International Journal of Computer Applications Technology and Research
Volume 2– Issue 6, 686 - 689, 2013, ISSN: 2319–8656

Presenting a New Method for Detection and Prevention of Single Black Holes Attack in AODV Protocol in Wireless Ad Hoc Network

Iman Zangeneh
Department of Computer Mathematics,
Science and Research Branch,
Islamic Azad University,
Mahshahr, Iran.

Sedigheh Navaezadeh
Sama Technical and Vocational Training College
Islamic Azad University
Mahshahr Branch,
Mahshahr, Iran

Abolfazl Jafari
Department of Computer,
Science and Research Branch,
Islamic Azad University,
Sari, Iran.

Abstract: There is no infrastructure in wireless ad hoc networks, and nodes independently manage the networks. Therefore, the connection between nodes is provided by the nodes themselves, and these nodes act as a router. In this case, they use routing protocol such as AODV. In order to provide the connections, nodes exchange data and control packages by trusting to each other. Since these networks have unique and special characteristics, they face with too much attack. One of these attacks is black hole attack in which destructive node attracts the network traffic, and destroys the packages. In this paper, black hole attack in AODV routing protocol has been investigated, and some solutions have been suggested. Simulation results indicate that, in proposed method, the rate of package delivery has been considerably increased in comparison with AODV.
Keywords: wireless ad hoc network, simulation, black hole attack, intrusion detection system, NS2 simulator.

1. INTRODUCTION

Wireless ad hoc networks are composed of independent nodes managing the networks without any infrastructures. In wireless ad hoc networks, topology is dynamic, and nodes can freely enter the networks or leave it. In these networks, the connections between the nodes is wireless. Due to this advantage, these networks are available in places where establishing wireless networks is not possible. Wireless ad hoc networks can be used in impassable or mountainous areas and battlefields where the soldiers can communicate with each other. Also, they can be used in natural events such as flood or earthquake. Since there is no fixed infrastructure in these networks, nodes act as a host and router [1; 2; 3], and they use different routing protocols in routing process such as AODV [4; 5]. Finding the route and sending the packages are performed in the network by the nodes themselves on the basis of mutual trusting. Due to the characteristics of wireless ad hoc networks such as lack of fixed infrastructure and the trust of nodes to each other, these networks are exposed to attacks. One of these attacks is black hole attack. In this attack, destructive node uses the vulnerability of routing packages in on-demand protocols like AODV, and attracts the network traffic. Finally, it destroys all packages. In AODV routing protocol, when the source node demands a route toward destination, middle nodes are responsible for detecting the route. In order to do this task, they send route demand packages to neighbors. This process continues until destination node or the node that has found a new route toward destination receives the package of route demand [6; 7; 8]. Destructive node does not do this work; rather, it immediately and falsely responses to the source node through which there is a new route to destination. After receiving this response, the source node sends data packages to black hole. Then, the black hole attracts and receives data packages, and destroys them. In this paper, a method has been suggested, and in this method, black hole node is identified in AODV routing, and then it is removed from routing process. In order to identify black hole attack, fidelity level is allocated to each node. Afterwards, fidelity levels of nodes are stored in a table called fidelity table. The network nodes store this table. This table is updated by the source node, and then it is distributed. In this way, other nodes can update their own fidelity table. Through using this table, collecting the responses in response table and changing the way of selecting AODV protocol, black hole node is identified in proposed method, and then it is removed from routing. Simulation results show considerable improvement of package delivery rate in comparison with AODV.

2. AODV ROUTING PROTOCOL

One of the protocols used in wireless ad hoc network for finding the route is routing protocol on the basis of AODV demand. In this protocol, all nodes cooperate with each other to find and discover the route through control messages such as route request (RREQ), route response (RREP) and route error (RERR). The characteristics of AODV are less overhead and less usage of band width due to small size of these packages. In order to be sure that there are no turns in finding and detecting the route, this protocol uses sequence number of destination for each destination entry. The procedure of finding the route by AODV is as follows: when the source node sends data to destination node, it distributes RREQ message, and then neighbor nodes in the source node receive this message. Each middle node investigates its own routing table by receiving RREQ. If there is no new route to destination node, then RREQ is sent to neighbors. This process continues until destination node or middle node that follows a new route toward destination receives RREQ. When RREQ is received by this node, RREQ message is created and sent inversely to source direction. When RREQ message moves in the network, the number of its steps increases by passing through each node. The node sending RREP expands its own routing table according to the number of steps, and then it updates the sequence number of destination node. Each RREQ has an indicator. When a node receives two RREQs with the same indicator, the newer RREQ is removed. In there are two routes toward receiving destination, then the route having maximum sequence number is selected. If sequence

numbers are same, the message with minimum number of steps is selected [9; 10].

3. BLACK HOLE ATTACK

The node performing black hole attack waits until one RREQ is received from neighbor nodes. After receiving RREQ, it, immediately and without investigating its own routing table, responses to the node sending RREQ by sending a false RREP. Black hole locates maximum sequence number and minimum steps in its own RREP. In this way, it deceives the node requesting the route. When the node sending RREQ receives RREP, it assumes that it has discovered the best route; therefore, it sends data packages to black hole. Black hole destroys all packages. Since black hole does not investigate its own routing table, it responses to the node requesting the route before other nodes. If black hole can attract the network traffic, then it provides prevention of service. There are two kinds of black hole attacks; namely, single black hole and cooperative black hole. In single black hole, there is a black hole node in the network, while in cooperative black hole, there is more than one black hole, and they cooperate with each other [11]. In this paper, single black hole attack is investigated.

4.LITERATURE REVIEW

According to [12], in order to discover single black hole attack, middle node sending RREP should introduce the node of next step. Source node sends a frequent request (FREQ) to the node of next step, and asks about responding node. If the node of next step is not destructive, then the accuracy of responding node can be identified. A method has been proposed by [13]. In this method, a request package of route confirmation is sent to next step of the respondent node. In the next step, by receiving request package of route confirmation, it tries to find out whether its routing table has a route toward destination or not. If there is any route, then it sends response package of route confirmation (CREE) to source node. This package involves route information. In this way, it identifies the accuracy of responding node. Overhead of this method is high due to high operations. As suggested by [14], by using timer, the source node waits until receiving several RREPs. Afterwards, RREPs are investigated. RREPs involving common nodes and steps are valid and reliable, and others are unreliable. Unreliable RREPs are not taken into account. According to [15], subversion of responding node can be identified through using survey packages of neighbors. A method has been proposed by [16] to identify cooperative black hole attack. In this method, data routing table (DRI), frequent request package (FREQ) and frequent response package (FREP) are used. There is an entry for each neighbor in DRI kept by node, and this indicates that whether node has been sent by the neighbor or not. The neighbors through which data has been sent are reliable. A method has been presented by [17] to identify black hole in DSR algorithm. In this method, the concepts of watchdog and route evaluator have been added to DSR algorithm. The duty of watchdog is to identify misbehavior of the nodes and to investigate whether the node has delivered packages to next step or not. This method is not efficient in collision conditions. In these conditions, it has the power of less transferring and removing lots of packages.

5. PROPOSED METHOD

In our method, AODV protocol is changed in a way that it prevents black hole attack. In this method, fidelity level is allocated to participating nodes, and this is the basis of nodes' reliability. This fidelity level is changed by the source node on the basis of loyal participation of the nodes. The source node sends RREQ package to neighbors. Afterwards, by using timer, it waits for some seconds to collect RREPs. These responses are collected until the end of timer time, and then they are stored in a table called table of response storage. Equation (1) is used to select the response.

RF=sequence Number*Node's Fidelity Level (1)

Where Sequence Number is available number of sequence in RREP, and Node's Fidelity Level is fidelity level of respondent node. This equation is calculated for each received response. Finally, the response whose RF (RREP's Fidelity) is higher than others is selected. If RF is same in two or more RREPs, then the response having minimum number of steps is selected. After selecting RREP, source node begins to send data packages. When data package is received, destination node sends ACK to the source node, and in this way, fidelity level of responding node increases. By receiving ACK, the source node can increase fidelity level of responding node because it has been proved that it is secure and reliable. Of the source node does not receive ACK after the end of timer time, then it reduces fidelity level of responding node in terms of identifying black hole attack. Fidelity tables are periodically exchanged among participating nodes. Since black hole nodes do not send packages, the source node does not receive ACK from destination node, so the source node immediately reduces fidelity level and does not use the received responses.

Figure 1, 2 and 3 show the way of collecting responses, general distribution of fidelity table and route selection in proposed
method.

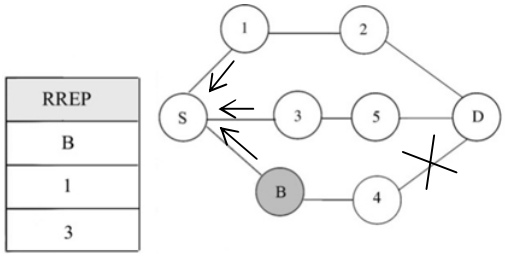

Figure 1: Collecting Responses

As it is observed in figure 1, the source node waits for some minutes after sending RREQ, and received RREPs are stored in response table.

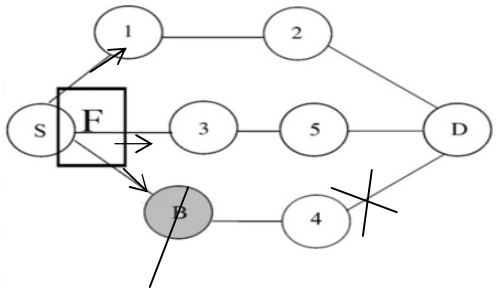

Figure 2: General distribution of fidelity table

Figure 2 shows distribution of fidelity table by the source node. After reducing fidelity level of black hole and distributing fidelity table by the source node, the value of response RF sent by black hole is reduced, and the response sent by black hole is not selected.

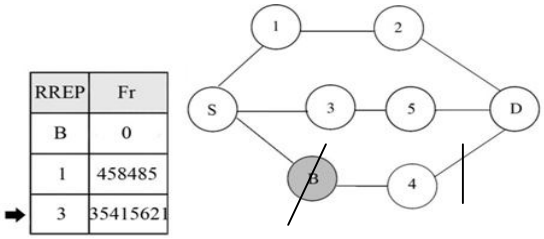

Figure 3: selecting a response

Figure 3 demonstrates the mode in which fidelity level of black hole node as well as its RF is zero. Among the nodes, the response of node 3 whose RF is high is used.

6. SIMULATION RESULTS

NS2 stimulator software has been used for simulation. The measured criteria for evaluating the efficiency of network are as follows: Delivery rate of package: refers to the ratio of the amount of data packages sent by the source node and the number of data packages received in final destination. End-to-end delay average: is delay average between data packages sent by the source node and data packages received by destination. This involves all delays created in the route, frequent delay in MAC layer and etc.

Routing overhead: is the ratio of produced control packages to sent data packages.

The number of nodes in the network is equal to 25 nodes. The perimeter of the network is 700*700 meters. These nodes are located in random places. In the scenario including black hole, one of these nodes is destructive node, and it performs black hole attack. Four traffic currents send data packages in the network with fixed rate. The size of packages is 512 byte. Duration of simulation is 300 seconds. Simulation is performed five times. The speed of nodes' movement toward random destination is different. Simulation results have been shown in the following diagrams. In these diagrams, AODV refers to the network without any black hole node, and routing is performed with AODV protocol. BAODV is a network with a black hole node, and routing is performed on the basis of AODV. FAODV is a network without any black hole node, routing is performed on the basis of proposed method, while BFAODV is a network with one black hole node, routing is performed according to proposed method. In scenario involving black hole node, the performance of proposed method is much better than AODV.

Figure 4: Delivery rate of package with different speeds

Figure 4 shows that when there is no black hole in the network, delivery rate of package in proposed method is lesser than AODV, but when there is a black hole, it has better application.

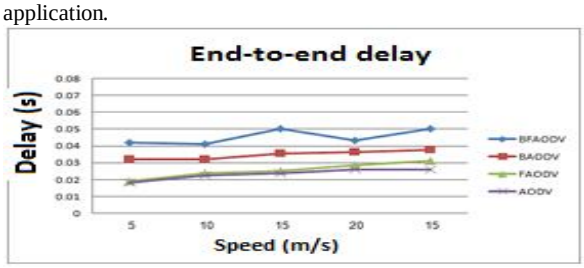

Figure 5: End-to-end delay in various speeds

Figure 5 demonstrates more delay of the proposed method in terms of sending data packages in comparison with AODV. This is due to source waiting to collect RREPs and calculation of the proposed method to select the response.

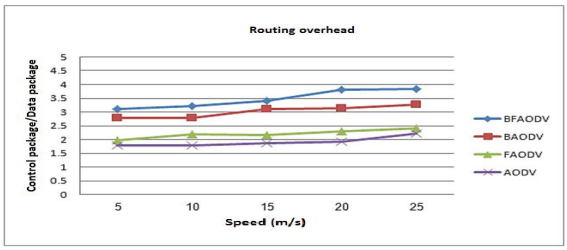

Figure 6: Routing overhead in different speeds

Also, due to much computing and general distribution of fidelity table, routing overhead in the proposed method is more than AODV. Black hole increases overhead due to sending control packages.

7. CONCLUSION

In this paper, a method has been proposed. In this method, according to behavior of black hole, the method of selecting AODV responses changes in a way that the source node ignores the response received from black hole node, and sends data packages from another route. This can be done by allocating fidelity level to network node, changing the way of selecting response, updating and distributing fidelity table by the source node. We simulated five scenarios by NS2 simulator. At first, five scenarios were simulated without a black hole node, and then they were simulated with a black

hole node. The results indicate that our proposed method has increased delivery rate of package from 22,32 percent to 42,34 percent in scenarios involving black hole. In this method, end-to-end delay and routing overhead is more than AODV due to waiting of the source node to collect response packages, more processing in comparison with AODV as well as general distribution of fidelity table.

8. REFERENCES

[1] H. Deng,.W. Li, and D. P. Agrawal, . 2002 Routing security in ad hoc networks, IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct.

[2] S. Lee, B. Han, and M. Shin, Robust routing in wireless ad hoc networks, in ICPP Workshops, pp. 73, 2002.I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. NewYork: Academic, 1963, pp. 271–350Zachman, John A., "A Framework for Information Systems Architecture", IBM Systems Journal, Vol. 26, No. 3, 1987.

[3] S. Makki, N. Pissinou, H. Huang, 2003 The Security issues in the ad-hoc on demand distance vector routing protocol (AODV), In Proc. of the 2004 International Conference onSecurity and Management (SAM'04), pp.427-432C. E. Perkins, E. M. B. Royer, and S. R. Das, Adhoc OnDemand Distance Vector (AODV) routing, RFC 3561, July.

[4] Y.C. Hu and A. Perrig, 2004A survey of secure wireless ad hoc routing, IEEE Security & Privacy Magazine, vol. 2, no. 3,pp. 28-39, May/June 2004.

[5] M. A. Shurman, S. M. Yoo, and S. Park, 2004. Black hole attack in wireless ad hoc networks, in ACM 42ndSoutheast Conference (ACMSE'04), pp. 96-97,Apr.2004.

[6] Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, Cross-feature analysis for detecting ad-hoc routing anoma-lies, in The 23rd International Conference on Distributed Computing Systems (ICDCS'03), pp. 478-487, May 2003.

[7] Y. A. Huang and W. Lee, Attack analysis and detection for ad hoc routing protocols, in The 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), pp. 125-145, French Riviera, Sept. 2004.

[8] Latha Tamilselvan, Dr. V Sankaranarayanan, Prevention of Co-operative Black Hole Attack in MANET, Journal of Networks, Vol. 3, No. 5, May 2008.

[9] 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.

[10] C. E. Perkins, E. M. B. Royer, and S. R. Das, Ad hoc On-Demand Distance Vector (AODV) routing, RFC 3561,July 2003.

[11] Hesiri Weerasinghe, Huirong Fu, Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks:Simulation Implementation and Evaluation, International Journal of Software Engineering and Its Applications Vol. 2, No. 3, July, 2008.

[12] H. Deng, W. Li, and D. P. Agrawal, Routing security in ad hoc networks, IEEE Communications Magazine, vol.40, no. 10, pp. 70-75, Oct. 2002.

[13] S. Lee, B. Han, and M. Shin, Robust routing in wireless ad hoc networks, in ICPP Workshops, pp. 73, 2002.

[14] M. A. Shurman, S. M. Yoo, and S. Park, Black hole attack in wireless ad hoc networks, in ACM 2nd Southeast Conference(ACMSE'04), pp. 96-97, Apr. 2004.

[15] Mehdi Medadian, M.H. Yektaie and A.M Rahmani, Combatwith Black Hole Attack in AODV routing protocol in MANET, 2009, AH-ICI 2009. First Asian Himalayas International Conference, pp: 1-5, 3-5 Nov. 2009.

[16] Lata Tamilselvan, Dr.V Sankaranarayanan, Prevention of Cooperative Black Hole Attack in MANET , Journal Of networks, Vol. 3, NO. 5, May 2008.

[17] S. Marti , T. J. Giuli, K. Lai, and M. Baker,Mitigating routing misbehavior in mobile ad hoc networks. In mobile Computing and Networking (MOBICOM), pages 255-265,2000.