Journal of Advances in Computer Research
Quarterly ISSN: 2008-6148
Sari Branch, Islamic Azad University, Sari, I.R.Iran
(Vol. 5, No. 1, February 2014), Pages: 13-18
www.jacr.iausari.ac.ir

Investigating the Effect of Black Hole Attack on AODV and DSR routing protocols in Wireless Ad Hoc network

Iman Zangeneh [1], Sedigheh Navaezadeh [2 *] , Abolfazl Jafari [3]

1) Department of Computer,mathematics, Science and Research Branch, Islamic Azad University, mahshahr, Iran

2) Teach in sama technical and vocational training college Islamic azad university mahshahr branch,mahshahr,iran

3) Department of Computer, Science and Research Branch, Islamic Azad University,sari, Iran

zangeneh_i@yahoo.com; snavaezade@yahoo.com; Abolfazl.jm@gmail.com

Received: 2013/08/14; Accepted: 2013/10/05

Abstract

Wireless ad hoc networks are composed of independent nodes managing the network without any infrastructure. The connection between nodes is provided by sending packages and by trusting to each other. Therefore, using efficient and certain protocols is the essential requirement of these networks. Due to special characteristics of wireless ad hoc networks such as lack of a fixed infrastructure, these protocols are exposed to many attacks. One of these attacks is black hole attack. In this attack, the node running this attack attracts data packages by sending a false response to source node and destroys them. In this paper, the effect of black hole attack on DSR and AODV routing protocol in wireless ad hoc network has been studied. The results simulated with NS2 simulator software show the weaknesses and advantages of these protocols when there are black hole nodes in the network.

Keywords: *wireless ad hoc network, black hole attack, AODV protocol, DSR protocol, NS2 simulator*

1. Introduction

In wireless ad hoc networks, there is no fixed infrastructure such as access points, and the nodes inside the network manage the network independently. In wireless ad hoc networks, topology is dynamic. Nodes continuously change their own places. New nodes can easily join the network at any time. In addition, the nodes inside the network can leave the network at any time. In these networks, connection between the nodes is wireless. Also, due to above mentioned characteristics, 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 [4][5]. These protocols are classified into three parts according to retaining discovered routes. The protocols of rotary table retain routing data and information in tables, and general distribution of these tables update routing table of all nodes. On-demand protocols in which route discovery operations are preferred when it is necessary. Combined protocols are a combination of two previous parts. Due to characteristics of wireless ad hoc networks such as lack of a fixed infrastructure and trusting the nodes to each other, these networks are exposed to some attacks. Routing protocols are mostly exposed to these attacks. Black hole attack is one of these attacks. In this attack, destructive node uses the vulnerability of routing protocol, and attracts network traffic, and finally, it destroys the packages.

In this paper, the effect of this attack on two routing protocols; namely, AODV and DSR, is investigated. For this purpose, three criteria; namely, end-to-end delay, routing overhead and delivery rate of packages, are evaluated. The results of this attack in three protocols simulated by NS2 simulator software show the weaknesses and advantages of these protocols in measured criteria.

2. AODV Routing Protocol

AODV is an on-demand routing protocol. In this protocol, routs are not kept in routing table for always, and these tables are not exchanged between nodes. When a node requires a route toward another node, it initiates route discovery operations. After discovering the route, the entry of this route is stored in routing table for three seconds. In these protocols, routing control messages are used such as route request (RREQ), route response (RREP) and route error (RERR). In discovering the routs, nodes cooperate with each other. When the source node is going to connect to destination node, it initiates route discovery operations. In order to do this, it generally distributes RREQ. This message is received by neighbor nodes of source node. Each middle node investigates its own routing table when RREQ is received. If there is a new route toward destination node in its routing table, then it inversely responses to source node by sending RREP; otherwise, it generally distributes RREQ. This process continues until destination node or middle node that follows a new route toward destination node receives RREQ, and in this way, it creates RREP message, and inversely sends it to source node. 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. Each middle node sends RREP when the sequence number of RREQ is smaller than the sequence number of its routing table. 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 [7][8].

1.2 Sequence Number

Sequence number acts as a time stamp. By using sequence numbers, nodes can recognize that sent and transferred information of which node is newer than other nodes. When the nodes send control messages such as RREQ, RREP and RERR, they increase their own sequence number.

3. DSR Routing Protocol

In this protocol, when the source node is connected to destination node, it creates RREQ message, and the source and destination nodes are recognized. Then, this package is generally distributed. If middle nodes do not have any route toward destination node in routing table, then they place information in package header and distribute it generally. Therefore, when message is received by a destination node, it involves information of destination nodes and their sequences. When RREQ is received by a destination node or middle node that has a route toward destination, RREP message is created, and this node inversely sends it from the list of RREQ header to the source node [9]. This method is efficient, but due to high volume of package headers in which information of middle nodes are stored and retained, too much load is imposed to the network, and high bandwidth is required. When the length of route increases, and there are too many nodes in the route, the size of packages increases, because information of many nodes should be included in packages header. When the source node receives RREP package, it can include destination route in data package header (DATA). Therefore, middle nodes know that which package should be sent to which node through this route. For this reason, this protocol is called dynamic source routing protocol. When a node cannot send a package to next node, RERR package is created, and it is inversely returned to the source node. In this way, the source node is informed about route disconnection, and the process of route discovery is initiated. The efficiency of this method decreases when the speed of nodes increases because some routes discovered by the source node in receiving RREP message may be destroyed [10].

4. Black Hole Attack

One of the attacks in wireless ad hoc network is black hole attack. In this case, destructive node waits until it receives RREQ message from neighbor nodes. When destructive node receives RREQ message, it, immediately and without investigating its own routing table, creates a route toward destination by sending a false RREP message. This work is done before sending a proper message by other nodes. Therefore, in requesting node, it is supposed that routing process has ended, and it initiates sending package to a destructive node. In this way, destructive node attacks to RREQ messages. If all routs are discovered and obtained, then all packages will be sent, and destructive node will not send packages and destroys all of them. This is called a black hole similar to real world black hole that swallows everything. In a successful black hole attack, destructive node should be placed in the center of wireless network. If destructive node in false RREP message locates another sacrificed node in its own place, then all messages will be sent to that node. In this way, the scarified node processes all received packages. Black hole attack affects the whole network. Black hole in RREP involves the maximum sequence number and minimum step numbers. In this way, it deceives requesting node of the route, and pretends that interval of destination node is one step. In the node sending RREP, it is supposed that, after receiving RREP, the best route is discovered; hence, data packages are sent to black hole. Black hole destroys all packages. If black hole is successful in attracting whole network traffic, then it provides an obstacle for 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. In this paper, by simulating single black hole attack in DSR and AODV protocols, the effect of this attack on two protocols is evaluated.

5. 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 30 nodes. The perimeter of the network is 1000*1000 meters. These nodes are located in random places. Five 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 results on the basis of various speeds of the nodes 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. DSR is a network without a black hole node, and routing is performed with DSR protocol, while BSDR is a network with a black hole node, and routing is performed on the basis of DSR protocol.

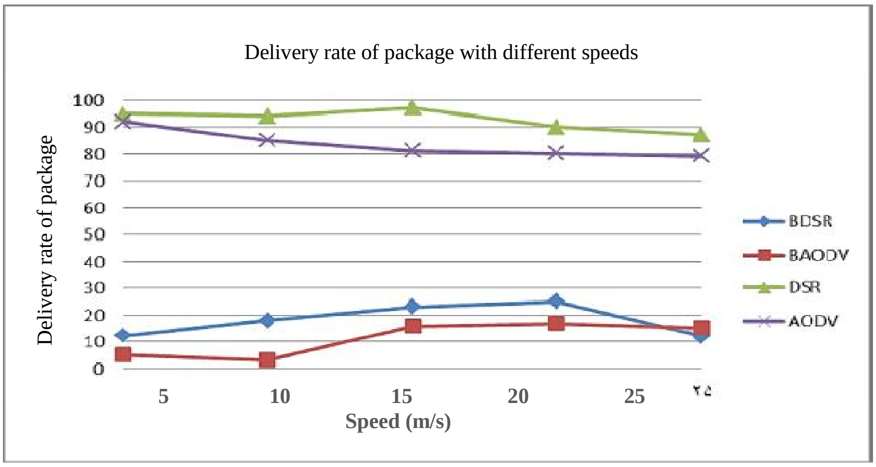

Figure 1: Delivery rate of package with different speeds

Figure 1 shows that when there is no black hole in the network, DSR performs better in terms of sending packages to destination. Black hole attack brings delivery rate of package to a low level in both protocols. However, DSR protocol performs better than AODV when the speed is low.

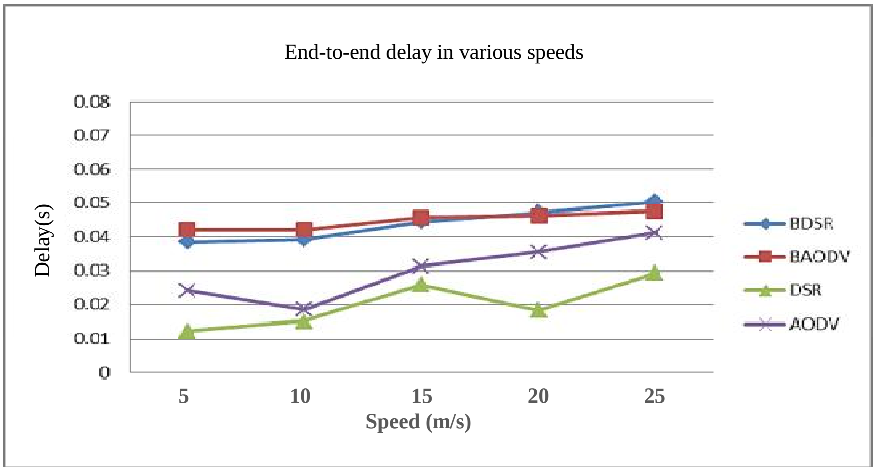

Figure 2: End-to-end delay in various speeds

Figure 2 demonstrates that when there is a black hole, end-to-end delay increases in various speeds. When there is no black hole, end-to-end delay in DSR is less than AODV, while when there is a black hole, this delay is great in AODV protocol in low speeds, and it’s great in DSR in high speeds.

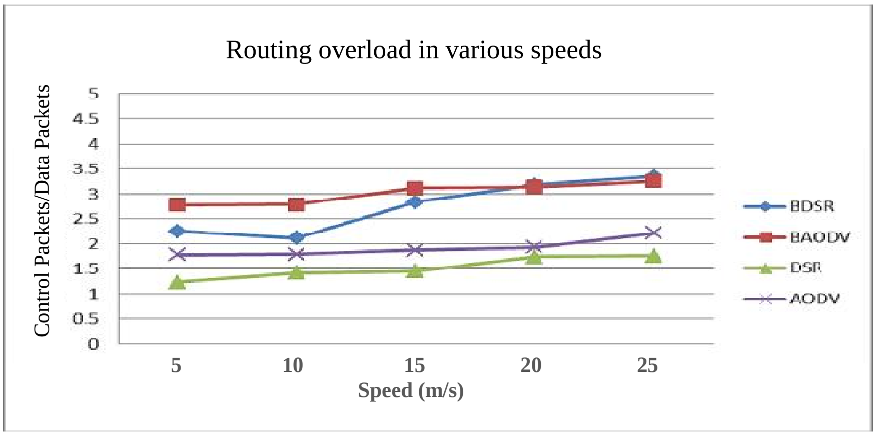

Figure 3: Routing overload in various speeds

Figure 3 shows routing overload in different speeds. When there is a black hole, routing overhead is high due to breaking the links. Routing overhead is great in DSR when the speed is high because routs of the source are mostly destroyed.

6. Conclusion

In this paper, DSR and AODV protocols whose tasks are routing of wireless ad hoc network have been studied. In addition, black hole attack against routing protocols in wireless ad hoc network has been explained, and the effect of this attack on AODV and DSR protocols has been evaluated. Black hole attack in two protocols has been simulated by NS2 simulator software. In order to evaluate black hole attack in various speeds, we simulated 10 scenarios by NS2 simulator. They were firstly simulated without black hole node and then with black hole node. The results indicate that black hole attack has increased delivery rate of package from 65 percent to 82.8 percent in

DSR protocol, and from 65.3 percent to 87.02 percent in AODV protocol. Also, routing overhead and end-to-end delay in two protocols have been increased due to black hole node. By comparing two protocols, it has been shown that DSR performs better than AODV in low speeds and in both modes: without a black hole and with the black hole. However, when speed increases, DSR protocol efficiency gradually decreases.

7. References

[1] 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.

[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, *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 2003.

[4] Y.C. Hu and A. Perrig, *A 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, *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] David B. Johnson and David A. Maltz, *"Dynamic source routing in ad hoc wireless network*", in Mobile computing, T. lmielinski and H. Kmh, Eds, Kluwer, ch.5, 1996.

[10] S.Mohapatra and P.Kanungo, "*Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS Simulator"*, ELSEVIER, procedia Engineering, pp. 69-76, 2012.