Journal of AL-Qadisiyah for computer science and mathematics Vol.9 No.2 Year 2017
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Black Hole Attack in Mobile Ad Hoc Network and its Avoidance

Ali Ayid Ahmad
Kirkuk University
College of Engineering
Electrical Engineering Dept.
aliayid2013@gmail.com

Ahmed Chalak Shakir
Kirkuk University
College of science
Computer Science dept
dr.ahmedchalak@uokirkuk.edu.iq

Recived : 14\8\2017 Revised : 29\8\2017 Accepted : 20\9\2017

Abstract: Mobile Ad Hoc Network is an infrastructure less wireless network where the mobile nodes leaves and joins the mobile network very frequently. The routing of the packets from source node to destination node, the routing protocol is used. On Demand Distance Vector Routing protocol is very common and implemented with Mobile Ad Hoc Network nodes to handle the operations of packet routing from by any node as a source node to destination node. In this paper prevention of black hole attack by modifying the On Demand Distance Vector routing protocol. The sequence number of 32 bit is initiated with the Route Reply and route sequence packet broadcast to determine the request reply from black hole node under the Mobile Ad Hoc Network. The sequence number and On demand Distance Vector Routing protocol are integrated with a mechanism to find the Request Reply of message containing routing information from source to destination node in Mobile Ad Hoc Network.

Keywords: MANET – Mobile Ad Hoc Network, DSR – Dynamic Source Routing, DSSR – Destination Sequence Routing, DoS – Denial of Service, AODV – On Demand Distance Vector Routing.

1. Introduction

Mobile ad hoc network (MANET) is very popular category of computer network at present scenario of communication network. It is a non infrastructure based network where the communicating nodes have the capability to self configure with respect to the current mobility. This category of network is also called wireless ad hoc network. The number of communication nodes in mobile ad hoc network is not fixed, it can increase and decrease with respect to time and mobility. MANET is composed by the mobile devices under the mobile wireless communication technology. Mobility is primary core requirement of this category of network.

Mobile ad hoc network provides the facility for nomadic computing interface with dynamic changing topology of wireless network. The network devices such as routing system device, switching device are also mobile under the mobile ad hoc networks. The dynamic topology of the network gives the flexibility to the computing nodes to join and leave the network anytime. In geographic location it is not possible to setup the infrastructure network, therefore, mobile ad hoc network removes this problem by establishing the communication system via computing devices with wireless networking infrastructure. Nodes of the mobile ad hoc network directly forwards the packet to each other.

Dynamic connectivity of mobile ad hoc network is supported by Dynamic Source Routing (DSR) and Destination Sequence Source Routing (DSSR) protocols. In mobile ad hoc network the node work as a host as well as a router to forwards the packets from incoming source to intermediate node or destination node. Due to lack of the infrastructure a Mobile Ad Hoc Network (MANET) is more prone to be attacked. Non infrastructure of MANET opens the opportunity to attacker to launch different categories of attacks in the network. With variety of network attacks, black hole attack is considered as inside attack for a MANET. Black hole attack disrupts the service of MANET and causes vary Sevier problem. The major problem associated with black hole attack with MANET is that the confidentiality of data contained under the packets are disclosed and network bandwidth consumed. This attack also exploits the routing protocol working with MANET.

Basic scenario of black hole attack is that an attacker node or system creates its validity in MANET by advertising itself as a valid node. It advertises its router path for nodes to carry to send the packets from source node to destination node. Whenever the attacker node register itself with MANET it becomes able to listen all the broadcasted Route Request packets of the different nodes. Once it gets the Router Request packet, it replies to the broadcasting node reply by its own path as the least cost path. The sender node updates its route path in routing table and follows that path to send the packet. Packets that go through that malicious path is intercepted by malicious node and also be dropped on it. The packet data also be intercepted and confidentiality of data is being broken by the malicious node.

The intelligent concept behind the attacker node is that it advertises the route to all other nodes in MANET by indicating that it is shortest router path. Black hole attack is generally considered as a type of Denial of Service (DOS) attack. It is one of the common security threat for a network such as MANET or any other categories of infrastructure and non infrastructure network.

Nodes of MANET is able to respond the Route Request (RRequest) message as this is functional aspect of ON Demand Distance Vector Routing (AODV) protocol. The concept behind the black hole attack and its scenario are presented under figure 1.

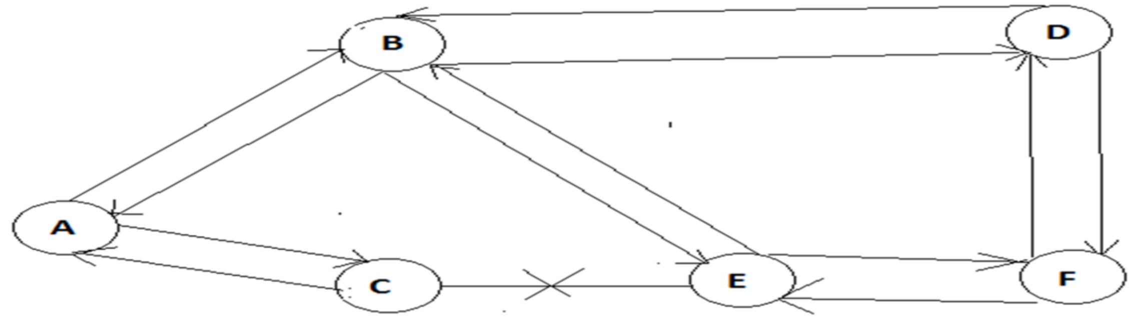

Figure1. Black hole attack scenario in MANET

Let A, be the source node and F be the destination node of MANET presented under figure 1. A, broadcasts the Router Request packet into the network to all current active nodes to get the route of node F. Now, consider that Node C is malicious node introduced itself in the MANET. This malicious node is attacker node under the MANET. Node C listens the broadcasted packet by A, and immediately reply the Route path to A via its own route to F. After reply by C an updates its routing table and follows the path to send the packets to F. Node C becomes able to get all the packets which are sent from A to F. Thus, C intercepts all the packets sent by A to F and dropped them. This consumes the network bandwidth and also confidentiality problems with the data packet which are sent from A to F and intercepted and dropped by C. This is termed as the black hole attack.

2. Related Work

Kashmeera N and Jyna B Shah in their research work stated the basic facts behind the black hole attack with MANET. They stated that mobile nodes self configure and MANET is automatically formed. MANET does not provides the centralized network management procedure so that the malicious node easily self configures itself with the network and drops all the packets passing through the path flowing to it from source node to destination node. Therefore, the security of AODV protocol working on each of the node of MANET is being compromised by black hole attack [1].

Vimal Bibhu and Kumar Roshan presented the preventive measure of black hole attack of MANET. Discrete properties of routing protocol is proposed by analysis of various routing protocol used for MANET. A new mechanism with AODV routing protocol of MANET is inserted to prevent the black hole attack with MANET. A combined protocol approach is taken to discover the new path for routing the packets with defined time interval. The old path of the routing table of nodes are refreshed with regular time interval. They tested the preventive measure of black whole attack with a MANET of 50 nodes with defined area of 1000 x 1000 square meter for movement with 5 meter per second speed. The result is approximated by calculation of throughput verses the number of black hole nodes with pause time of 0 second. 40 second, 120 second and 160 second when threshold value reaches to 1 [2].

Marpu Dev Adas and Vinay Kumar, proposed an authentication mechanism for the prevention of black hole attack with MANET. A prototype is built which simulates the black hole attack and its preventive measures. Their built prototype serves as proof of concept behind the protection of MANET from black hole attack. The result of simulation is optimal and encourage to employ the authentication mechanism with MANET [3].

Ashly Thomas and Nisha P John, produce a review of the black hole attack with AODV protocol used in MANET. They stated that the firewall and encryption systems used with the MANET nodes are not sufficient to prevent the black hole attack. They make survey and review the existing solution of the black hole attack on AODV protocol [4].

Marti et all given the solution for detection of malicious node in MANET by the use of watchdog. In this technique when a node forwards a packet to next node then it watches that the node which accepts the packets further forwards to next node or not. This process continues till the last node which forwards the packet to destination node. Whenever the node finds that the next node does not forward the packet with a given threshold time, then the node understand that the next to which the packet is forwarded is a malicious node in the network. But, this technique has two problems. First, the node must have to trust the information of the other node in the network and second problem is that watchdog would not be able to differentiate the ambiguous collision [5].

Scan et al all have propose two different methodologies to protect the MANET from the entry of malicious node to protect the network from black hole attack. These two proposed methods are local collaboration and information cross validation. In local collaboration each neighboring node monitor each other. In case of second method such as cross validation each node cross checks the transmission overhead of its neighbor nodes. These two methods provide the self organized, distributed and localized solution for the prevention of black hole attack by malicious node in MANET [6].

S. Ramaswamy produced an algorithm that claims about the prevention of black hole attack with MANET. Additional Data Routing information is maintained by each of the node of network. A replies to Router Request packet, node also sends the Identity of its next hop and make the entry of identity into the additional data information table. If the receiver node of reply finds that Identity is not trustable as that does not exist in its table then it again broadcast the Route Request. Similar condition is checked each when the sender node of Route Request gets the reply from non trustable node [7].

3. Required Properties of Routing Protocols for MANET

Routing protocols of MANET must have some desirable properties to route the packets from source node to destination node. These properties are inherited from the existing routing protocols. Some of the important characteristics of MANET routing protocols are defined with following sub sections

3.1 Distributed MANET Operation

The protocol that is used for routing in MANET should have to follow the distributed operation management aspects. This property is required due to fact that the nodes in MANET always joins and leaves the network frequently. Therefore, distributed management functionality is needed to manage the network operation efficiently.

3.2 Loop Free Operation

The operational procedures of the MANET routing protocol must ensure the loop free operational situation. This ensures the operation more efficiently and also prevents the wastage of network bandwidth which is consumed by creating the loop for routes.

3.3 On Demand Operations

The on demand operational aspects of MANET reduces the control overhead and also enhance the utilization of network resources. Hence, for on demand services the deployed protocol of network operation of MANET should have the reactive property. The periodic broadcast of control information should be prevented and on demand service with control information is optimized under the MANET.

3.4 Provision of Bi-Direction Communication Link

The protocol must supports the bi-direction communication support under the MANET. The radio signal has the characteristics to be propagated in all directions so that the protocol must have to support the bi-directional link for all the links of nodes of MANET.

3.5 Communication Security

The communication among the nodes of MANET is required to be secured. Therefore, protocol must ensure the maximum security from the impersonation and other wireless categories of attacks. The security measures such as authentication, encryption and authorization are should be implemented through the routing protocols of MANET. The protocol should have the additional security layer to handle the security measures properly and effectively.

3.6 Power Save

The mobile nodes are operated through battery power and it is limited power resource. Hence, the protocol must employ some mechanism to save the power of nodes in MANET. The saving of power can be achieved by employing the strategy which push the nodes in standby when the node is idle.

3.7 Multiple Route to Route Packets

The congestion and change of topology reactions with the network is reduced by constructing the multiple routes for the packets from source node to destination node. This multiple route reduces the routing protocol to discover new route by broadcasting Route Request packet by providing the other route as stored under the routing table which is valid. Therefore, the time and packet transmission time becomes lower for a node in the MANET.

4. Proposed Solution for Black Hole Attack Problem with MANET

In this research work AODV protocol is modified to support the prevention of black hole attack in MANET. The modification in AODV protocol working mechanism is taken to avoid the black hole attack by making twice reply for Route Request broadcasted packet by node. A 32 bit sequence number of Route Reply message is introduced to AODV protocol. It is also oblivious that the destination node is nearby to the black hole node. Thus, in this case the first Route Reply message is sent by destination node and second Route Reply message is sent by black hole node. In this case the source gets two routing path for the destination node. In this circumstance only first Route Reply routing information is employed by source node to send the packets to destination node.

The selection of first Route Reply routing information is derived by comparing the sequence numbers with the half of the value of maximum value of sequence number. If the first Route Reply message contains the sequence number which lies under the half of maximum value of sequence number then it is considered that the this Route Reply message is coming from valid node in MANET. This is established by passing the check with difference is either less than or equal to half of the maximum sequence number formed by 32 bits sequence number. Thus, the source node becomes able to switch itself to adopt the first Route Reply message routing information [8][9].

5. Designed Algorithmic Steps

Step 1. The source node A gets the first request reply message

Step 2. Source node A checks about the freshness by Received Destination Sequence Number > = Broadcast Destination Sequence Number.

Step 3. If the Received Destination Sequence Number is greater than or equal to Broadcast Sequence Number then source node A sends the packets to destination F through the first routing path that gets from first Request Reply message and increases the count by 1.

Step 4. When source node A gets another Request Reply message then it gain checks the freshness of the Request Reply Message as used in Step 2.

Step 5. If the current Request Reply message Received Destination Sequence Number is greater than Broadcast Sequence Number then count is again increased by 1.

Step 6. The source node A performs additional check on current received Request Reply by applying the given below mechanism. If Count is greater than 1 and Received Destination Sequence Number > = Broadcast Sequence Number then source node A considers that the containing routing information of current Request Reply message is also genuine and not coming from black hole node.

Step 7. When the check performed by source node A from step 6 fails then it determines that the routing information path of current Request Reply message is coming from black hole node. Therefore, source node A discards the current routing path of Request Reply message and adopts only the first path of first Request Reply Message.

Above algorithmic steps are employed over the AODV protocol modification. The proposed change of AODV algorithm clearly states about the prevention of black hole attack.

5.1 Simulation Setup

The result of proposed research for preventing the black hole attack is verified by verifying the result with NS-2 simulation. The simulation setup is is produced under table 1.

TABLE1. Simulation Setup in NS2

Simulation Package	NS-2
Time of Simulation	100 second
Nodes of Manet	10
Protocol	Modified AODV
Pause Time	1 Second
Max Speed	20 mili second
Max Connection	20 % of n
Malicious Node taken	5
Area	750 x 750

5.2 Result Analysis

The ratio of packet delivery and throughput are taken. Throughput is obtained by dividing total packets sent by received packets Ration of packet delivery is obtained as dividing total packet received by total packet sent.

Thus, the result of the given scenario is presented under table 2,and 3 for throughput and ratio of packet delivery are mentioned respectively

TABLE2. Throughput in Kbps with No. of Black Whole Nodes

Throughput (Kbps)	No. Black Hole Nodes
80	1
78	2
77	3
74	4
66	5

TABLE3. Ratio of packet delivery with No. of Black Hole Nodes

Packet Delivery Ratio	No. Black Hole Nodes
90	1
89	2
87	3
82	4
75	5

The throughput and ratio of packet delivery are graphically shown in figure 2 and 3. The graph is plotted through spreadsheet utility.

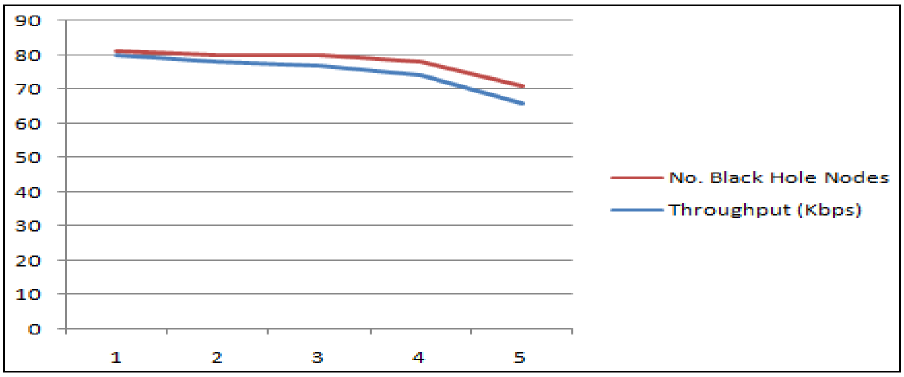

Figure2. Throughput in Kbps with No. of Black Whole Nodes

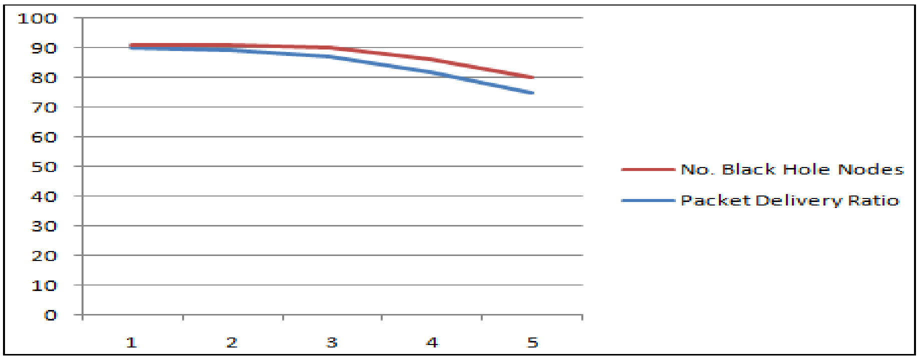

Figure 3. Ratio of Packet Delivery with No. of Black Whole Nodes

Conclusion

Black hole attack is a very big problem of Mobile Ad Hoc Network. Black hole node drops the communicated packets from source node to destination node. It also discloses the confidentiality of packet data. Prevention of black hole attack requires the efficient and proactive mechanism by modification of existing routing protocols used for the MANET. In this proposed research AODV protocol is modified to prevent the black hole attack in MANET. Stepwise modification by which the sequence of broadcasted Route Request packet and received Route Reply. In the proposed mechanism two different Route Reply with sequence numbers are compared separately when the message comes from nearby nodes with half of the value of maximum value of 32 bit sequence number. If the message sequence number of received Route Reply message is equal or less than half of the maximum value of sequence number then it is considered that the Route Reply comes from genuine node not from the black hole node.

References

[1] K. Khachar and J. Shah, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks: A Survey", IOSR Journal of Computer Engineering, vol. 16, no. 2, pp. 108-112, 2014.

[2] K. Roshan and V. Bibhu, "Preventive Aspect of Black Hole Attack in Mobile AD HOC Network", International Journal of Computer Network and Information Security, vol. 4, no. 6, pp. 49-55, 2012.

[3] M. Devadas and V. Kumar, "Protecting Mobile Ad Hoc Networks from Black Hole Attacks", International Journal of Computer Science and Mobile Computing, vol. 3, no. 12, pp. 224-230, 2014.

[4] N. John and A. Thomas, "Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review", International Journal of Scientific and Research Publications,, vol. 2, no. 9, pp. 1-6, 2012.

[5] S. Marti, T. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", MOBICOM), pp. 255-265, 2000.

[6] H. Yang, J. Shu, X. Meng and S. Lu, "Self-organized network-layer security in mobile ad hoc networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 261-273, 2006.

[7] S. Ramaswamy, H. Fu, M. Sreekantaradhya and J. Dixion, "Prevention of cooperative black hole attack in wireless ad hoc networks", ICWN'03, pp. 570–575, 2003.

[8] O. Gonzalez, M. Howarth and G. Pavlou, "Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Network", Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium, 2007.

[9] A. Aggarwal, "Dealing with Black Hole Attack in Mobile Ad Hoc Network (MANET)", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 1256-1259, 2013.

مهاجمة الثقب الاسود في شبكة الجوال وتجنبها

احمد جالاك شاكر	علي عايد احمد درويش
جامعة كركوك	جامعة كركوك
كلية العلوم	كلية الهندسة
قسم علوم الحاسبات	قسم الهندسة الكهربائية

المستخلص:

ان شبكة الإعلان المخصص للجوال هي بنية تحتية للشبكة اللاسلكية حيث تغادر العقد المتنقلة وتنضم إلى شبكة الهاتف النقال في كثير من الأحيان بشكل متكرر. ان توجيه الحزم من عقدة المصدر إلى عقدة الوجهة يتم باستخدام بروتوكول التوجيه، وعلى بُعد الطلب فان ناقلات بروتوكول التوجيه وتنفيذها مع العقد هو امر شائع جدا في شبكة الجوال المخصص للتعامل مع عمليات توجيه الحزمة من قبل أي عقدة كعقدة مصدر لعقدة الوجهة. في هذا البحث نستنتج الوقاية من هجوم الثقب الأسود عن طريق تعديل بروتوكول ناقلات التوجيه وبُعد الطلب. ويبدأ عدد التتابع البالغ 32 بت مع إرسال رزمة رد وتسلسل المسار لتحديد رد الطلب من عقدة الثقب الأسود في الشبكة المخصصة للجوال. حيث يتم دمج رقم تسلسل وبروتوكول التوجيه للناقلات و البعد على الطلب مع آلية للعثور على طلب رد الرسالة التي تحتوي على معلومات التوجيه من المصدر إلى عقدة الوجهة في الشبكة الإعلانية المخصصة للجوال.