INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review

Nisha P John
M. Tech student, Department of Computer Science andEngineering
MES College of Engineering Kuttippuram, Kerala, India

Ashly Thomas
Assistant Professor, Department of Computer Science and Engineering
MES College of Engineering Kuttippuram, Kerala, India

Abstract:

An ad-hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. Networks are protected using many firewalls and encryption software's. But many of them are not sufficient and effective due to its limited power and mobility. The ultimate goal of the security solutions for wireless networks is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. Black hole attack is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on- demand routing protocols such as Ad-Hoc On Demand distance vector (AODV). In this paper, we have surveyed and compared the existing solutions to black hole attacks on AODV protocol.

Keywords: *MANET, AODV, Black hole attack*

Introduction

A mobile ad-hoc network [1] is a self organizing net- work that consists of mobile nodes that are capable of communicating with each other without the help of fixed infrastructure. On the contrary to traditional wired networks that use copper wire as a communication channel, ad-hoc networks use radio waves to transmit signals. Mobility, an advantage of wireless communication, gives a freedom of moving around while being connected to a network environment. Ad-hoc networks are so flexible that nodes can join and leave a network easily. But this flexibility of mobile nodes results in a dynamic topology that makes it very difficult in developing secure ad-hoc routing protocols. Security being a serious issue, the nature of ad-hoc networks makes them extremely vulnerable to adversarys malicious attacks. First of all, the use of wireless links renders a mobile ad-hoc network to be vulnerable to attacks of various types - black hole attack being one of them [2]. Unlike wired networks where an adversary must gain a physical access to network wires or pass through several lines of defense at firewalls and gateways, attacks on mobile ad-hoc network can come from all directions and target at any node. Compared to traditional wired networks (a network in which network traffic could be monitored at central devices such as switches and routers), mobile ad-hoc networks have no network concentration points to filter traffic.

The use of wireless links, lack of fixed infrastructure and the characteristic of dynamic topology associated with adhoc networks make it impossible to use wired network security mechanism as is.

In the rest of this paper, we summarizes the basic operation of AODV protocol and Black hole attack and describe some methods that have proposed for detecting or preventing these attacks and provides a comparison for the methods and finally, we conclude the paper.

Ad-Hoc Routing Protocols And Black Hole Attack

An ad-hoc routing protocol [3] is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile adhoc net- work. Being one of the category of ad-hoc routing protocols, on-demand protocols such as AODV (Ad-hoc On demand Distance Vector) and DSR (Dynamic Source Routing) establish routes between nodes only when they are required to route data packets.

AODV [4] is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network.

In an ad-hoc network that uses AODV as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery. Every neighboring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its routing table. It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. If a node finds a fresh enough route, it unicasts an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has fresh route to the destination node is received by the source node.

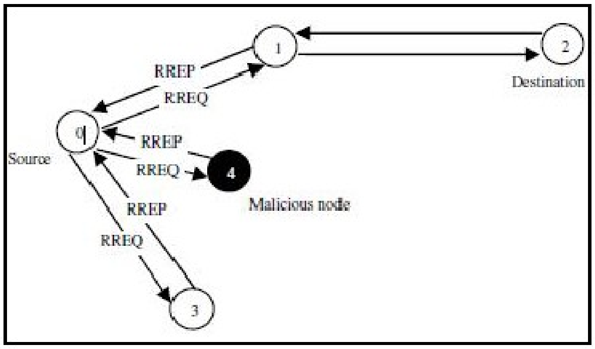


Figure 1: Black hole attack in AODV

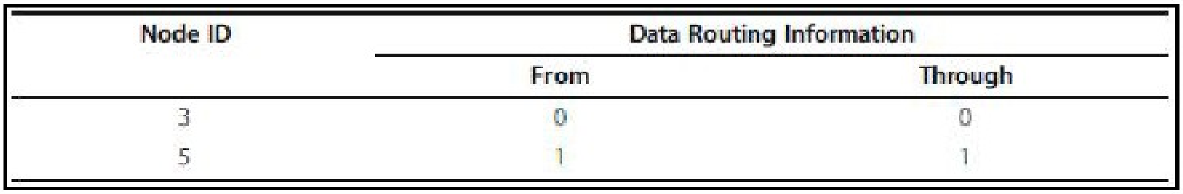
Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad- hoc networks. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to drop all the network traffic it receives from source nodes. This deliberate dropping of packets by a malicious node is what we call a black hole attack [5].

A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As shown in Fig. 1 above, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1, 3 and 4. However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2.

An RREP message from a malicious node [6] is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them on.

Literature Survey

In this section, we review six different methods for the detection and removal of black hole attacks in AODV based Mobile Ad-Hoc networks.



Node ID	Data Routing Information	
	From	Through
3	0	0
5	1	1

Figure 2: DRI table for node1

DRI table and Cross checking scheme

H. Weerasinghe and H. Fu [7], introduces the use of DRI (Data Routing Information) to keep track of past routing experience among mobile nodes in the network and crosschecking of RREP messages from intermediate nodes by source nodes to identify the cooperative black hole nodes, and utilize modified AODV routing protocol to achieve this methodology. Every node needs to maintain an extra DRI table, 1 represents for true and 0 for false. The entry is composed of two bits, From and Through which stands for information on routing data packet from the node and through the node respectively.

As shown in Table, the entry 1 1 implies that node 1 has successfully routed data packets from or through node

5, and the entry of 0 0 means that node 1 has not routed any data packets from or through node 3. The procedure of proposed solution is simply described as below. The source node (SN) sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the

INs honesty. After that, SN sends the further request to INs NHN for asking its routing information, including the current NHN, the NHNs DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path.

Advantages

- Identification of multiple collaborative black hole nodes in a MANET.
- Discovery of secure paths from source to destination that avoid collaborative black hole nodes acting in cooperation.

Disadvantages

- The main drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table. It is evident that maintaining past routing experiences wastes memory space as well as consuming a significant amount of processing time which contributes to slow communication.
- The second drawback is over consumption of limited bandwidth. Cross-checking of the validity of routes contained in RREP message from an intermediate node is implemented by sending a FREQ (Further Request) message to the next-hop of the particular intermediate node. Sending additional FREQ messages consumes a significant amount of bandwidth from an already limited and precious resource.

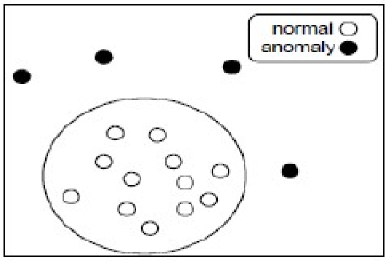


Figure 3: Distribution of network state

- If there is not any attack in the network, this scheme works very slowly and has a huge overhead for checking all nodes in a route.

Dynamic Learning Scheme

Kurosawa et al. [8] proposed a dynamic learning method to detect a black hole node. In this approach, the normal state views are updated periodically to adapt to the frequent network changes and clustering-based technique is adopted to identify nodes that deviate from the normal state. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a black hole node, otherwise, the data of the latest observation is added into dataset for dynamic updating purposes. However, it does not involve a detection mode, such as revising the AODV protocol or deploying IDS nodes, thus, it does not isolate black hole nodes.

They have adopted the following 5-step process:

- Feature selection: To express state of the network at each node, multidimensional feature vector is defined. Usually the number of sent out RREQ and the number of received RREP, The average of difference of Dst Seq in each time slot between the sequence number of RREP message and the one held in the list are taken as features.
- Calculate mean: The mean vector values of these features are calculated, as shown in eqn where D represents training data set for N time slot.

  $$xD=1/N(\sum^{n}_{i=1} X_i)$$

  Hence the initial training data refer to the data collected in the first interval of the network, i.e. T0
- data sample x to the mean vector as shown here.

  $d(x)=|x-xD|\wedge 2$

  From the learning data set, the distance with the maximum value is extracted as threshold Th.

  $T_h = d(xI)$

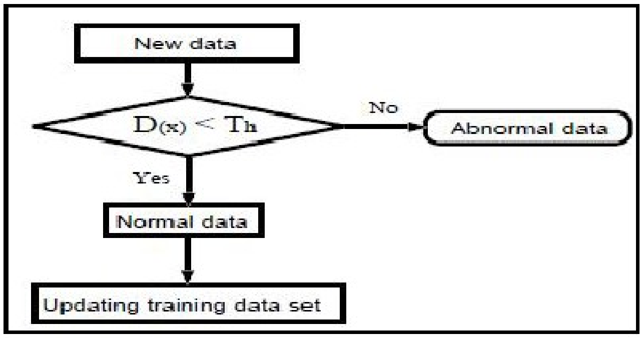


Figure 4: Flowchart for Dynamic learning system method

- Anomaly detection: When the distance for any input data sample is larger than the Th, it is considered deviates from the normal traffic and hence, judged as an attack. $d(x > Th$: attack $d(x) \leq Th$: normal
- Dynamic training: By using data collected in initial time, the calculated mean vector will be used to detect the next period time interval. If it is judged as normal, the corresponding data set will be used as learning data set, else, it is treated as data with attack and consequently discarded. This learning process is repeated for every interval.

Advantages

- Here adopt anomaly-based detection technique; detecting any deviation from the established normal profile.

Disadvantages

- This technique suffers from a high false-alarm rate especially when the normal behaviour definitions are still unclear and non-standard in wireless ad hoc networks.

DPRAODV Scheme

In paper [9] authors P. Raj have proposed Detection, Prevention and Reactive AODV (DPRAODV) Scheme. A new control packet called ALARM is used in DPRAODV, while other main concepts are the dynamic threshold value. Unlike normal AODV, the RREP_seq no is extra checked whether higher than the threshold value or not. If the value of RREP_seq no is higher than the threshold value, the sender is regarded as an attacker and updated it to the black list. The ALARM is sent to its neighbors which includes the black list, thus the RREP from the malicious node is blocked but is not processed. This sequence number threshold is calculated by average of tables entries sequence numbers in a certain period of time. According to this scheme, the black hole attacks not only be detected but also prevented by updating threshold which responses the realistic network environment.

Advantages

- Main benefit of this method is simplicity.
- On the contrary of other methods, no energy is consumed for monitoring.

Disadvantages

DPRAODV simply detects multiple black holes rather than cooperative black hole attack.

- This method may also make mistake when a node is not malicious, but according to its higher sequence number may be entered into blocked list.

- This process takes a considerable amount of time to notify all nodes for a large network in addition to the network overhead that can be caused by ALARM broadcast

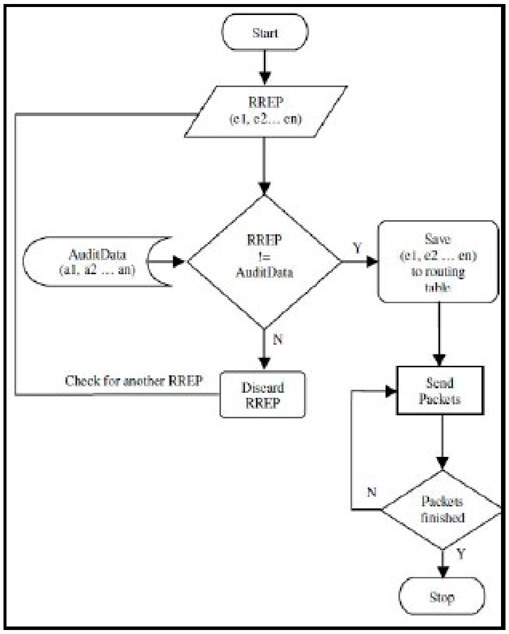


Figure 5: Flowchart of Intrusion Detection by IDAD

IDAD Scheme

In [10] authors Alem, Y.F et al. proposed a solution based on Intrusion Detection using Anomaly Detection (IDAD) to prevent attacks by the both single and multiple black hole nodes. IDAD assumes every activity of a user can be monitored and anomaly activities of an intruder can be identified from normal activities. To find a black hole node IDAD needs to be provided with a pre-collected set of anomaly activities, called audit data. Once audit data collected and it is given to the IDAD system, which is able to compare every activity with audit data. If any activity of a node is out of the activity listed in the audit data, the IDAD system isolates the particular node from the network.

<u>Advantages</u>

- The reduction of the number of routing packets in turn minimizes network overhead and facilitates a faster communication.

- To avoid false positive alarms of intrusion detection, this technique checks multiple anomaly conditions.

Disadvantages

- Neighbour nodes may give false information.

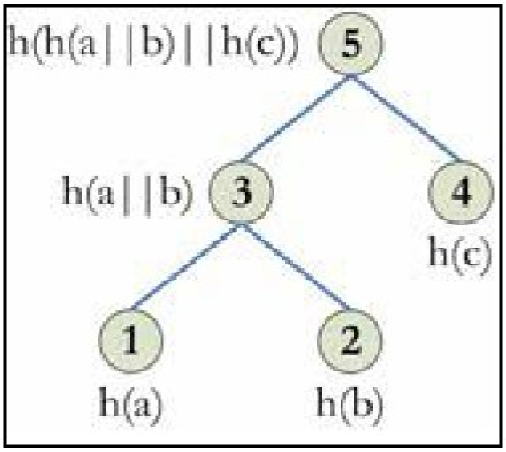


Figure 6: Merkle tree example

Merkle Tree Method

Main idea of [11] is using of Merkle tree. Merkle tree is a binary tree which each leaf contains a hash value and intermediate nodes use leaves hash values to create a new combined hash. Fig. 6 shows this process in one Merkle tree.

h denotes a one-way hash function. For e.g. , the function SHA-1 [12]. | is the concatenation operator. Values of leaves 1,2,4, respectively, are: h(a), h(b), h(c).The value of the interior node 3 is: h(h(a)|h(b)) which is the hashing result of the concatenation of values of children 1 and 2. Idem for the node 5 whose value is h(h(h(a)||h(b))||h(c)) and children are: 3 and 4.

For detecting black hole attack, each node contains a hash which is combination of nodes id and a secure value that only the node knows. Source node has concatenation of all hashes of one route to destination in its memory. The procedure of checking hash values is showed in figure. In the Fig. 7, each node sends concatenation of its hash and previous nodes in route with RREP packet from destination to source. Source node compares this value with prior saved hash value of this route in its memory and if any differences found, it then informs other nodes about maliciousness of this route. Difference between saved value and new value shows that one node may drops RREQ packets and does not send packets to destination that does not have correct value.

Advantages

- In this method all nodes do not monitor each other so a lot of energy is not consumed for monitoring.
- Detecting cooperative black hole attacks is another benefit of this scheme.

Disadvantages

- If a secure constant value is considered for hash, malicious nodes in the path after a time period can drop packets easily and do not send them to destination, because its hash is constant and does not have any guarantee for detecting attacks.
- This method does not refer to how source node first gathers concatenated hash value of all route values.
- If calculation process of hash is performed all the time, the huge overhead is created.

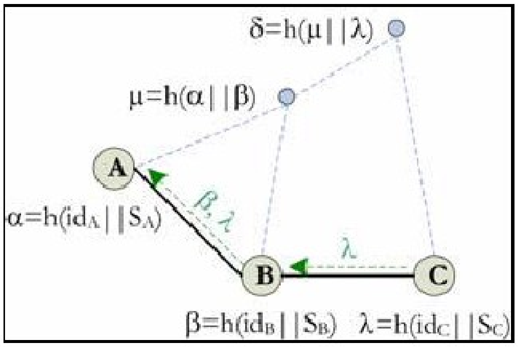


Figure 7: Merkle tree Detection Process

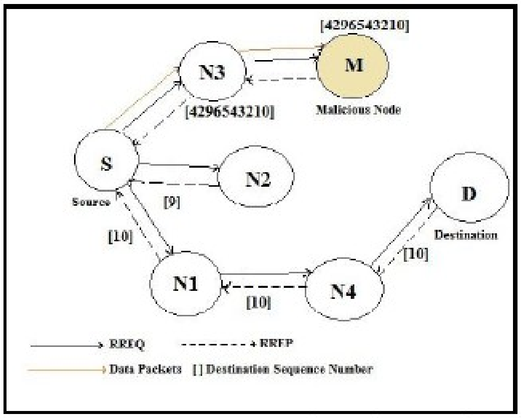


Figure 8: AODV Protocol Packet Exchange

Sequence Number Comparison Scheme

Lalit Himral et al [13] have proposed 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 or intermediate node who has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely it is from the malicious node, immediately remove that entry from the RR-Table.

Destination Sequence Number [14] is a 32-bit integer associated with every route vand is used to decide the freshness of a particular route. The larger the sequence number, the fresher is the route. In Fig 8, Node N3 will now send it to node. Since node N1 and node N2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3 is also expected to be received by node M (assumed to be a malicious node). Thus, node M being malicious node, would generate a false RREP control message and send it to node N3 with a very high destination sequence number, that subsequently would be sent to the node S. However, in simple AODV, as the destination sequence number is high, the route from node N3 will be considered to be fresher and hence node S would start sending data packets to node N3. In this method before sending data packets firstly source node will check the difference between sequence numbers. If it is too large, obviously the node will be a malicious one, and it will be isolated from the network. Otherwise it simply transfers the data packets to the destination node.

Advantages

- This solution may be used to maintain the identity of the malicious node as MN-Id, so that in future, it can discard any control messages coming from that node.

Disadvantages

- This method cannot find multiple black hole nodes.

Observation And Analysis

The various solutions to black hole attacks are analyzed and made a comparison based on different criteria and depicted in Table 1.

Schemes	Introduced new packets (yes/no)	Modifies AODV (yes/no)	Detection type	Drawbacks
DRI & Crosschecking	yes	yes	Co-operative black hole	Memory overhead
Dynamic learning	no	no	Single black hole	High false alarm rate
DPRAODV	yes	no	Single black hole	Time Delay Routing overhead
IDAD	yes	no	Multiple black hole	Cannot detect new types of attacks
Merkle tree	no	no	Co-operative black hole	Huge overhead
Sequence no: comparison	no	yes	Single black hole	Sequence no: limit overhead

Table 1: Comparison Chart

Conclusion And Future Scope

Black Hole Attack is a main security threat that affects the performance of the AODV routing protocol. Its detection is the main matter of concern. Due to the inherent design disadvantages of routing protocol in MANETs, many researchers have conducted diverse techniques to propose different types of prevention mechanisms for black hole problem.

This paper has consolidated various works related to black hole attack detection methods in AODV-based MANETs and pointed out their advantages and disadvantages and at the end, we compared these methods from some aspects and observe that the mechanisms detects black hole node, but no one is reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations. For future work, to find an effective solution to the black hole attack on AODV protocol.

Acknowledgement

The authors wish to thank the reviewers and the editors for their valuable suggestions and comments that helped improve the paper.

Reference

1. H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," Wireless Communications, IEEE, vol. 11, no. 1, pp. 38–47, 2004.
2. P. Goyal, S. Batra, and A. Singh. A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications IJCA, 9(12):24–28, 2010.
3. M. Abolhasan, T. Wysocki, and E. Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1):1–22, 2004.
4. C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on. IEEE, 1999, pp. 90–100.
5. G. Sandhu and M. Dasgupta. Impact of blackhole attack in manet. International J. of Recent Trends in Engineering and Technology, 3(2), 2010.
6. EO Ochola and MM Eloff. A review of black hole attack on aodv routing in manet. 2011.
7. H. Weerasinghe and H. Fu. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In Future generation communication and networking (fgcn 2007), volume 2, pages 362–367. IEEE, 2007.
8. H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato. A dynamic anomaly detection scheme for aodv- based mobile ad hoc networks. Vehicular Technology, IEEE Transactions on, 58(5):2471 –2481, jun 2009.
9. P.N. Raj and P.B. Swadas. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. Arxiv preprint arXiv:0909.2371, 2009.
10. Y.F. Alem and Z.C. Xuan. Preventing black hole attack in mobile ad-hoc networks using anomaly detection.In Future Computer and Communication (ICFCC), 2010 2nd International Conference on, volume 3, pages V3–672. IEEE, 2010.
11. A. Baadache and A. Belmehdi. Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks. Arxiv preprint arXiv:1002.1681, 2010.
12. D. Eastlake and P. Jones, "Us secure hash algorithm 1 (sha1)," 2001.

13. 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.
14. M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks," in Network Protocols Ninth International Conference on ICNP 2001.IEEE, 2001, pp. 14–23.