV Encryption decryption

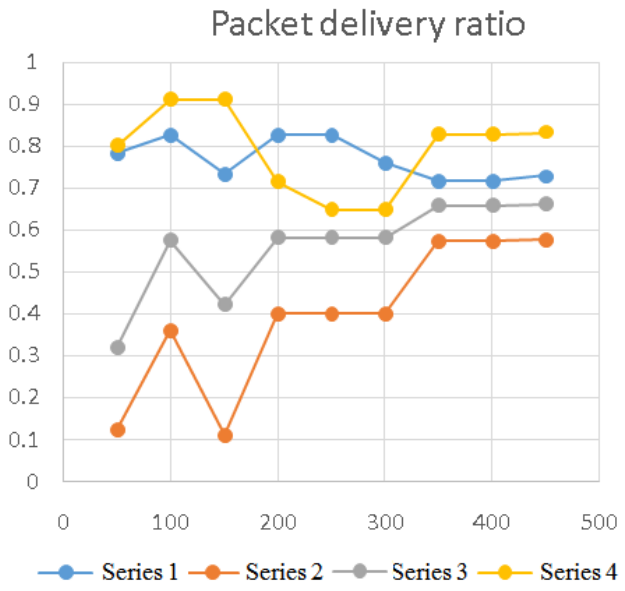

Figure 3. Packet Delivery Ratio of AODV, Black Hole, IDS and AODV Encryption decryption

Figure 3 show the graph for Packet Delivery Ratio of AODV without Black Hole attack, AODV with Black Hole attack, IDSAODV and AODV Encryption Decryption. When analyzing the results show that the Packet Delivery Ratio of AODV without Black Hole attack by 97.62%, AODV with Black Hole attack by 11.26%, IDSAODV with Black Hole attack by 33.18%,AODV Encryption Decryption with Black Hole attack by 97.85%. The Black Hole attack decreases the Packet Delivery Ratio in AODV with Black Hole attack and IDSAODV with Black Hole attack 86.36% and 64.44%. AODV Encryption Decryption improves the Packet Delivery Ratio by 64.67% as compared to IDSAODV with Black Hole attack.

9. Conclusions

In this paper we presented the effect of the Black Hole attack in MANET using simulator NS2.Any time the malicious node can enter the Ad hoc network, no security in the nodes and lack of infrastructure. Ad hoc network was open network to a lot of attacks. Our proposed uses the AODV encryption decryption protocol to Overcome Black Hole attack. The RREQ message is encrypted at the source node and send through the neighbors to the destination node using pre-shared key, destination node only can decrypt the RREQ message and send the RREP message to the source node, start to established route to destination. The black hole node cannot decrypt RREQ message and minimize the effect of the Black hole attack. Evaluate the performance AODV Encryption Decryption of Throughput and Packet Delivery ratio better than IDSAODV. The simulation result state that the proposed protocol gives higher security and may have less packet drops and throughput.

References

[1] Abdalrazak T. Rahem, H K Sawant ―Collaborative Trust based Secure Routing based Ad-hoc Routing Protocol ‖ in International Journal of Modern Engineering Research (IJMER) Vol.2, Mar-Apr 2012.

[2] Enrique Hern´andez-Orallo, Manuel D. Serrat, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni ―Improving Malicious Node Detection in MANETs Using a Collaborative Watchdog in IEEE Communications Letters, Vol. 16, No 5, May 2012.

[3] R. Lu, X. Lin, H. Zhu, and X. Shen, ―SPARK: A New VANETBased Smart Parking Scheme for Large Parking Lots, Proc. IEEE INFOCOM ‘09, Apr. 2009.

[4] Satoshi Kurosawl, Hidehisa, Nakayama, NeiKato,AbbasJamaipour and Yoshiaki Nemoto, “ Detecting Blackhole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning Method”, International Journal of Network Security,vol.5,no.3,pp.338-346,2007.

[5] S. Amutha and 2Kannan Balasubramanian, “Detection and Prevention of Black Hole Attack on MANET Routing Protocols” Australian Journal of Basic and Applied Sciences, 9(5) March 2015, Pages: 281-289.

[6] S. DOKURER, “Simulation of Black hole attack in wireless Ad-hoc network”, Master’s thesis Atılım University, September 2006.

[7] AnkitaChaturvedi, Sanjiv Sharma, “A new Technique for Preventing Black Hole Attack in Mobile Ad-hoc Network” International Journal of Advance in Computer Science and Technology, vol 3, No. 10, October 2014.

[8] B. Sun, Y. Gunan, J. Chen and U. Pooch, “Detection Black-Hole Attack in Mobile Ad-Hoc Networks” 5th European personal Mobile Communications Conference, pp.490-495, Scotland, 2003.

[9] Raj PN, Swadas PB,”DPRAODV a dynamic learning system against blackhole attack in aodv based manet”, International Journal of Computer Science Issue, vol. 2, pp. 54-59, 2009.

[10] Firoz Ahmed, Hoon Oh, “An Encryption Based Black Hole Detection Mechanism in mobile Ad Hoc Networks”, ” International Journal of Security and its Applications, vol. 7, No. 6 (2013). Pp. 1-10.

[11] ns-2:http://www.isi.edu/nsnam/ns/.

[12] C. Perkins, E. Belding-Royer, S. Das, ” Ad hoc On-Demand Distance Vector (AODV) Routing”, July 2003.