ISSN 2320 – 2602
Volume 3, No.10, October 2014
International Journal of Advances in Computer Science and Technology
Available Online at http://warse.org/pdfs/2014/ijacst023102014.pdf

A New Technique for Preventing Black Hole Attack in Mobile Ad-hoc Networks

Ankita Chaturvedi[1], **Sanjiv Sharma**[2]
[1]M.Tech Student, Madhav Institute of Technology and Science Gwalior, India, anki_ch26@yahoo.com
[2]Asst. Prof., Madhav Institute of Technology and Science Gwalior, India, er.sanjiv@gmail.com

ABSTRACT

A mobile ad hoc network (MANET) is an infrastructure-less autonomous system in which mobile nodes connected through wireless links are free to move randomly. The characteristics of MANET exhibit more vulnerability to communication related attacks. One of these attacks is Black hole attack. In this paper, the effect of black hole attack on the network performance is analyzed using AODV and IDSAODV routing protocols. A new protocol Improved IDSAODV (IIDSAODV) is also proposed that is a modification of IDSAODV protocol to reduce the effects of black hole attack. Network simulator ns-2.34 is used for the simulation. The packet delivery ratio, network throughput and average end-to-end delay of protocols are calculated and analyzed under black hole attack. A comparative analysis of these protocols is also presented in the paper.

Key words: Mobile ad hoc networks, AODV, IDSAODV, Black hole attack.

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of autonomous nodes that are self-managed. These networks do not need any pre-existing infrastructure and therefore can dynamically be setup anywhere at any time. In these networks, mobile nodes are connected through wireless links and are free to move randomly. At the same time, these nodes also act as routers and this property extends the limited wireless transmission range of each node by multi hop packet forwarding. These networks have applications in various fields like in military and rescue operations where the soldiers are connected by establishing a temporary network at the place which has been collapsed after a disaster like an earthquake.

Mobile ad hoc network has the typical features like unreliable links, frequent changes in topology and lack of incorporation of security features in statically configured wireless routing protocols [1]. These features make mobile ad-hoc networks more susceptible to suffer from the malicious behaviors than the traditional wired networks. Hence, there is a need to pay more attention towards the malicious activities in the mobile ad hoc networks.

There are various possible attacks in the mobile ad hoc network and black hole attack is one of them. In this attack, a malicious node absorbs and then drops all the packets going through it. In case of Ad-hoc On-Demand Distance Vector (AODV) [2] routing protocol, source node initiates the path discovery process by broadcasting a route request packet (RREQ). Intermediate node takes part into this process by further broadcasting this RREQ. A black hole node does not follow this process and sends back a fake route reply (RREP) packet to the source node pretending that it has an optimal path to the destination [3]. Therefore, the source node starts to send its data packets via this malicious node which then drops all the data packets.

This paper is based on black hole attack in wireless adhoc networks. Using network simulator ns-2 (version 2.34) [4], this paper provides effect of black hole attack on the performance of the network. A protocol named BLACKHOLEAODV [5] is implemented that exhibits the black hole behavior in AODV protocol; consequently the performance of the network evaluated using with and without black holes. Result of observation shows, performance of the network deteriorated greatly in the presence of a black hole.

This paper proposed a modification of IDSAODV in form of a solution that ignores the first route reply and imposes a check on the second route reply to reduce the effect of black hole node in an ad hoc network. Ns-2 simulator is employed for evaluating the network performance and it also analyzes the results with respect to existing protocols AODV and IDSAODV [5].

2. RELATED WORK

A lot of work has been done in the field of detecting misbehavior in MANETs. A survey of such schemes is presented in [6-8]. An overview of some schemes for coping with black hole attacks is discussed below:

B. Sun et al. [9] proposed a method that is based on the scheme of detection and response. In detection phase, the neighborhood-based method is used to recognize the black hole attack. Once the attack is detected, it responses against the attack. In response phase, a routing recovery protocol is used to build the correct path to the destination. In recovery protocol, the source node sends a Modify_Route_Entry control packet to the destination node to renew routing path. In this scheme, a lower detection time, higher throughput and accurate detection probability are acquired with no increment in routing control overhead. However, this scheme does not work if the attackers cooperate to forge the fake reply packets.

H. Deng et al. [10] proposed a method to overcome black hole attack that works on the principle of disabling the reply message from the intermediate nodes. In this method, the intermediate nodes are banned from sending out RREP and hence, only the reply from actual destination node is trusted. This modified protocol is based on the assumption that malicious node normally come from intermediate node. This protocol is implemented by modifying the mechanism to generate RREP in AODV protocol. In this modification, the intermediate nodes are not allowed to generate any RREP packet. This method potentially increases the routing delay in large networks and may provide a malicious node the ability to fabricate a reply message on behalf of the destination node.

S. Dokurer [5] proposed idsAODV, which is another modified AODV that is designed to reduce the effect of black hole attack. This method is implemented by modifying the routing update mechanism in AODV protocol. The process to ignore the first establishment route is added to the routing update process. The main strategy is that initially the data is transmitted through first established route but if the second reply message arrives then the data transfer is switched to the second route. This protocol assumes that the first RREP message that arrives at a source node is from a malicious node, and hence ignores this RREP. This method improves the packet delivery but there is also a limitation, for example, if the second RREP message received at a source node comes from a malicious node, it is not able to avoid it.

N. Mistry et al. [11] proposed a solution by modifying the original AODV protocol. In this approach, basically the working of the source node is modified by using an additional function Pre_ReceiveReply(Packet P). A table Cmg_RREP_Tab, a timer MOS_WAIT_TIME and a variable Mali_node are added to the data structures of the AODV protocol. Its basic idea is to store all the RREPs in the Cmg_RREP_Tab table until the time MOS_WAIT_TIME. After completion of this time, the source node analyses all the stored RREPs and discard the one having unexpectedly very high destination sequence number. The node that sent this RREP is suspected to be the malicious node. Once, malicious node is identified, this method selects a reply having highest destination sequence number from Cmg_RREP_Tab table. The identity of the malicious node is stored in the variable Mali._node. Using this identity, any control message from this node can be discarded in the future. All this idea is implemented in the function Pre_ReceiveReply(). To maintain freshness, the Cmg_RREP_Tab is flushed after choosing a RREP from it. Once the malicious node has been detected, the operation of this method works same as that of original AODV. This method has a drawback of increased routing overhead in terms of MOS_WAIT_TIME and execution time of Pre_ReceiveReply().

The EAODV [12] is an enhancement of protocol called ERDA [13]. The main strategy is the assumption that at any point of time the actual destination node will send the RREP. Hence, all previous route entry including from malicious nodes will be overwritten by latest incoming RREP. The updating process will continue until RREP from the actual destination node is received. Subsequently, the process detection and isolation starts to analyze all received RREPs using heuristic method adopted from [14] followed by the process of isolating suspected malicious nodes. EAODV protocol is implemented by modifying the AODV routing update mechanism involving two processes to mitigate the black hole attack; changing the routing update logic expression and adding detection and isolation process. There is also a limitation that EAODV adds two processes in the mitigation methods that cause extra delay and energy usage.

3. PROPOSED WORK

This paper proposes a new protocol by enhancing the existing protocol IDSAODV. IDSAODV works on the principle of ignoring the first established route to reduce the effects of the black hole attack. Since a black hole node always responds with a fake reply without wasting any time, it is reasonable to assume that first route reply will arrive from a black hole node. In IDSAODV, this assumption is taken into consideration. Initially, the data transfer is started with the receipt of the first RREP message but if the second RREP message arrives, the data transfer is switched to the new route. This idea may not work in some cases like if the destination node is nearer than the black hole node then the first RREP message may come from the destination node and the second one from the black hole node. In such a case, the source will send all its data through the second path that is established by the black hole node.

To overcome this problem, a solution is proposed in this paper that is based on the checking of second RREP message and the solution is named as "Improved IDSAODV (IIDSAODV)". IIDSAODV uses the sequence number attribute of AODV protocol to overcome this problem. Sequence number is a 32-bit unsigned integer with the highest value of 4294967295 (HSN). A broadcasted destination sequence number is one of the fields of RREQ message and has been received in the past by the source for any route towards the destination. A received destination sequence number is the sequence number that is received from RREP message [15].

In IIDSAODV, initial working is same as that of IDSAODV. In contrast of IDSAODV, when the source gets a second RREP, it performs a check using the broadcasted and received destination sequence numbers. In the check of second RREP, the difference between the broadcasted and received destination sequence numbers is calculated and compared to the half of the highest possible sequence number (HSN). For passing this check, the difference should be less than or equal to (HSN/2). If the second RREP passes this check, then only the source node will switch to this path. If this check fails, the source node will continue to send its data through the path that is established by first RREP. A scenario of 7 nodes to verify this check is created in which the receiver node is intentionally placed nearer than black hole node so that the first RREP will arrive from receiver node. This scenario is tested with IDSAODV and IIDSAODV in ns-2.

Figure 1 shows the network animation for IDSAODV, it can be seen that the source is sending data to black hole node i.e., second RREP arrives from black hole node and therefore the source switches to second path which is established by the black hole node.

Figure 2 shows the network animation for IIDSAODV in which the source is sending data to receiver node i.e., when second RREP arrives from black hole node with highest destination sequence number, it fails to pass the check and chooses to send the data through first established path.

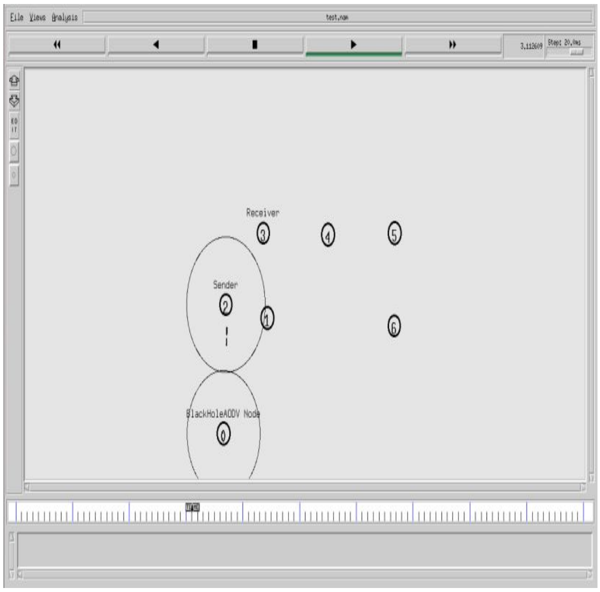

Figure 1: Network Animation for IDSAODV

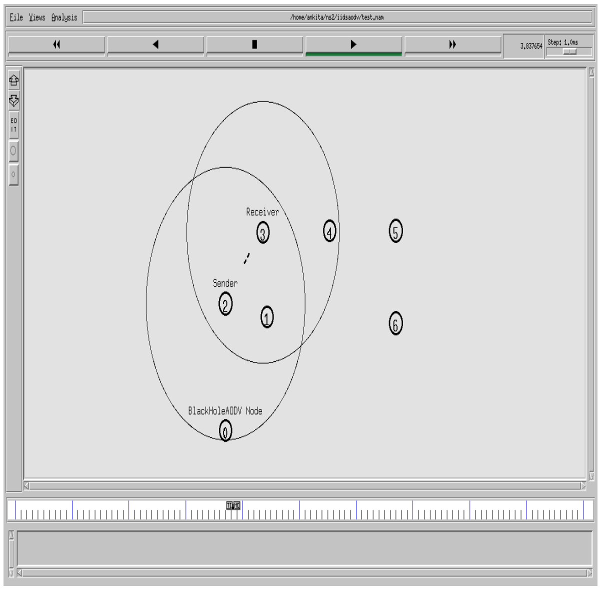

Figure 2: Network Animation for IIDSAODV

To analyze the effect of black hole attack, a protocol "BLACKHOLEAODV" is implemented in ns-2. Node which adopts this protocol behaves like a black hole node. To reduce the effect of black hole attack, IDSAODV and IIDSAODV are implemented. The different network scenarios with varying number of mobile nodes and connections are created. Connections are the number of source-destination pairs in a network. First, we tested these scenarios with AODV protocol without black hole attack. Then in each scenario a black hole node is added by using the BLACKHOLEAODV protocol. These scenarios are used to analyze the performance of networks with AODV, IDSAODV and IIDSAODV. It is analyzed that with IIDSAODV, the packet delivery ratio, throughput and average end-to-end delay of the network is the highest.

3.1 Pseudo code for IIDSAODV

RREP: Route Reply message
RSN: Received destination sequence number
BSN: Broadcasted destination sequence number
Path1: Established by first RREP message
Path2: Established by second RREP message
HSN: Highest possible sequence number (32-bit unsigned integer value i.e., 4294967295)

```
Step1: Source S receives a RREP message (First
       RREP).
Step2: Source S checks its freshness (i.e., RSN >=
       BSN).
Step3: If RSN >= BSN then Source S starts
       transmitting data to Destination D through
       Path1 and set count = 1.
Step4: If Source S receives a second RREP then
       again S checks its freshness.
Step5: If second RREP is fresh (i.e., RSN >= BSN)
       then increase count by 1.
Step6: Source S imposes an extra check on second
       RREP i.e.
       If (count > 1 && ((RSN – BSN) <=
       (HSN/2))), then source S will switch to path2.
Step7: If this check fails, then it means that second
       RREP may be from a black hole node and
       hence source S will continue to send data
       through path1.
```

4. SIMULATION ENVIRONMENT

For the simulation, network simulator ns-2 (ver. 2.34) is used. AODV is used as the basic routing protocol and all the data packets are CBR packets of size 512 bytes. The connection pattern and node movement are generated using cbrgen and setdest utility of ns-2. The parameters that are used for ns-2 simulations shown in the table 1 below:

Table 1: Parameters used for ns-2 simulation

Parameter	Value
Simulator	NS-2 (ver.- 2.34)
Simulation Time	100 s
Number of nodes (n)	10, 20, 30, 40,50
Routing Protocol	AODV
Traffic Model	CBR
Terrain Area	750 x 750
Pause Time	1 s
Maximum speed	20 m/s
Maximum Connection	20% of n
No. of malicious node	1

5. RESULT AND ANALYSIS

To evaluate the packet delivery ratio, throughput and end-to-end delay; simulation is done with varying number of mobile nodes and connections i.e., source-destination pairs. Network simulator ns-2 (version 2.34) is used for the simulation. The awk-scripts are used to calculate the results and these results are plotted using xgraph utility of ns-2. It should be noted that all the analysis and comparison is performed using a single black hole node.

Figure 3 shows the graph for packet delivery ratio of AODV without black hole attack and AODV, IDSAODV, IIDSAODV under black hole attack. It can be seen that under attack, PDR of IIDSAODV is the highest as compared to AODV and IDSAODV. It is analyzed that the presence of a black hole decreases the PDR of AODV by 83.79% which in case of IDSAODV and IIDSAODV, increases by 40.41% and 78.16% respectively. It is obvious that the proposed protocol IIDSAODV improves the PDR by 37.75% as compared to IDSAODV.

Similarly, Figure 4 shows the graph for throughput of the network under same situations as that of PDR. It is analyzed that the presence of a black hole decreases the throughput of AODV by 77.86% which in case of IDSAODV and IIDSAODV increases by 20.66% and 73.59% respectively. It is clear that the proposed protocol IIDSAODV improves the throughput of the network by 52.93% as compared to IDSAODV.

Similarly, Figure 5 shows the graph for average end-to-end delay under same situations as that of PDR and Throughput. It is analyzed that the presence of a black hole decreases the end-to-end delay of AODV by 88.74% which in case of IDSAODV and IIDSAODV, increases by 44.15% and 71.61% respectively. It is clear that the proposed protocol

IIDSAODV increases the end-to-end delay by 27.46% as compared to IDSAODV.

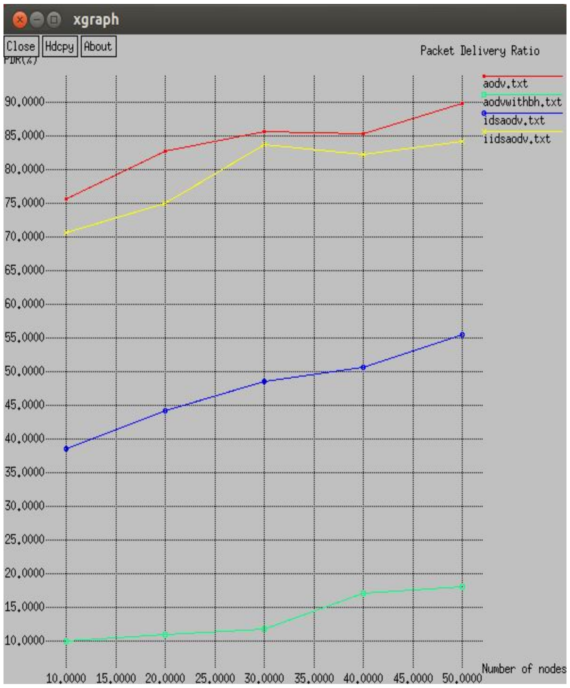

Figure 3: Packet Delivery Ratio v/s Number of nodes

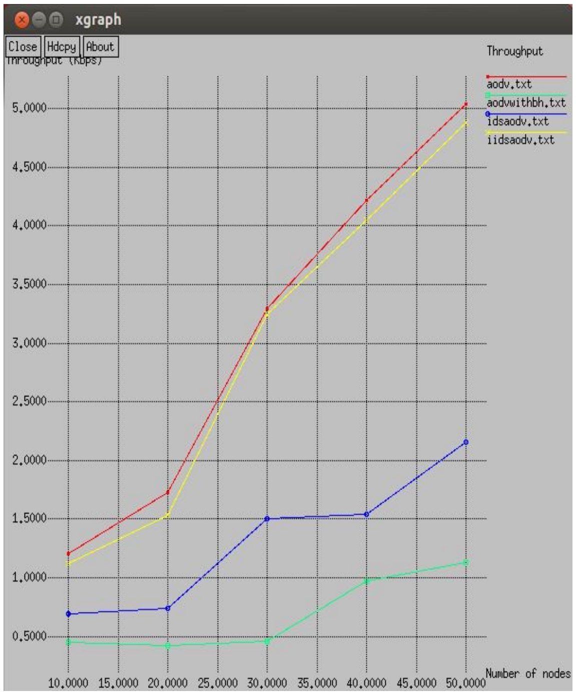

Figure 4: Network Throughput v/s Number of Nodes

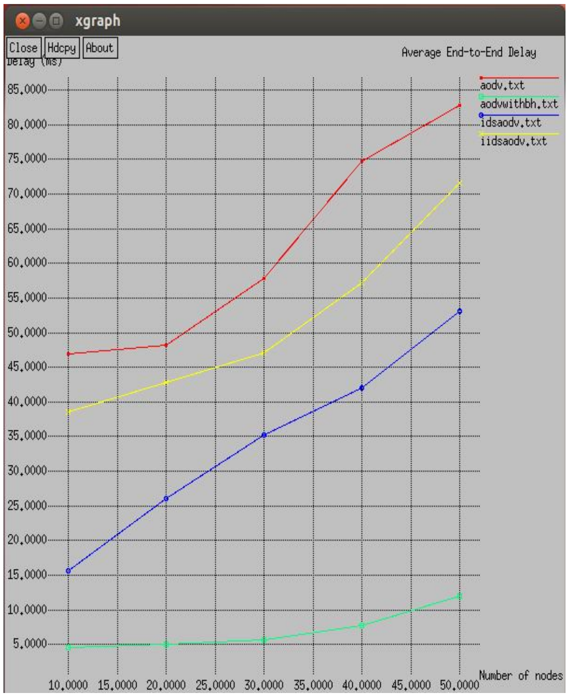

Figure 5: Average End-to-End delay v/s Number of Nodes

6. CONCLUSION

In this paper, the effects of black hole attack are analyzed in ad hoc networks. For demonstrating the effect of a black hole, a protocol BLACKHOLEAODV is implemented in ns-2. A solution IIDSAODV is also proposed to reduce the effect of black hole attack, which is an improvement over existing protocol IDSAODV. The different scenarios of varying network sizes and number of connections are created. A black hole node is also added in each scenario using BLACKHOLEAODV protocol. The analysis and comparison of AODV, IDSAODV and IIDSAODV is performed using these network scenarios. It has been analyzed that among the three protocols, IIDSAODV provides the best results for packet delivery ratio, network throughput and end-to-end delay.

The proposed protocol IIDSAODV has all the advantages of the existing protocol IDSAODV. First, it can work together with the AODV protocol, as it does not make any modification in the packet format. Second, it does not require any additional overhead to keep a black hole list through a different protocol. Additionally, it overcomes the drawback of IDSAODV which is the probability of second RREP being from a black hole node by imposing a check on it.

REFERENCES

[1] A. Mishra and K. M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book "The Handbook of Ad Hoc wireless Networks (Chapter 30)", CRC Press LLC, 2003.

[2] C. E. Perkins and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing". In The Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, February 1999.

[3] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto. "Detecting Black hole 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.

[4] NS by Example, http://nile.wpi.edu/NS, 14 May 2006.

[5] S. Dokurer,"Simulation of Black hole attack in wireless Ad-hoc networks", Master's thesis, AtılımUniversity, September 2006.

[6] F. H. Tseng, L. D. Chou and H. C. Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences, Vol. 1, No. 4, pp.1-16, doi:10.1186/2192-1962-1-4, 2011.

[7] A. Chaturvedi, S. Sharma, "Exploring Intrusion Detection Schemes and their Comparison in MANETs", International Journal of Computer Applications, vol. 71, No. 10, pp. 55-59, doi:10.5120/12398-8780, June 2013.

[8] T. Anantvalee and J. Wu, "A survey on Intrusion Detection in Mobile ad Hoc Networks", Book Series Wireless Network Security, Springer, pp. 170-196, ISBN: 978-0-387-28040-0, 2006.

[9] B. Sun, Y. Guan, J. Chen and U. Pooch, "Detecting Black-hole Attack in Mobile Ad-Hoc Networks," 5th European Personal Mobile Communications Conference, pp.490-495, Scotland, 2003.

[10] H. Deng, W. Li, D. P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communication Magazine, vol. 40, No. 10, pp. 70-75, October 2002.

[11] N. Mistry, D. C. Jinwala, M. Zaveri, "Improving AODV Protocol Against Blackhole Attacks", Proceedings of the International MultiConference of Engineers and Computer Scientists 2010 Vol. II, IMECS, 17-19 March, Hong Kong, 2010.

[12] Z. Ahmad, K.A. Jalil, J.A. Manan, "Black hole effect mitigation method in AODV routing protocol", 7th International Conference on Information Assurance and Security (IAS), pp. 151-155, doi:10.1109/ISIAS.2011.6122811, Melaka, 2011.

[13] K.A. Jalil, Z. Ahmad, and J.A. Manan, "An Enhanced Route Discovery Mechanism for AODV Routing Protocol ", ICSECS 2011, Part III, CCIS 181, pp. 408–418, Springer-Verlag Berlin Heidelberg, 2011.

[14] N. H. Mistry, D. C. Jinwala and M. A. Zaveri, "MOSAODV: Solution to Secure AODV against Blackhole Attack ", (IJCNS) International Journal of Computer and Network Security, Vol. 1, No. 3, December 2009.

[15] C. Perkins, E. B. Royer, S. Das, " Ad hoc On-Demand Distance Vector (AODV) Routing Internet Draft", RFC 3561, IETF Network Working Group, July 2003.