Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

Resolving Black hole Attack in AODV using Proposed Intrusion Detection System

Mukesh Azad
M.Tech(CSE) Student
Uttarakhand Technical University

Sanjay Kumar
Department of CSE
Uttarakhand Technical University

Rohit pal
M.Tech(IT) Student
Graphic Era University

Anant Verma
M.Tech(PED)
DIT University

***Abstract* : Ad hoc networks are characterized by open medium, dynamic topology, distributed cooperation and constrained capability with more challenges for security. Routing security is the most important factor in the security of the entire network. However, few of current routing protocols have the consideration about the security problems. This paper emphasizes on the black hole attack in the AODV protocol. To provide security in AODV protocol, firstly we have to trace malicious behavior of node. Specially, we analyzed the black hole node behavior and proposed a security system to detect such black hole node in the network and made the secured system that optimizes the loss of packets from such type of attack.**

1. Introduction

A MANET is an autonomous collection of mobile users that communicate over relatively "slow" wireless links. The nodes are mobile so the network topology may change swiftly and unpredictably over time. The network is decentralized thus all network activity, including discovering the topology and delivering messages must be accomplished by the nodes themselves. [2]

Each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. The network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. An ad hoc wireless network should be able to handle the possibility of having mobile nodes, which will most likely increase the rate at which the network topology changes. Accordingly the network has to be able to adapt quickly to changes in the network topology. This implies the use of efficient handover protocols and auto configuration of arriving nodes.

1.1 Routing Protocols in MANETs

Routing protocols may generally be categorized as:

a) Table-driven or Proactive routing protocols.
b) On-demand or Reactive routing protocols.

Table-driven or Proactive routing protocols :

A Proactive (Table-driven) Routing Protocol attempts to allow each node using it to always maintain an up-to-date route to each possible destination in the networks, the protocol periodically exchanges routing information with other nodes in order to allow new route to be discovered and existing route to be modified if they break due to factors such as node mobility and environmental changes.

On-demand or Reactive routing protocols :

A Reactive (On Demand) Routing Protocol only attempts to a discover a route to some destination when it has a packet to route to some destination when it has a packet route to that destination and does not already know a route there; the protocol catches known routes and uses a flooding based discovery protocol when a needed route is not found in the cache [20]. E.g. AODV (Ad hoc On demand Distance Vector) Routing Protocol.

The Path finding mechanism for AODV is as follows:

When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node[1]. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination

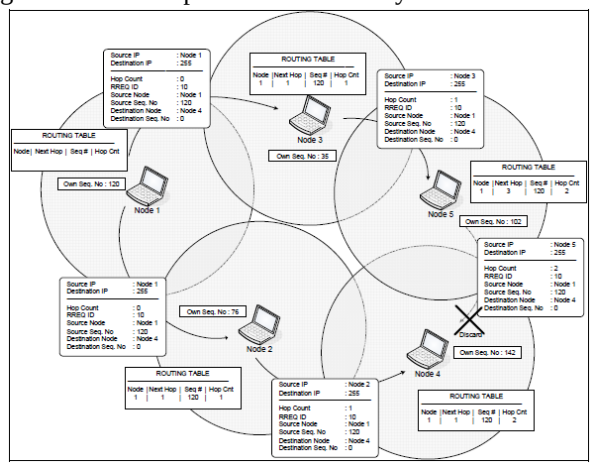

Figure 1 – Propagation of the RREQ message

node or an intermediate node that has a fresh enough route entry for the destination. Figure 1 shows how

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

the RREQ message is propagated in an ad-hoc network.

Fresh enough means that the intermediate node has a valid route to destination formed a period of time ago, lower than the threshold. While the RREQ packet travels through the network, every intermediate node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node.[4]

Afterwards the RREP message is unicasted to the source node. The difference between the broadcasting an RREQ and unicasting RREP can be seen from Figures 1 and 2. While the RREQ and the RREP messages are forwarded by intermediate nodes, intermediate nodes update their routing tables and save this route entry for 3 seconds, which is the ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol. Figure 2 shows how the RREP message is unicasted and how the route entries in the intermediate nodes are updated.

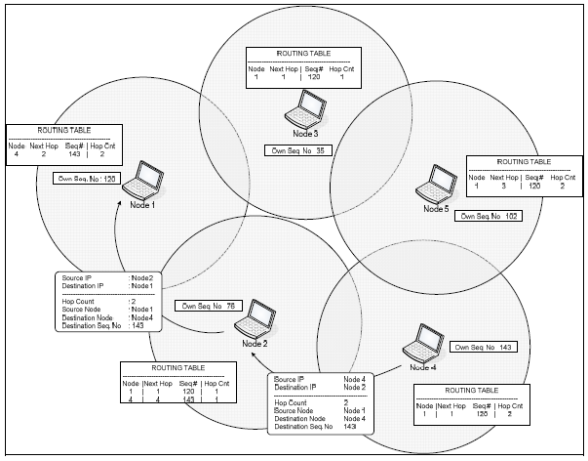

Figure 2 – Propagation of the RREP message

2. Black Hole Attack in MANETs

Black Hole Attack is severely affect the data flow in the network. In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets. To explain the Black Hole Attack we added a malicious node that exhibits Black Hole behavior in the network, Figure 3 we assume that Node 3 is the malicious node.

When Node 1 broadcasts the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that includes the highest sequence number of Node 4, as if it is coming from Node 4. Node 1 assumes that Node 4 is behind Node 3 with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will reach Node 4 but Node 3 will drop all data packets.[3]

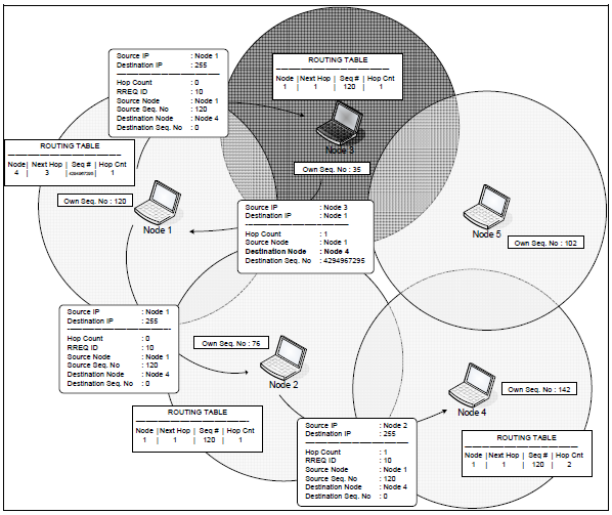

Figure 3 – Illustration of Black Hole Attack

In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets.[2]

3. Proposed Work & Implementation

In this paper we discussed about the black hole attack that how a black hole node works and now we move to the mechanism to be implemented to resolve the black hole attack.

3.1 Proposed Mechanism

In this work, we have tried to evaluate the effects of the Black Hole attacks in the wireless Ad-hoc Networks. To achieve this we have simulated the wireless ad-hoc network scenarios which includes Black Hole node using NS-2(Network Simulator version 2) [14]. To simulate the Black Hole node in a wireless ad-hoc network we have implemented a new

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

protocol that drops data packets after attracting them to itself. In this paper we present NS and our contribution to this software. We added a new protocol "blackholeaodv" by slightly modifying AODV, to show the effects of the black hole attack and after that we created a cache to store the information about the reply from various nodes, for the solution to resolve the black hole node. This cache is implemented in the new protocol "idsaodv", contains an entry for each reply from the nodes of the network. When a black hole node receives a request, it immediately makes a reply without analyzing the shortest path, so the time getting a reply from a black hole node is minimum that can be compared with other replies to get the secured and shortest path. So the sender waits for a while to get all the replies and then prefers the path that has minimum nodes if the time for first reply is very short compared to other replies.

4. Experiments and Results Analysis

This analysis verifies of our experiments that we have done previous section. The data is extracted from blackholeAttack.tr and idsAODV.tr and packet loss is calculated. Figure 4 and Figure 5 shows the scenarios for attack of black hole node that how the increased packet loss % and decreased throughput, in presence of black hole node.

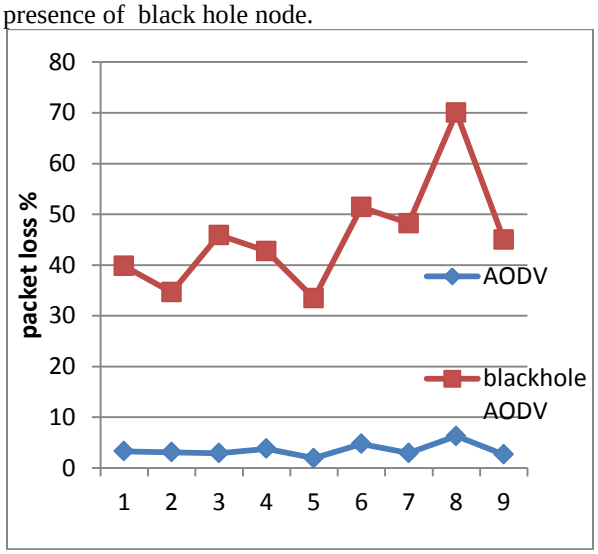

Figure 4 -- Scenario for packet loss

Now, we can see that packet loss % increased significantly in presence of a black hole node but when we take the other nodes as ids node the packet loss % is decreased. This is conformed from the Figure 6 and Figure 7 that the packet loss % is decreased and throughput is increased, in presence of ids nodes even when the black hole node is present in the network.

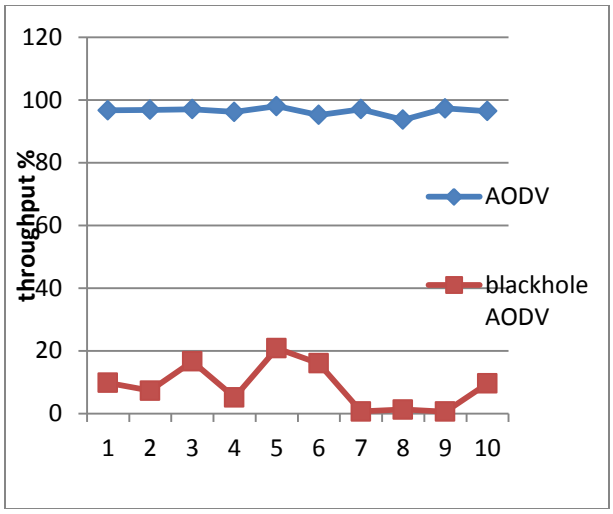

Figure 5 -- Scenario for throughput

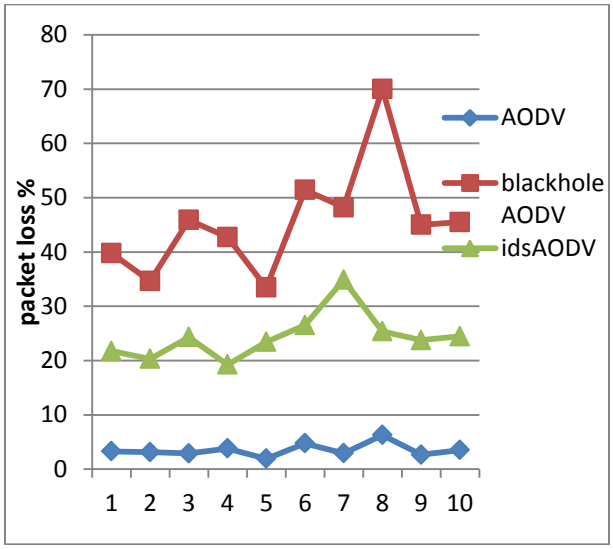

Figure 6 -- Scenario for packet loss

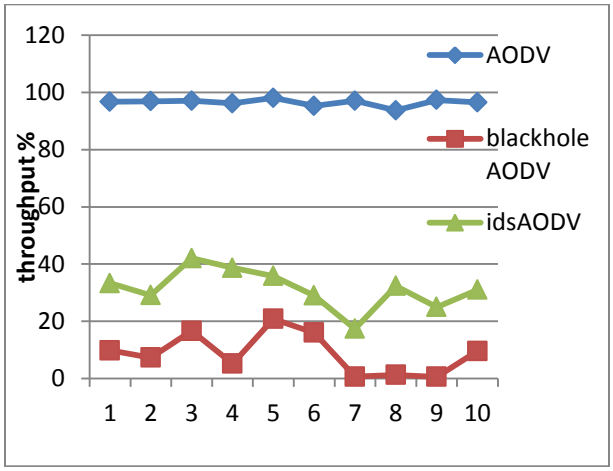

Figure 7 -- Scenario for throughput

Proc. of the Second Intl. Conf. on Advances in Electronics, Electrical and Computer Engineering -- EEC 2013

ISBN: 978-981-07-6935-2

5. CONCLUSION AND FUTURE WORK

5.1 Conclusion

In this study, we analyzed effect of the Black Hole in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. We simulated different scenarios where each one has 20 nodes that use AODV protocol and also simulated the same scenarios after introducing one Black Hole Node into the network. Moreover, we also implemented a solution that attempted to reduce the Black Hole effects in NS-2 and simulated the solution using the same scenarios. Our simulation results are analyzed below:

Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network. In graphs of simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase.

5.2 Future Work

We simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be determined.

In our thesis, we try to eliminate the Black Hole effect in the network. But detection of the Black Hole Node is another future work. In our work, we assume the black hole node is detected and tried to eliminate its effects. There are many Intrusion Detection Systems (IDS) for ad-hoc networks. These IDSs could be tested to determine which one is the best to detect the Black Hole. Our solution tries to eliminate the Black Hole effect at the route determination mechanism of the AODV protocol that is carried out before the nodes start the packets. Additionally, we used UDP connection to be able to count the packets at sending and receiving nodes. If we had used the TCP connection between nodes, the sending node would be the end of the connection, since ACK packets do not reach the sending node. This would be another solution for finding the Black Hole Node.

This takes place after the route determination mechanism of the ADOV protocol and finds the route in a much longer period. Our solution finds the path in the AODV level. Finding the black hole node with connection oriented protocols could be another work as a future study.

References

[1] Buchegger, S. and Boudec, J. 2002. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes—Fairness In Distributed Ad hoc NeTworks. In Proceeding ACM Workshop Mobile Ad Hoc Networking and Computing (Switzerland, 2006). 226-236.

[2] Hongmei Deng, Wei Li, Dharma P. Agarwal, “Routing Security in Wireless Ad-Hoc Networks” in IEEE Communication Magazine Oct. 2002.

[3] Kwan-Wu Chin, John Judge, Aidan Williams and Roger Kermode,” Implementation Experience with MANET Routing Protocols” ACM SIGCOMM Computer Communications Review ,Volume 32, Number 5: November 2002.

[4] P.Michiardi and R. Molva,"Ad hoc Networks Security",IEEE Press Wiley, New York, 2003.

[5] Sudipto Das, “Security issues in Mobile Ad-Hoc networks”, Springer, 2003

[6] T. R. Sheltami, and H. T. Mouftah, “A Comparative Study of On-Demand and Cluster-Based Routing Protocols in MANETs,” IEEE EWCN, April 9-11, 2003, Phoenix, Arizona, USA, pp. 291-295.

[7] Han L, "Wireless Ad hoc Network", October 8, 2004.

[8] Wei, G., Zhongwei, X. and Zhitang, L. 2005. Dynamic trust evaluation based routing model for ad hoc networks," IEEE International Workshop on Future Trends. 727-730.

[9] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks ,” Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[10] Jun Liu*, Jiejun Kong, Xiaoyan Hong, Mario Gerla ,'Performance Evaluation of Anonymous Routing Protocols in MANETs', *IEEE Wireless Communications and Networking Conference 2006 (WCNC06)*, Las Vegas, April 2006.

[11] I. Msadaa. Int´egration de la Norme IEEE 802.16 dans l’environnement de simulation NS2. Computer Science Master’s thesis, Ecole Nationale des Sciences de l’Informatique, Tunisia, Dec. 2006.

[12] Li H, Singhal M (2006) A secure routing protocol for wireless ad hoc networks. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences - Volume 09, pages 225.1–, Washington, DC, USA. IEEE Comput Soc

[13] Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini, “Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs Networks ,” 32nd IEEE Conference on Local Computer Networks 0742-1303/07 $25.00 © 2007 IEEE.

[14] Kamanshis Biswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network", Master Thesis, Thesis no: MCS-2007:07, March 22, 2007.

[15] Qingting Wei, Hongzou. “Efficiency Evaluation & Comparison of Routing Protocols in MANETs” in International Symposium on Information Science & Engineering . Volume: 2 Information Science and Engineering, 2008. ISISE '08.

[16] Samian N, Maarof MA, Razak SA (2008) Towards identifying features of trust in mobile ad hoc network. In

ISBN: 978-981-07-6935-2

Proceedings of the 2008 Second Asia International Conference on Modelling & Simulation (AMS), pages 271–276, Washington, DC, USA, 2008. IEEE Comput Soc

[17] Saxena N, Tsudik G, Yi JH (2009) Efficient node admission and certificateless secure communication in short-lived manets. Parallel and Distributed Systems, IEEE Transactions 20(2):158–170.

[18] Payal N. Raj and Prashant B. Swades, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET" , IJCSI International Journal of Computer Science Issues, Vol. 2, 2009 ISSN (Online): 1694-0784 ISSN (Print): 1694-0814.

[19] Vaithiyanathan, Gracelin Sheeba.R, Edna Elizabeth. N, Dr.S.Radha, "A Novel method for Detection and Elimination of Modification Attack and TTL attack in NTP based routing algorithm", 2010 International Conference on Recent Trends in Information, Telecommunication and Computing 978-0-7695-3975-1/10 $25.00 © 2010 IEEE.

[20] Shailender Gupta, Chander Kumar, "Shared Information based Security Solution for Mobile Adhoc Networks", International Journal of Wireless and Mobile Networks, Vol. 2,No. 1, February 2010.

[21] Jain, S., Jain, M., and Kandwal H. Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. J. Computer Applications, Vol. 1, No. 7, 37-42, 2010.

[22] Ming-Yang Su, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems , Computer Communications, Volume 34, Issue 1, 15 January 2011, Pages107-117

[23] Jan von Mulert, Ian Welch, Winston K.G. Seah, Security threats and solutions in MANETs: A case study using AODV and SAODV, Journal of Network and Computer Applications, Volume 35, Issue 4,July2012,Pages1249-1259

[24] Sergio Pastrana, Aikaterini Mitrokotsa, Agustin Orfila, Pedro Peris-Lopez, Evaluation of classification algorithms for intrusion detection in MANETs, Knowledge-Based Systems, Volume36,December 2012, Pages217-225