Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

Impact Factor: 5.258

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 2, February 2016, pg.305 – 311

DETECTION OF BLACK HOLE ATTACK USING SAODV PROTOCOL

Vinod Bhupathi, P Priyanka, G Srikanth Reddy
Assistant Professor, IT Dept, Vardhaman College of Engineering, Hyderabad
Assistant Professor, IT Dept, Vardhaman College of Engineering, Hyderabad
Assistant Professor, IT Dept, Vardhaman College of Engineering, Hyderabad

Abstract:

Mobile Ad-hoc network is a self organized infrastructure less network where a mobile node communicates each other for communication. The mobile nodes usually takes a support of protocol to transfer information from one node to another node. The wireless network is vulnerable against various types of attacks such as Black Hole, Warm Hole, Byzantine Attack etc. In this paper, we discuss the effect of black hole attack with AODV protocol and proposes a solution with SAODV Protocol. At first we create a network in which mobile nodes use AODV protocol to transfer data packets from one node to another node, then a malicious black hole attack is implemented in the same network to measure throughput, packet delievery ratio and delivery ratio and delay of attacker implemented network. The SAODV with security mechanism to avoid the implemented attack and transfer packets securely to measure throughput and packet delivery ratio. At last we compare the performance of AODV implemented network and SAODV implemented network for a Black Hole.

Introduction:

A mobile ad-hoc network is a wireless network with self configuring network. The wireless networks consists a large number of wireless devices connected for information exchange from one host to another host called as routing. Routing is a process of forwarding packets from one host to another host in the network. Routing in MANET can be done two ways, where as in pro-active routing protocols every node continuously maintains the routing information of the network. In Reactive routing [2] protocols every node maintains the information of only active paths to the destination nodes. The pro-active routing protocols are Ad hoc on Demand distance vector routing (AODV), Dynamic source Routing (DSR) etc.

AODV protocol is most widely used protocol for MANET. All mobile nodes work in cooperation to find a route path from source to destination node. The data transmission takes place only after the route is established. There are three types of control messages in AODV protocols. They are Route Request (RREQ) [1], Route Reply (RREP) and Route Error (RERR). To find the path of destination node the RREQ message is broadcasted to all the neighboring in the network. The destination node which receives the RREQ message, it sends a RREP packet to the sender verifying the packet or message. This generally explains how a packet is being forwarded in the pro-active networks.

Security is always an important issue in the process of communication in network. There are two types of attacks in ma net. The passive attack does not disrupt proper operation of the network. The attacker snoop's the data exchanged in the network without altering it. In active attack [3], the intruder attempts to alter or destroy the data being exchanged in the network. There are different types of active attack, some of them are Black hole attack, warm hole attack, Byzantine attack etc.

In Black hole attack [5], a malicious node uses the routing protocol to advertise itself as having the shortest path to the node packets it wants to intercept. The attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply consisting of an extremely short route. If the malicious reply reaches the requesting node before the reply from the actual node, a forged route gets created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to drop the packets to perform a denial-of-service attack. In our study we analyzed the results of various simulations that ran black-hole attack in wireless ad-hoc network and the effect of this attack on packet delivery.

In this paper we propose method to find the secure AODV protocol in the following manner:

a. We Create a base wireless sensor network with 20-50 number of nodes use AODV as a routing protocol and transfer packets from sender to receiver i.e., a standard network creation with AODV protocol.
b. We Implement attack Black hole in the created network and transfer packets from sender node to receiver i.e., attacker implementation without security.

c. We Implement a Black hole attack with created network and transfer packets from sender node to receiver with security mechanism i.e., attacker implementation with security.
d. We Measure Throughput, Packet delivery ratio and delay of attacker implemented network and outputs are shown using graphs i.e., Performance measures of Attacker Implemented network.
e. Compare performance of AODV implemented network, Attacker implemented network and Secure AODV implemented network and outputs are shown using graphs i.e., Result Analysis by implementing plot graphs.

The Section 2 describes

Related Work:

Mc donald [6] proposes a protocol based on network and link layer acknowledgement but can be failed in heavy traffic as the acknowledgement packet may not reach in time and packets like UDP do not provide any acknowledgement at all. They have implemented the solution using DSR protocol. TAODV [7] is a other protocol based on trust which has two messages like Trust Request (TREQ) and Trust Reply (TREP). S. marati [8] introduced a concept of watch dog, where the intruder node watches the user information. S. park[9] proposed a method where the destination waits for the multiple sender's for a RREP packet. Satoshi has proposed a method [2] based on the number of RREQ messages sent and RREP messages received. It calculated the average sequence number and try to find out the malicious node, as the malicious node will send RREP messages with extremely higher sequence number.

Proposed Algorithm:

The proposed algorithm Secure AODV protocol is used to mitigate the black holes and warm holes in a Manet. At first a standard network is created with a AODV protocol then an attacker implementation is done without security and later an attacker implementation with a security is done. And then performance measures such as Through put, packet delivery. Then a Secure AODV protocol with security mechanism to avoid the implemented attack and transfer packets from sender to receive and performance measures are done for the secure AODV protocol.

Secure ad hoc on demand vector routing protocol is an extension to the AODV protocol for computing security mechanism with collaborative black hole attack and wormhole attack. The AODV protocol has a provision of sending a gratuitous RREP packet to the destination node. Whenever a intermediate node has a route towards destination, in addition to sending the RREP to the source, it also uni casts a gratuitous RREP to the destination node. In our protocol the gratuitous RREP is conceptualized and simulated as the CONFIRM packet. Thus, a CONFIRM packet is uni casted/routed by the RREPN to the destination. Note that it can be sent

only if the RREPN has a route towards destination. It is only after the receipt of CONFIRM will the destination a wait for packets from the source. In order to facilitate cross checking by the source (of the route claimed by the RREPN), the source unicasts a CHCKCNFRM to the destination. Upon CHCKCNFRMs receipt the destination replies by broadcasting a REPLYCONFIRM to the source, only if it received a CONFIRM and a CHCKCNFRM. Since a black hole does not possess a route towards the destination, it fails to send the CONFIRM, thus reply to the CHCKCNFRM is never generated by the destination. This leads the source to conclude that the RREP sending node was the black hole one. The proposed algorithm will hereafter be called as the Secure AODV protocol. It gets its name from the utilization of the gratuitous RREP.

Simulation Parameters:

We plan to simulate in NS2 (Network Simulator). NS2 simulator generates a TCL (Tool Command Language) file. On running a TCL file it results three more files, namely the first one is Terminal File which shows the status of the packet from which node the packet is forwarded and to which node the packet is delivered. The second file is NAM (Network Animator) file which is a visual display showing all the mobile nodes and how packets flow along the network. The third file is the Trace File which shows all the corresponding information regarding the network and data flow.

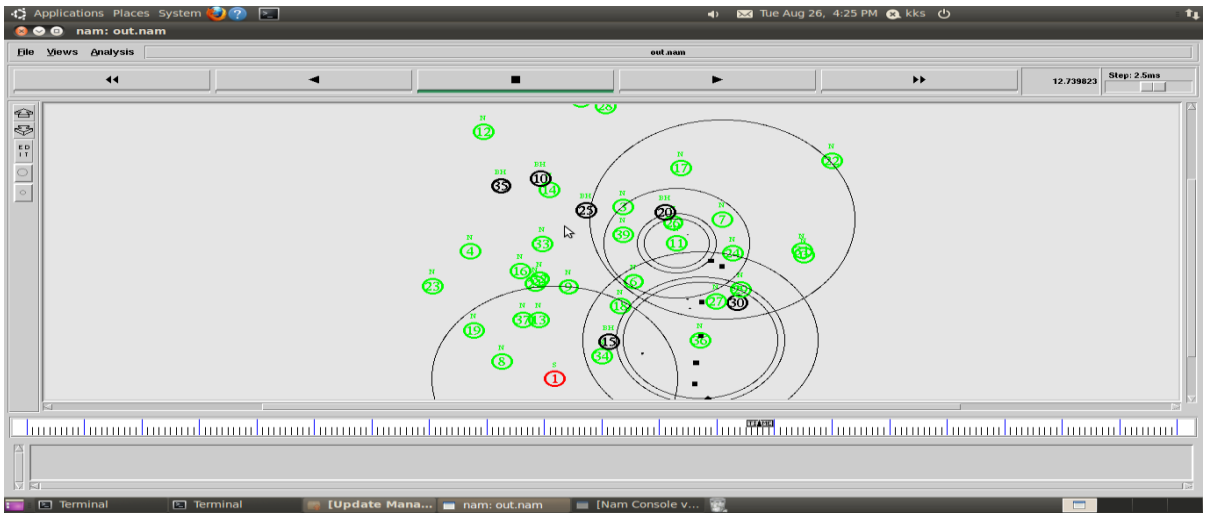
PARAMETER	SPECIFICATION
Simulation tools used	NS2 Network Simulator NS 2.35
Simulation Time	10s, 20s
Number of nodes	10,20,40,60,100,250,500,750,1000
Transmission Range	250m
Maximum Speed	0-22 m/s
Application Traffic	CBR [constant Bit Rate]
Packet Size	512 bytes
Protocol	AODV, Secure AODV
Node Mobility Model	8 Pkts/s
Types of Attack	Black Hole, Warm Hole Attack

A network is created with multiple nodes which uses a AODV protocol. Then an attacker node is implemented, where it generates the performance of the manet. Then a security mechanism is implemented to mitigate the malicious nodes, a method to reduce the Black hole and warm hole

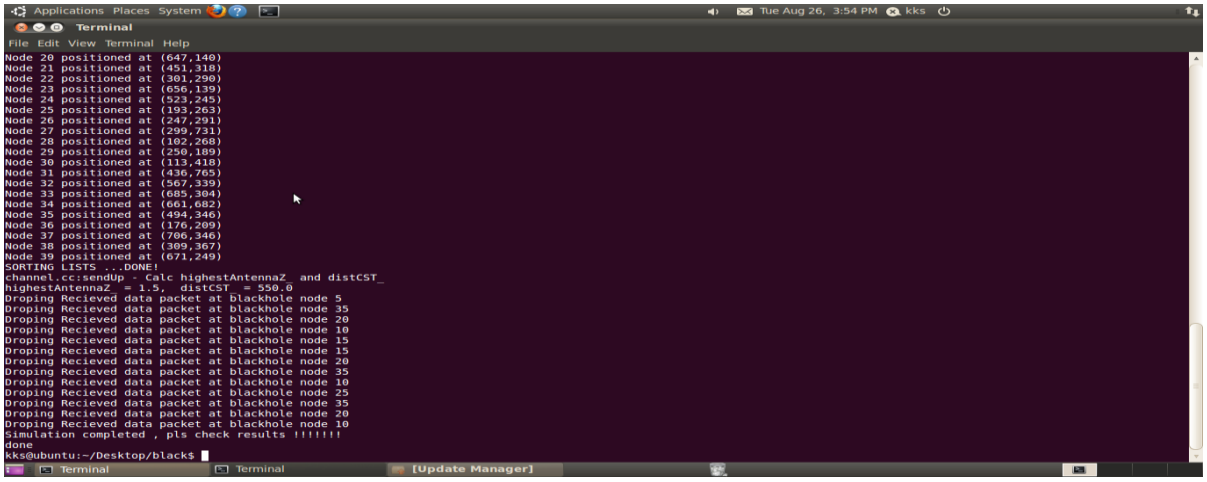
is simulated. And a plot graph is generated based on the performance of the manet with Black hole and warm hole in a secure AODV protocol.

Result Analysis:

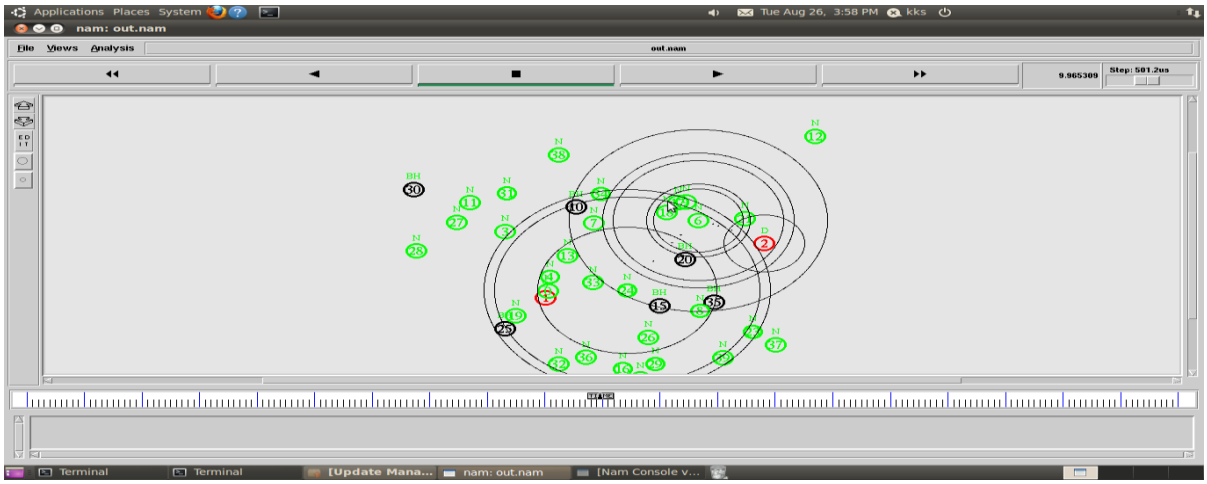
In this module we compare the existing implemented AODV protocol and new implemented secure AODV protocol.
we Analysis the performance of normal AODV protocol and secure AODV protocol.
At first a AODV protocol without attack is implemented & then we plan to mitigate the same network with a malicious node in it. Where a malicious node is implemented in AODV protocol.



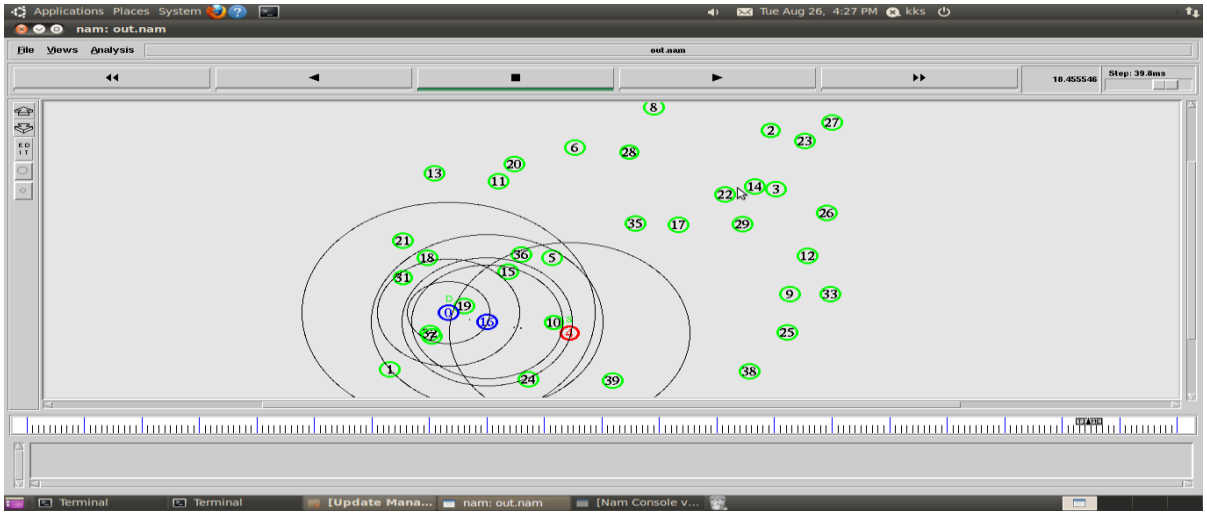
By introducing the malicious nodes, the packet drop can be done. The below simulation results show the packet drop in a manet when a black hole is implemented.



Then a AODV protocol with a trust approach is applied:



We plan to mitigate the Black hole in the below manet:



Conclusion:

In this paper, we propose a trust based mechanism to avoid the Black hole. We discuss a simple yet mechanism to identify the misbehaving nodes to detect black hole. A base wireless network is created with AODV protocol and then we implement a black hole attack. Then a SAODV protocol is proposed on to detect the black hole attack. The comparison graphs of two protocols AODV and SAODV is done to detect the packet drop, throughput and packet delivery ratio. The results shows that a secured protocol is being developed to detect the black hole attack. In the

future we plan to identify more different types of attacks with a Secure AODV for secure data transmission.

References:

1. Abhay kumar rai, rajiv rajan tiwari, “Different Types of Attacks on Integrated MANET-Internet Communication”,.
2. Amit Shrivastava, Nitin Chander, “Overview of Routing Protocols in MANET’s and Enhancements in Reactive Protocols ”,
3. Fidel Thachil, K C Shet, “A trust based approach for AODV protocol”, 2012 International Conference on Computing Sciences.
4. L. Lazos, R. Poovendran, “Preventing Wormhole Attacks on Wireless Ad HocNetworks”,.
5. Shree om, mahammad Talib, “Wireless Ad-hoc Network under Black-hole Attack”, International Journal of Digital Information and Wireless Communications (IJDIWC) 1(3): 591-596.
6. Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Proc. 8th Ann. Int’l Conf. Mobile Computing and Networking (MobiCom’02), ACM Press, 2002.
7. Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehaviour in mobile ad hoc networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, MOBICOM, Boston, Massachusetts, August 2000.
8. Asad Amir Pirzada and Chris McDonald. Establishing Trust In Pure Ad-hoc Networks. In Proceddings 27th Australasian Computer Science Conference (ACSC'04), Dunedin, New Zealand, 26(1), pages 47-54, January 2004.
9. A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks. PhD thesis, Department of Computer Science and Engineering, The Chinese University of Hong Kong, 2003
10. Seungjin Park, M. Al-Shurman and Seong-Moo Yoo. Black Hole Attack in Mobile Ad hoc Network, ACMSE'04, Huntsville, AL, U.S.A., April, 2004.

