2012 International Conference on Computer Networks and Communication Systems (CNCS 2012)
IPCSIT vol.35(2012) © (2012) IACSIT Press, Singapore

CAODV Free Blackhole Attack in Ad Hoc Networks

Watchara Saetang [1] and Sakuna Charoenpanyasak [2]

Center of Excellent in Wireless Sensor Networks (CoE-WSN)

Department of Computer Engineering, Faculty of Engineering

Prince of Songkla University, Hatyai, Songkhla, Thailand

[1] st_watchara@hotmail.com, [2] jsakuna@coe.psu.ac.th

Abstract. Ad hoc networks are the network that having no infrastructure or base station. A node communicates directly to the others with its transmission range. The essential requirement in ad hoc network is the security. The well-known attack is the black hole that having a malicious node advertised itself as a shortest path. This will decrease a throughput of network. In this paper, Credit based on Ad hoc On-demand Distance Vector (CAODV) routing protocol is proposed to detect and eliminate the blackhole attack. The NS-2 simulator has been used to analyze both CAODV and AODV when the blackhole attack is injected in the network. By using our proposed protocol, we can achieve the throughput improvement at about 47 percentages.

Keywords: Ad hoc networks, AODV, Blackhole attack and CAODV

1. Introduction

The infrastructureless is a major characteristic of the ad hoc networks. Each node has communicated as a peer to peer connection and having a direct connection with the neighbor nodes with in their transmission range. The network is a self-configuration that having abilities to discover and maintain the route without manual management. Moreover, ad hoc networks can also perform multi-hop wireless networks.

Currently, several efficient routing protocols have been proposed [1]. Ad hoc On-demand Distance Vector (AODV) [2] routing protocol is widely used in ad hoc networks. AODV is a reactive routing protocol that only requested a route when the node requests. Route discovery operation is used to discover the route by using Route Request (RREQ) and Route Reply (RREP) control messages. When a source node needs to send the data to the destination node, it will broadcast RREQ to the others. When a destination node receives RREQ, the RREP will be returned to the source node. Then, source node receives RREP and uses the information in RREP without checking the correctness of routing information. Therefore, during a route discovery in AODV, the blackhole attack can harm the network easily.

The blackhole attack has a high opportunity to occur in ad hoc networks, especially in the AODV [3]. The blackhole node is easily able to crash the network became each node assumes to be trusted. In the route discovery, the blackhole node replies the RREP with fake information back to the source node, as soon as the RREQ is received. In this case, the source node will take that information to select the route immediately. This leads to pass the data to the destination via the blackhole node. The blackhole attack is one of Denial of Services (DoS), therefore, it is powerful to decrease the throughput of the networks. The several detection blackhole attack methods have been proposed such as the anomaly-based detection techniques [4] and promiscuous monitoring approaches [5]. However, these methods have some weaknesses such as complicate computation and consuming the extra resources.

This paper proposes Credit based on AODV (CAODV) routing protocols to protect the network from blackhole attack. Our CAODV uses credit for checking the next hop node. CAODV will initial a credit to the

next hop node in the route discovery phase. When the existed node in the route table sends one packet, it will decrease one credit of the next hop node. The destination node will send Credit Acknowledge (CACK) to the source node as soon as it receives the data packet. The intermediate node receives CACK and increases a credit of the next hop if the next hop can be trusted. On the other hand, if the destination node cannot receive the data packet and nodes in the path cannot receive CACK, the credit will be decreased to zero. This means the next hop node cannot to be trusted and also be marked as a blacklist node.

The remaining of this paper is organized as follows. The AODV protocol is explained in Section 2. The blackhole attack is described in Section 3. Our proposed protocol named CAODV is introduced in Section 4. The simulation results using NS-2 are analyzed in Section 5 to show the comparison between AODV and CAODV. The last section is the conclusions.

2. Ad hoc On-demand Distance Vector (AODV) routing protocol

The AODV routing protocol is one kind of the reactive routing protocol. The route is thus requested only when needed. A source node broadcasts a RREQ when the data is required to send to a destination node. A route is created when each intermediate node receives RREQ if the intermediate node is not the destination node and never received this RREQ before, it will broadcast the RREQ. The RREP is unicast to the source node when the receiving node is the destination node. The source node will check and choose the shorted path when it receives more than one RREP. The route is only updated if the hop count in RREP is smaller than the existing route in route table. The route discovery operation in AODV shows in Fig. 1.

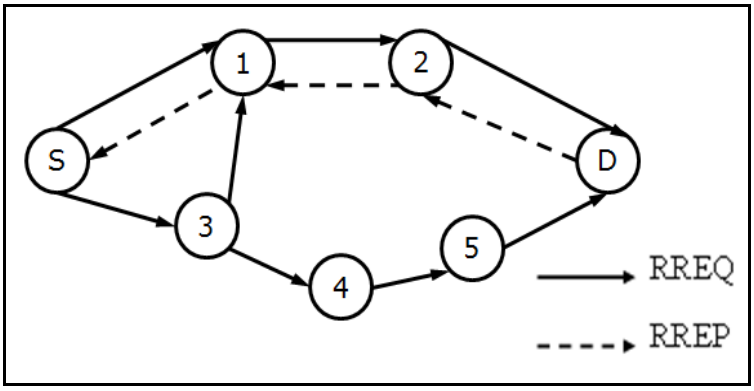


Fig. 1 Route discovery in AODV

From Fig. 1, the example of AODV route discovery is shown. Node S is a source node and node D is a destination node. In this scenario, node S needs to send the data to node D. Node S broadcasts RREQ to its neighbour (node 1 and node 3). Both node 1 and 3 do not have route to node D, therefore they broadcast to its neighbour immediately. This process has been repeated until node D receives RREQ. Node D will unicast RREP back to node S via node 2 and 1, respectively. When node S receives RREP, the communication path to destination is completed.

Another operation in AODV is route maintenance. Route Error (RERR) is used to notify to the source node when route is broken. Route discovery is invoked again. If the route is failed nearly the destination node, the local repair is deployed. AODV is a good routing protocol to manage or discovery the route in ad hoc networks; AODV has more vulnerable to attack. For example, the fake information can be found in RREP if a malicious node pretends to be a destination node and generates RREP to a source node. Because of AODV lacking a mechanism to handle or detect the false information in RRER, this kind of attack can easily occur in ad hoc networks.

3. Blackhole attack in AODV

The blackhole attack is easily to found in AODV routing protocol. The attack is occurred when a route discovery in AODV is used by a source node or a local repair is invoked. Therefore, a source or intermediate node starts to broadcast RREQ to its neighbor. When the malicious node receives RREQ, it sends the fake routing information back to the source node claiming that it is an optimum route. When the source node

receives RREP with the fake route information containing a smallest hop count, the source node will create invalid path to a malicious node. All data packets will be dropped by malicious node when the source node transmits the data. Therefore, a throughput of networks is greatly reduced because of the blackhole attack.

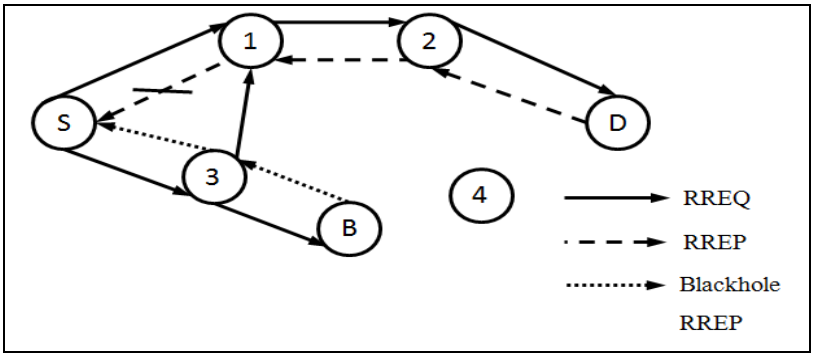


Fig. 2 Blackhole attack in AODV

Fig. 2 shows an example of blackhole attack on AODV in MANETs. Node S is a source node, node D is a destination node and node B is a blackhole node. Node S needs to send data to node D. Then AODV route discovery is used. Node S starts to broadcast RREQ to the neighbour nodes. When node B receives RREQ form node 3, it replies RREP with fake information to node S immediately. In this case, the hop count is equal to 1. When node S receives RREP, it will create the path to node B instead of the destination node. The RREP from node D will be dropped because the hop count of malicious node is smaller than node D. When node S starts to send the data packets to destination, all data will be dropped.

The routing control message in AODV has not been checked in ad hoc networks. Therefore, the blackhole attack is easily occurred and the performances of the ad hoc networks are reduced. H. A. Bala and et al. has studied the impact of blackhole attack in ad hoc networks based on AODV routing protocol. In their experiments, the network consist 20 mobile-nodes and one blackhole node. The result of blackhole attack shows that the packet is dropped up to 90 percentages [6].

Several algorithms to handle the blackhole attack have been proposed recently. For example, K. Lakhani et al. proposed the Watchdog algorithm to check the next hop node that sending the data packet by overhearing all of the packets [7]. By using their solution, the throughput was increased by 10-18 percentages. Unfortunately, nodes in the network have to wake up all-time. This consumed high power dissipation. This consumed both resource and power more than the original AODV. S. khurana proposed Reliable Ad hoc On-demand Distance Vector (RAODV) [8] using Reliable Route Discovery Unit (RRDU). This mechanism was deployed when source node received the multiple RREPs. When a destination receives RRDU, RRDU-reply was replied to the source node. The source node selected the path that having the RRDU-reply. Unfortunately, RAODV cannot detect the blackhole attack when there was only one route to destination. N. Mistry et al. proposed a source node to keep the multiple RREPs for checking information in RREP [9]. When the source node received RREP, the destination sequence number in RREP and the information threshold were compared. However, the blackhole attack can still occur when the destination sequence number and threshold was not different. As we can see, the some algorithms can detect and protect the blackhole but they took a lot of resources. Moreover, in some algorithms the blackhole cannot be solved. Thus, we propose CAODV to get rid of the blackhole attack without consuming the extra resources.

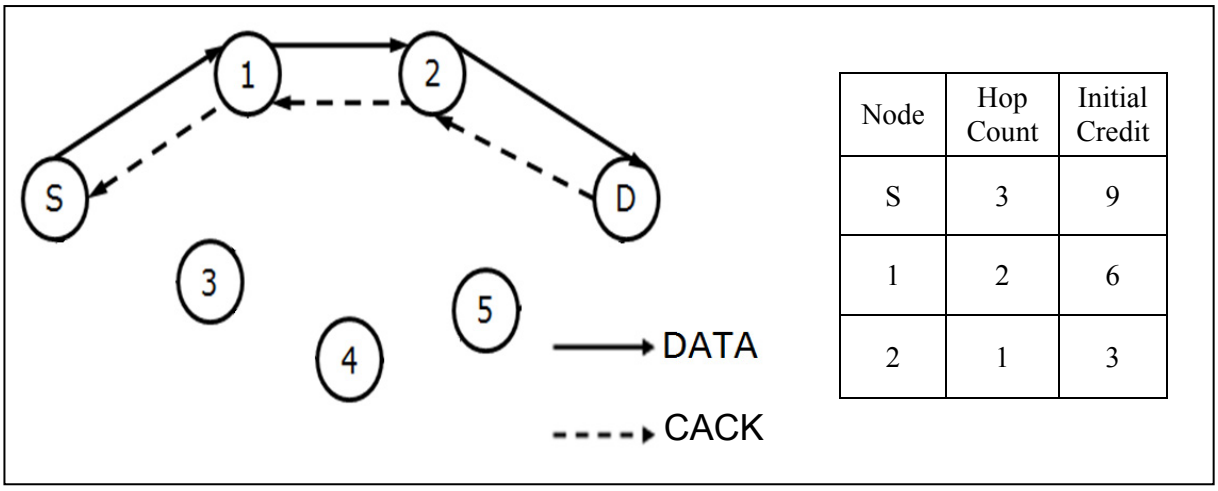
4. The proposed protocol – Credit based on AODV (CAODV)

To protect a blackhole attack in AODV, CAODV is therefore introduced in this paper. We deploy a credit mechanism to check the next hop whether it can be trusted or not. The credit is initiated in a route discovery phase. The credit is defined as followings:

$$\text{Credit} = \begin{cases} \text{Hop count}*3 & \text{; initial state} \\ \text{Credit}+2 & \text{; when destination node sends credit acknowledge} \\ \text{Credit}-1 & \text{; send 1 packet} \end{cases}$$

Note: $\text{Credit}_{Max} = 5*(\text{Hop count}+2)$

At the beginning, a source node broadcasts RREQ to other nodes until a destination node or node having a route to destination replies RREP back to source. The receiving node will assign a credit to the next hop node or who sent RREP. When a node in the path sends one packet, one credit is deducted from the next hop node. As soon as a destination node receives data packet, it will send Credit Acknowledge (CACK) back to a source node. A node within a way back will increase credit of the next hop by 2 to indicate a higher trust level of the next hop. On the other hand, credit will be decreased if a node cannot receive CACK. The node will be untrusted and marked as a blacklist, when a credit reaches zero.



Node	Hop Count	Initial Credit
S	3	9
1	2	6
2	1	3

Fig. 3 Example of CAODV routing protocol

Fig. 3 shows an example of a credit mechanism in CAODV. Node S is a source node that sends data to node D. In this scenario, the route discovery is used and the path contains node S, node 1, node 2 and node D. The credit is initialled by using a hop count multiplied by 3. Thus node 1 is the next hop of node S having 9 credits at the beginning. The credit in node 1 and 2 is decreased by 1 when the data is transmitted to node D. Node D will return CACK back by using the reserved path to source node when the data is received. Node with the path will increase a credit after it receives CACK. Finally, node S adds 2 credits to node 1, when it can receive the data packet. This made the credit of node 1 to be 10 credits. However, the credit has limited to the hop count multiplied 5 to limit the number of data packet when is a malicious node. However, the blackhole attack in CAODV is limited by credit of next hop. When nodes in the path cannot to receive CACK form the destination node, the credit of next hop will become zero. This means the next hop node is blackhole node. The next hop will be a blacklist node. Thus, the packets from a blacklist node will be dropped, eventually.

5. The Simulation Results

This section will show and describe the comparison results of the throughput between AODV and CAODV when the blackhole attack is injected to the networks. This experiment has been done on Networks Simulator2 (NS-2). We declare to use 30 nodes with 2 connections in the networks. In the first connection, there is no attack and start at 10 s. The second connection will have a blackhole attack and start at 20 s. The throughput results of both AODV and CAODV are shown in Fig. 4 and 5, respectively.

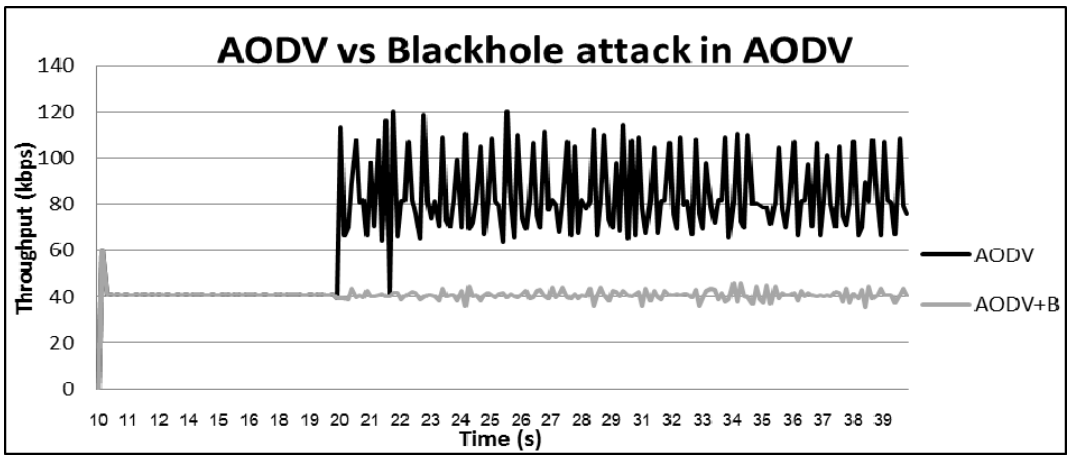


Fig. 4 The comparison of the throughputs between AODV normal operation and blackhole attack

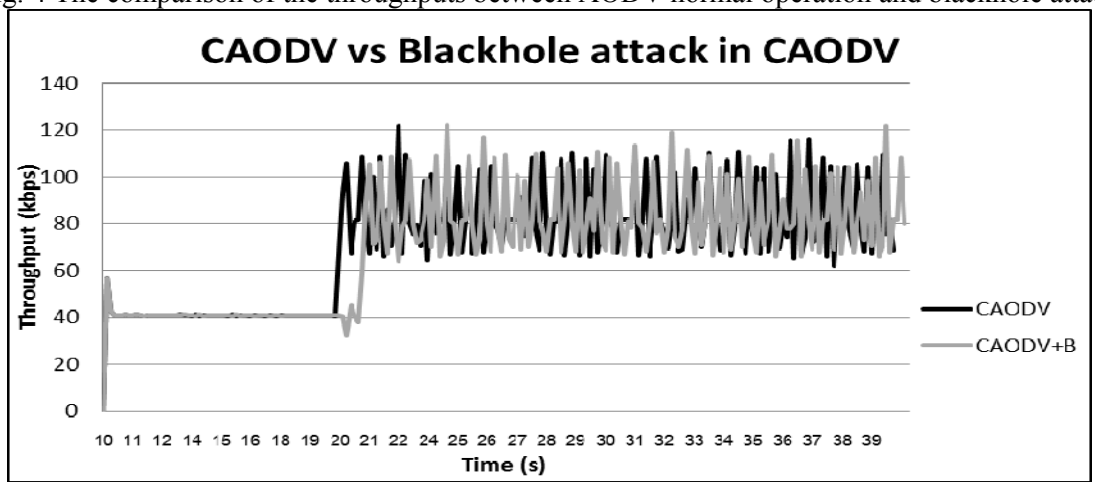


Fig. 5 The comparison of the throughputs between CAODV normal operation and blackhole attack

Fig. 4, the comparisons of the throughputs between AODV with normal operation and AODV with blackhole attack. The average throughput of AODV in normal operation is 70.51 kbps while the blackhole attack has a throughput at 40 kbps. In the scenario of CAODV, a throughput of CAODV with normal operation is 69.89 kbps and when it is attacked by blackhole attack, the average throughput is 69.15 kbps as shown in Fig. 5. From the result in Fig. 5 shows that the blackhole attack cannot harm the network when CAODV is employed. Meanwhile, the blackhole attacks the network that used AODV and decrease throughput at about 47 percentages.

6. Conclusions

According to the nature of AODV routing protocol in ad hoc networks, the blackhole attack is able to harm and decrease a throughput of network, especially in the route discovery phase. Therefore, CAODV has been proposed in this paper. By using a credit mechanism, we can detect and protect a malicious node before the blackhole attack is occurred. We have successful demonstrated that the blackhole cannot attack the networks when our CAODV is employed. In contrast with CAODV, we found the average throughput of the original AODV is decreased at about 40 percentages when the network is attacked by the blackhole.

7. References

[1] S. H. H. N. Ghazani, J. J. Lotf and R. M. Alguliev, "A New Survey of Routing Algorithm in Ad Hoc Networks," 2nd Int. Conf. on Computer Engineering and Technology, vol. 3, pp. 684-688, 2010.

[2] C. E. Perkins and E. M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," Proc. 2nd IEEE Mobile Computer Systems and Applications, pp. 90–100, 1999.

[3] H. Deng, W. Li and D. P. Agrawal, "Routing Security in Wireless Ad Hic Networks," IEEE Communications Magazine, pp. 70-75, 2002.

[4] Y. A. Huang and W. Lee, “Attack Analysis and Detection for Ad Hoc Routing Protocols,” 7th Int. Symposium on Recent Advances in Intrusion Detection, pp. 125-145, 2005.

[5] R. A. R. Mahmood and A. I. Khan, “A Survey on Detecting Black Hole Attack in AODV based Mobile Ad Hoc Networks,” Int. Symposium on High Capacity Optical Networks and Enabling Technologies, pp. 18-24, 2007.

[6] H. A. Bala, R. Kumari and J. Singh, “Investigation of Blackhole Attack on AODV in MANET,” Journal of Emerging Technologies in Web Intellingence, vol. 2, no. 2, pp. 96-100, 2010.

[7] K. Lakhani, H. Bathla and R. Yadav, “A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET,” Int. Journal of Computer Science and Network Security, vol. 10, pp. 40-45, 2010.

[8] S. Khurana, N. Gupta, and N. Aneja, “Reliable Ad-hoc On-demand Distance Vector Routing Protocol,” Int. Conf. on Systems and Int. Conf. on Mobile Communications and Learning, pp. 98-103, 2006.

[9] N. Mistry, D. Jinwala and M. Zaveri, “Improving AODV Protocol against Blackhole Attacks,” Proc. Int. Multi Conf. of Engineers and Computer Scientists, vol.11, pp.1034-1039, 2010.