Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol.3, No.9, 2013
www.iiste.org

A survey on mitigation methods to Black hole Attack on AODV routing protocol

Amin Mohebi
Faculty of Computing and Technology, Asia Pacific University of Technology and Innovation. (UCTI), Malaysia
Tel: +6-018-666-3947 amin_524@me.com

Prof.Dr.simon scott
Faculty of Computing and Technology,
Asia Pacific University of Technology and Innovation. (UCTI), Malaysia
Simon@apu.edu.my

Abstract

AODV is a routing protocol that is designed for MANETs and it is using the on-demand routing method to establish the routes between nodes. The main benefit of this protocol is establishment of desired routes to destination when the source node requires and it keeps the routes as long as they are needed. The black hole attack is a common attack that can be accrued in AODV protocols. In this kind of attack, the attacker uses of one or more malicious nodes which advertise themselves in the network by setting a zero metric to all the destinations that causes all the nodes toward the data packets to these malicious nodes. The AODV is vulnerable against black hole attacks due to having network centric property, where all the nodes have to share their routing tables for each other. In this paper, we present the survey of existing mitigation methods that have been proposed to secure AODV.

Keywords: Mobile Ad hoc Network (MANET); Black hole attack; Cooperative Black hole attack; Ad-hoc On-demand Distance Vector (AODV).

1. Introduction

Mobile Ad-hoc Network is a group of mobile nodes without any fixed infrastructure therefore the nodes communicate with each other based on the unconditional trust. The security is more complicated in MANET when compared with ordinary network which the intruder may get physical access to the wired link or pass over security holes at firewalls and routers. Mobile ad hoc network does not have a well-defined line of protection due to its infrastructure-free and each node shall be prepared for any threat. In wireless ad-hoc networks, the most important concern is routing issues. Actually, the old-fashioned techniques are not suitable in MANETs thus there is a need to modify current TCP/IP model to provide efficient functionality which has been made the routing protocols as key research area for investigators and challenging task as well. There are various routing protocols in MANET which are categorized in term of functionality as following: reactive protocols, proactive protocols and hybrid protocol. Reactive protocols are known as On Demand Reactive protocols which never initiate route discovery, unless they are requested by a source node. Proactive routing protocols maintain the updated topology of the network and each node knows the other nodes in the network in advance. Hybrid protocol is created by exploiting the benefits of both reactive and proactive protocols which could be used to achieve better results. These protocols suffer various attacks that advertise themselves in the entire network. (i.e. black hole attack, worm hole attack, gray hole attack, etc) In this paper, the aim is to investigate on AODV routing protocols in term of black hole attacks. Black hole is one of the most common attacks against the AODV routing protocol. The black hole attack will disrupt the network and affect the whole network performance. The malicious node in a black hole will pretend to have the shortest and freshest route to the destination node by manipulating the control message to forge other nodes to send their data through its node.

2. Over view of AODV routing protocol

AODV has been considered as reactive protocol which uses control messages (i.e. Route Request message (RREQ),

Route Reply Message (RREP) and Route Error Message (RERR)) to discover a route to destination. This protocol establishes a route when a node wishes to communicate with the other node which it has no route; therefore AODV will offer topology information for the node. Two phases of this protocol are described below.

2.1 Route Discovery

When a source node wishes to transmit data packets, it sends a REEQ to its neighbors. The neighbors act by two ways. If there is an available valid route to destination, they will reply RREP to the source node. But if there is no a valid route, they will rebroadcast RREQ to their neighbors. While transmitting a RREQ packet, every neighbor node enters the previous node's address and its Bid. . A timer associated with each entry is also maintained by the node in an attempt to remove a RREQ packet in case the reply has not been received before it expires. Figure 1 illustrates an example of route discovery mechanism in AODV. Suppose that node "A" wants to forward a data packet to another node (destination) "G". The source node sends a RREQ to its neighbors. As shown, the neighbors do not have an available route to destination hence; the neighbors also forward RREQ to their neighbors until finding a node which has a fresh enough route to destination or destination node is located itself.

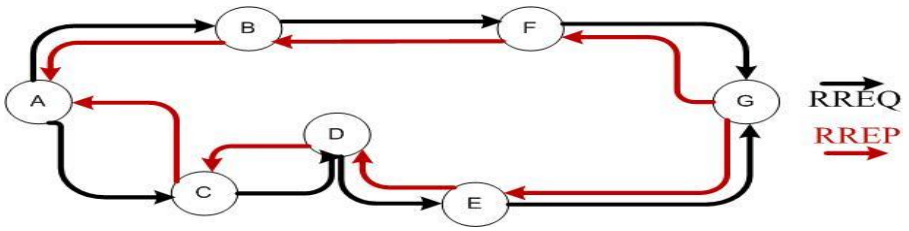


Figure 1. Route discovery in AODV

2.2 Rout maintenance

The route maintenance mechanism works as following: if a node finds a link down that makes one or more than one link inaccessible from the source node or neighbors nodes, it broadcasts an RERR to inform the source node and the end node. This is depicted in figure 2.3 which shows the link between "E" and "G" is broken hence a RERR message will be generated in node "E" and send to the source node to notify this node.

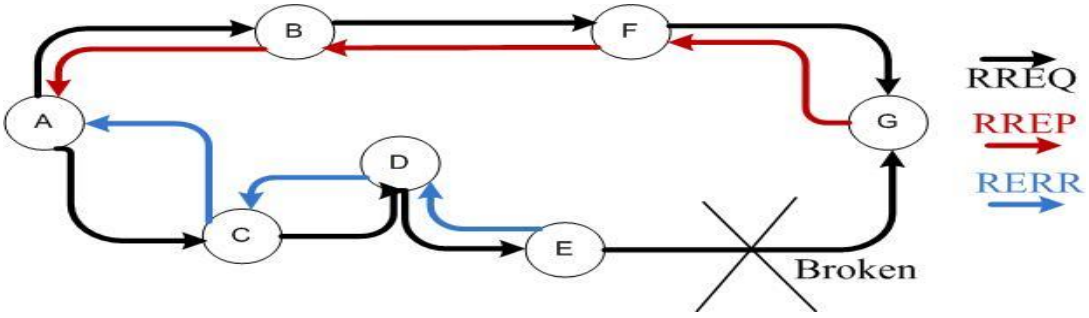
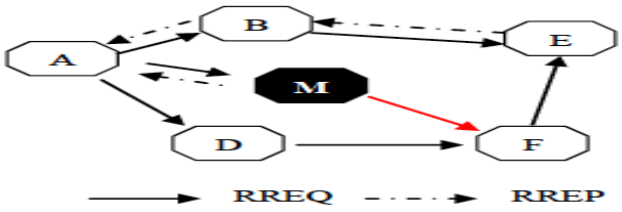


Figure2. Route maintenance in AODV

3. Black hole Attack on AODV Routing Protocol

The black hole attack includes malicious nodes that forge the nodes to drop the data packets. When a source node wishes to communicate with the other nodes or transmits the data packets to the destination, it sends a RREQ to its neighbors to know the true path to the destination. If there is one or more malicious node (black hole node), it receives the RREQ then sends a fake RREP to sender which shows malicious node already has a true path to the destination and this RREP message includes false routing information and fake higher sequence number that shows it is a fresh path. When the sender of RREQ receives the RREP, it assumes the malicious node as true node then it transmits the data packets within the route that specified by black hole node. Black hole nodes receive the data packets without sending the packets to the destination or the other nodes. By creating routing loops, network congestion and channel contention, attackers degrades the network performance. This kind of attack is illustrated in the figure 3. The source node transmits RREQ packets to its neighbor nodes "B" and "D" to discover fresh route to the destination "F". The black hole node "M" immediately respond to the source node without checking its routing

table to say it has a fresh path to the intended destination which is done by sending a fake RREP to the source node "A". The source node "A" considers that the route discovery has been done then rejects other RREP message from other nodes. Then, the attacker will drop the received packets without sending to the destination "F".



. Figure 3: Single Black hole attack

However, in case of multiple black hole nodes which act in coordination the level of detectability is low. In this form of black hole attack, multiple black hole nodes are cooperating with each other to attack the intended node or network. For example, as shown in figure 4, the black hole node "B" is cooperating with black hole node "B2" which is its teammate as the next hop.

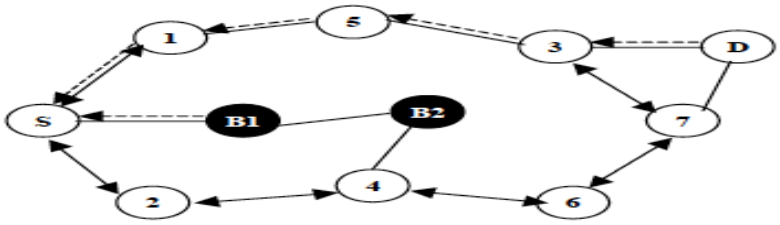


Figure 4. Cooperative black hole attack

4. Solutions to Black hole Attack in MANET

Deng [4] used On-Demand Distance Vector (AODV) and proposed a solution for black holes attacks. This solution related to when an intermediate node applies for RREQ, the RREP packet should be included information about the next hop to destination. Next, the source node sends a further request (FREQ) to next hop of replied node to know about replied node and route to the destination. This approach may help to identify the reliability of the replied node if the next hop is trusted. But the drawback of this solution is related to cooperative black hole attacks on MANETs. This approach could be used for individual attacks but cannot avoid cooperative attacks. For instance, if the next hop also cooperate with the replied node, "yes " which will be replied for both question and the source node will trust on next hop and send data within the replied node that may be a black hole node

Sun Guan and Chen [1] used On-Demand Distance Vector (AODV) as their routing protocol. The detection scheme utilized neighborhood-based technique to discover the black hole attacks and represent a routing recovery protocol to create a reliable route to the destination. They designed a method with two parts to encounter with black hole attack. These parts are included: detection and response. The authors simulated their work by NS2 and the results illustrated that the scheme effectively is able to find black hole attack with no much control overhead to the network. The authors discovered that the amount of passing packet over the network might be enhanced by at least 15% and the false positive possibility will be less than 1.7%. This scheme will be failed to detect black hole attack when that attacker decides to forge the fake reply packets selectively and detection of cooperative black hole attack was the next problem of their solution.

A study has been conducted by Latha Tamilselvan [7] who proposed a solution to enhance the original AODV protocol. This concept was designed by setting timer in the RimerExpiredTable to collect the other request from other nodes when receiving the first request. The packet's sequence number and the received time will be stored in a Collect Route Reply Table (CRRT), calculating the timeout value based on the arriving time of the first route request then it judges the validation of the route based on the threshold value. The author simulated this solution by (GloMoSim) and results indicate that packet delivery ratio was improved with low delay and overhead.

Shurman and Park [10] used two techniques to avoid the black hole attack in mobile ad hoc networks. The first technique will find at least two routes from the source to the destination node. The second technique is related to number of unique sequence used. The authors simulated the proposed approach by NS2 and they confirmed that these techniques have less numbers of RREQ and RREP in comparison with current AODV. Second technique might be better than first technique due to the sequence number which is contained all packet in the original routing protocol. These techniques were failed to discover cooperative black hole attacks.

Chang, Rei Heng, Cheng, and Shun Chao Chang [2] conducted a study on distributed and collaborative procedure which was proposed to detect black hole nodes. This cooperative procedure works as following:Each node finds the local anomalies.The sender node sends a message to the neighbor of the infected node by calling a cooperative detective.Each node gathers information over overhearing packets to recognize the suspicious nodes, when recognizing one, the detecting node will initiate the local detection procedure to evaluate whether the suspicious one is a malicious black hole node. If one node is confirmed as a black hole node, the global reaction will notify the entire of network by sending a warning message. This solution used of the voting scheme which means participating all the nodes to vote to a infected node. This approach help to detect the individual black hole nodes but when an attacker uses cooperative black hole node to impersonate the nodes the voting scheme and detection of cooperative attacks will be complex and impossible.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto [12] proposed a dynamic learning approach to find black hole attack in MANET. This method was intend to observe the characteristic change of node within a given time and a node will be recognized as black hole node if its characteristic change goes over the particular time. The Characteristics will be observed in the number of sent RREQs and the number of received RREPs and the mean destination sequence numbers of RREQs and RREPs. This approach is not able to isolate the black hole nodes due to absence of detection mode such as revising the AODV protocol. Moreover, this comes with bigger processing overhead and the determination of optimal threshold values remains unresolved.

Payal , Swadas [11] used AODV as their routing protocol by proposing a dynamic learning system to detect black hole attack based on MANET to avoid black hole attack by notifying the other nodes in the network. Generally, a node receives RREP packet and it checks first the value of sequence number in its routing table. If the sequence number is higher than the threshold value, it will be considered as malicious node. The threshold value will be dynamically updated in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The authors used of advantage of AODV protocol that the source node announces the black hole to its neighbors in order to be refused and removed. Also, deploying the dynamic learning system improved the average end-to-end delay and normalized routing overhead. However, if a cooperative attack occurs in MANET, detecting process will be too complex so, this solution cannot be used for cooperative attacks.

In a study Djenouri and Badache [5] presented an approach for monitoring, detecting and eliminating the black hole attacks in mobile ad hoc network. In the first phase (monitoring), an effective method of random two-hop ACK was used. The authors used a Bayesian approach for node accusation which was deployed to enable node redemption before judgment. The benefit of this approach is to prevent false accusation attacks vulnerability and reducing the false positives which can be occurred by channel conditions and nodes mobility. This approach might be used for all types of packet droppers, selfish and malicious nodes that cause a black hole attack. This solution was able to detect attacker when dropping the packets. The authors used GloMoSim simulator to simulate their approach and they stated that the random two-hop ACK would be considered as effective as the normal two-hop ACK in high true and low false detection but greatly decreasing the overhead more than ordinary two-hop ACK. This approach used cooperatively witness-based verification however, it not able to prevent to collaborative black hole attacks and multiple malicious nodes.

Hesiri Weerasinghe [6] used a methodology to detect multiple black hole nodes that working collaboratively as a collection to begin cooperative black hole attacks. Actually, this author used Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP) to produce a slightly modified version of ADOV protocol. In this paper, the focus has been on the cooperative black hole attacks in MANET routing.

This solution has been compared with the currently available solution proposed by Deng **(**op. cit.**)** and also the performance of both solutions compared with original AODV by QualNet simulator in term of throughput, packet loss rate, end-to-end delay and control packet overhead. The author confirmed that original AODV and solution proposed by Deng **(**op. cit.**)** deeply suffer from multiple black hole attacks and this new solution can present better performance in compare to the previous solutions in term of throughput rate and minimum packet loss. However, this solution also could not solve completely cooperative attacks.

Rutvij, Sankita and Devesh [13] investigated on some of the existing approaches for black hole and gray hole attack and presented a novel solution against these attacks which is able to find effectively short and secure routes to destination. Their theoretical analysis illustrated that this approach properly can increase packet delivery ratio (PDR) with negligible difference in routing overhead. The authors believed that this algorithm could be used for the other reactive protocol and also finds and eliminates malicious
nodes within the route finding phase. Nodes receiving RREP confirm the truth of routing information; source node broadcasts a list of malicious nodes when sending RREQ. Nodes update route tables when they get any information of malicious nodes from received routing packets. No additional control packet can be mentioned as benefit of this algorithm and there is minor difference in routing overhead which is the ratio of the number of routing related transmissions to the number of data related transmissions. Additionally, the malicious nodes would be isolated and packet delivery ratio (PDR) will greatly be improved.

5. Comparison of Various Solutions to Black hole Attack

The various solutions to black hole attacks proposed by several authors are analyzed and made a comparison based on important parameters and depicted in Table 1.

The detection techniques which make use of reactive routing protocols have low overheads, but have high packet loss problem. Most of the discussed solutions, in particular Method1, Method2, Method3, Method4, Method 5, Method 6, Method 7 and Method 8 suffer to detect cooperative black hole attacks. The authors did not focus on the behavior of black hole attacks when they are cooperating in a group. In contrast, Method9 and Method10 present good performance in terms of throughput and minimum packet loss percentage compared to other solutions and original AODV which is affected by cooperative black holes. Based on performance results shown in Table 1, we can conclude that Method9 and Method10 outperform the other detection methods. However simulating more features could increase one's detection rate, the feature-selection activity can be computationally expensive on the node itself. Hence, understating both performance and cost impacts of proposed solutions is an important task which helps to find out the method best suited to the specific requirements of the operational environments.

6. Conclusion

This paper has focused on the numerous researches done in term of black hole attack on AODV-based MANETs. There are several proposals for detection and mitigation of black hole attacks in MANETs. However, most of solutions are not properly working against single black hole attacks and they suffer of detection of cooperative black hole attacks. The author has made a comparison between the existing solutions, but there is no reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations. In conclusion, the author recommends that using the hybrid techniques could be a proper way to detect cooperative black hole attacks. For future work, to find an effective solution to the black hole attack on AODV protocol which can be proposed via simulation to give better network performance in terms of various network parameters like Packet Delivery ratio, End to End Delay, throughput, and mobility.

Table 1: Comparison of available solutions

Technique proposed by	Techniques / Solutions	Routing protocol	Introduced new packets (yes/no)	Modifies AODV/ Routing tables(yes/no)	Type of attack	Results
Deng,2002	Further request (FREQ)	AODV	yes	No	Single Black hole	Routing overhead, Cannot prevent cooperative black holes.
Sun Guan and Chen,2003	Neighborhood based technique	AODV	No	No	Single Black hole	Not able to detect cooperative attack
Shurman , Yoo S, Park ,2004	Using two novel techniques	AODV	Yes	Yes	Single black hole	Time delay
Satoshi Kurosawa, 2007	Dynamic learning approach	AODV	Yes	Yes	Single Black hole	Bigger processing overhead
Tamilselvan L, Sankaranarayanan V (2007)	Time-based Threshold detection Scheme	AODV	Yes	No	Single black hole	The increase of end-to-end delay when the malicious node is away from source node
Chang,Tung-Kuang (2007)	Voting scheme	AODV	Yes	Yes	Single black hole	Not able to detect cooperative attack
Djenouri and Badache (2008)	Random Two- hop ACK and Bayesian Detection Scheme	AODV	Yes	Yes	Single black hole	Not able to detect cooperative black hole attack
Payal,Swadas,2009	Dynamic learning system	AODV	Yes	Yes	Single black hole	Improve the average end to end delay and normalized routing overhead

Hesiri Weerasinghe, 2011	Data Routing Information (DRI) table and cross checking	AODV	Yes	Yes	Cooperative black hole	Better performance in compare with Deng (op. cit.) and ordinary AODV
Rutvij, Sankita and Devesh (2012)	Using intermediate node to detect malicious node	AODV	Yes	Yes	Cooperative black hole	Improve Protocol Delivery Ratio (PDR)

7. Reference

[1]. Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch "Detecting Black-hole Attack in Mobile Ad Hoc Network". 5th European Personal Mobile Communications Conference, Glasgow, April 2003 Volume 492, Issue, 22-25 pp. 490 – 495.

[2]. Chang Wu Yu, Wu T-K, Cheng RH, Shun chao chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Network", Emerging Technologies in knowledge Discovery and Data Mining, Vol. 4819, Issue 3, pp 538-549,2007.

[3]. Deng H, Li W, Agrawal DP (2002) Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine 40(10):70–75. doi: 10.1109/MCOM.2002.1039859.

[4]. Djenouri D, Badache N (2008) Struggling Against Selfishness and Black Hole Attacks in MANETs. Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6.

[5]. Hesiri Weerasinghe , 2011, on Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks Proceedings of the IEEE International Conference on Communications, Jun. 24-28

[6]. Latha Tamilselvan & Sankaranarayanan, V. (2007). Prevention of Blackhole Attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) Pages 21-27.

[7]. Mahmood Salehi and Hamed Samavati. (2011). Simulation based Comparison of Ad hoc Reactive and Proactive Algorithms Under the Effect of New Routing Attacks. *2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies*. 6 (2), p100-105.

[8]. Mohammad AL-Shurman,Seon-Moo Yoo and Seungiin Park," Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04,April 2-3,2004,Huntsville,AL,USA.

[9]. Mahmood Salehi and Hamed Samavati. (2011). Simulation based Comparison of Ad hoc Reactive and Proactive Algorithms Under the Effect of New Routing Attacks. *2012 Sixth International Conference on Next Generation Mobile Applications, Services and Technologies*. 6 (2), p100-105.

[10]. Payal N. Raj, Prashant B. Swadas "DPRAODV: A Dyanamic Learning System against Blackhole Attack in Aodv Based Manet" IJCSI International Journal of Computer Science Issues, Vol. 2, pp 54-59 2009

[11]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, 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, Nov. 2007

[12]. Rutvij H. Jhaveri , Sankita J. Patel. (2012). DoS Attacks in Mobile Ad-hoc Networks: A Survey. *2012 Second International Conference on Advanced Computing & Communication Technologies*. 2 (2), p535-540.